

# Introduction to Quantum Programming and Semantics

Week 6: Monoids and comonoids

Chris Heunen



THE UNIVERSITY *of* EDINBURGH  
**informatics**

# Overview

- ▶ Monoids: multiplication of states
- ▶ Comonoids: 'copying' of states
- ▶ Cloning: prove no-cloning and no-deleting
- ▶ Products: characterize when tensor product is product

# Copying

What does `copying` object *A* mean?

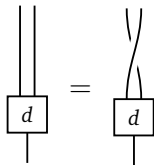
# Copying

What does **copying** object  $A$  mean? Type should be  $A \xrightarrow{d} A \otimes A$

# Copying

What does **copying** object  $A$  mean? Type should be  $A \xrightarrow{d} A \otimes A$

- ▶ shouldn't matter if we switch both output copies

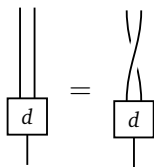


cocommutativity

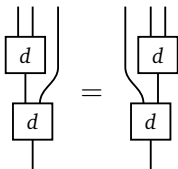
# Copying

What does **copying** object  $A$  mean? Type should be  $A \xrightarrow{d} A \otimes A$

- ▶ shouldn't matter if we switch both output copies
- ▶ if copying twice, shouldn't matter if take first or second copy



cocommutativity

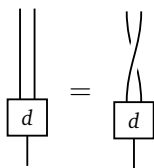


coassociativity

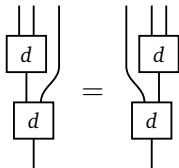
# Copying

What does **copying** object  $A$  mean? Type should be  $A \xrightarrow{d} A \otimes A$

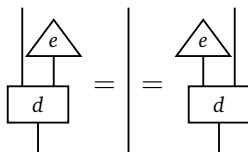
- ▶ shouldn't matter if we switch both output copies
- ▶ if copying twice, shouldn't matter if take first or second copy
- ▶ output should equal input: uses **deletion**  $A \xrightarrow{e} I$



cocommutativity



coassociativity

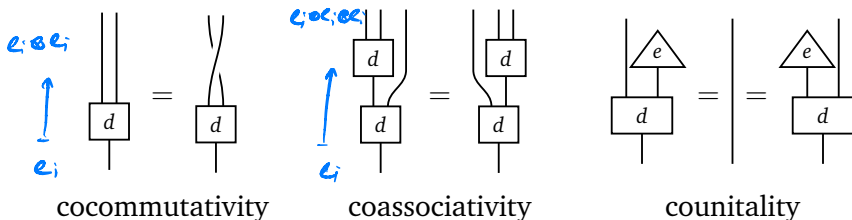


counitality

# Copying

What does **copying** object  $A$  mean? Type should be  $A \xrightarrow{d} A \otimes A$

- ▶ shouldn't matter if we switch both output copies
- ▶ if copying twice, shouldn't matter if take first or second copy
- ▶ output should equal input: uses **deletion**  $A \xrightarrow{e} I$



Triple  $(A, d, e)$  is called **(cocommutative) comonoid**.

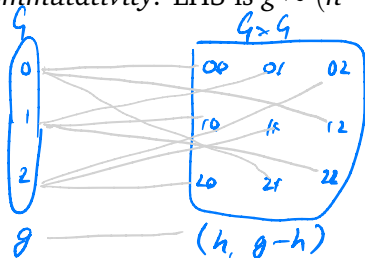


## Example comonoids

- ▶ In **Set**, the tensor product is a Cartesian product. Every object carries a unique comonoid with comultiplication  $a \mapsto (a, a)$  and counit  $a \mapsto \bullet$ , which is cocommutative.

## Example comonoids

- ▶ In **Set**, the tensor product is a Cartesian product. Every object carries a unique comonoid with comultiplication  $a \mapsto (a, a)$  and counit  $a \mapsto \bullet$ , which is cocommutative.
- ▶ In **Rel**, any group  $G$  forms a comonoid with comultiplication  $g \sim (h, h^{-1}g)$  and counit  $1 \sim \bullet$ .  
*Counitality:* LHS is  $g \sim h$  where  $h^{-1}g = 1$ , RHS is  $g \sim 1^{-1}g$ .  
The comonoid is cocommutative iff the group is abelian.  
*Cocommutativity:* LHS is  $g \sim (h^{-1}g, h)$ , RHS is  $g \sim (k, k^{-1}g)$ .



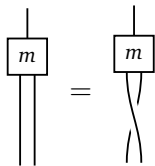
(made some mistakes)

## Example comonoids

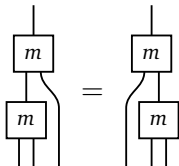
- ▶ In **Set**, the tensor product is a Cartesian product. Every object carries a unique comonoid with comultiplication  $a \mapsto (a, a)$  and counit  $a \mapsto \bullet$ , which is cocommutative.
- ▶ In **Rel**, any group  $G$  forms a comonoid with comultiplication  $g \sim (h, h^{-1}g)$  and counit  $1 \sim \bullet$ .  
*Counitality:* LHS is  $g \sim h$  where  $h^{-1}g = 1$ , RHS is  $g \sim 1^{-1}g$ .  
The comonoid is cocommutative iff the group is abelian.  
*Cocommutativity:* LHS is  $g \sim (h^{-1}g, h)$ , RHS is  $g \sim (k, k^{-1}g)$ .
- ▶ In **FHilb**, basis  $\{e_i\}$  for a Hilbert space gives a cocommutative comonoid, with comultiplication  $e_i \mapsto e_i \otimes e_i$  and counit  $e_i \mapsto 1$ .

# Monoids

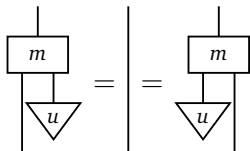
Dually:



*commutativity*



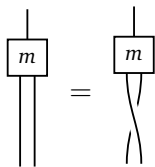
*associativity*



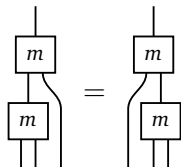
*unitality*

# Monoids

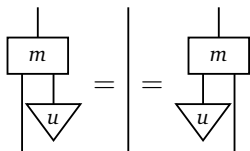
Dually:



*commutativity*



*associativity*

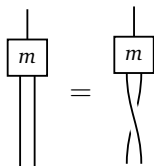


*unitality*

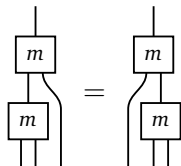
Triple  $(A, m, u)$  is (commutative) monoid.

# Monoids

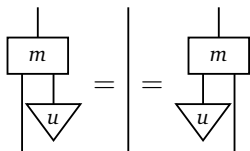
Dually:



*commutativity*



*associativity*



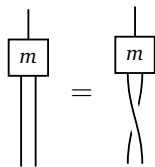
*unitality*

Triple  $(A, m, u)$  is **(commutative) monoid**. Examples:

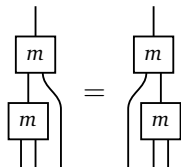
- ▶ Tensor unit  $I$ , with multiplication  $\rho_I = \lambda_I$  and unit  $\text{id}_I$ .

# Monoids

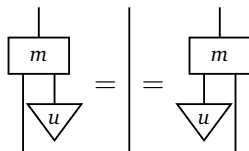
Dually:



*commutativity*



*associativity*



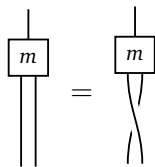
*unitality*

Triple  $(A, m, u)$  is (**commutative**) **monoid**. Examples:

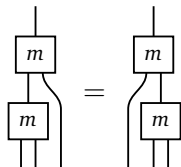
- ▶ Tensor unit  $I$ , with multiplication  $\rho_I = \lambda_I$  and unit  $\text{id}_I$ .
- ▶ A monoid in **Set** is just an ordinary monoid; e.g. any group.

# Monoids

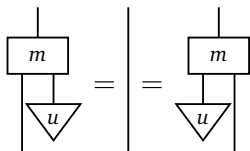
Dually:



*commutativity*



*associativity*



*unitality*

Triple  $(A, m, u)$  is (**commutative**) **monoid**. Examples:

- ▶ Tensor unit  $I$ , with multiplication  $\rho_I = \lambda_I$  and unit  $\text{id}_I$ .
- ▶ A monoid in **Set** is just an ordinary monoid; e.g. any group.
- ▶ A monoid in **Vect** is an *algebra*: a set where we can add vectors and multiply with scalars, and also multiply vectors bilinearly. E.g.  $\mathbb{C}^n$  under pointwise multiplication and unit  $(1, 1, \dots, 1)$ . E.g. vector space of  $n$ -by- $n$  matrices with matrix multiplication.



# Homomorphisms

Draw comultiplication as  $\varphi'$ , counit as  $\varphi$ , multiplication as  $\mu$ , unit as  $\nu$ .

# Homomorphisms

Draw comultiplication as  $\varphi'$ , counit as  $\varphi$ , multiplication as  $\mu$ , unit as  $\eta$ .

Choosing bases  $\{d_i\}$  and  $\{e_j\}$  makes  $H$  and  $K$  in **FHilb** comonoids.

# Homomorphisms

Draw comultiplication as  $\varphi'$ , counit as  $\varphi$ , multiplication as  $\mu$ , unit as  $\eta$ .

Choosing bases  $\{d_i\}$  and  $\{e_j\}$  makes  $H$  and  $K$  in **FHilb** comonoids.

Functions  $\{d_i\} \rightarrow \{e_j\}$  respect comultiplication and counit.

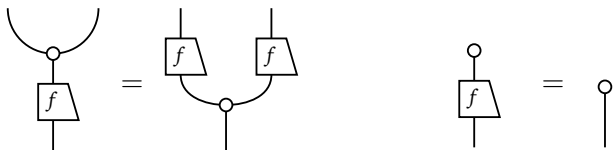
# Homomorphisms

Draw comultiplication as  $\varphi'$ , counit as  $\varphi$ , multiplication as  $\mu$ , unit as  $\eta$ .

Choosing bases  $\{d_i\}$  and  $\{e_j\}$  makes  $H$  and  $K$  in **FHilb** comonoids.

Functions  $\{d_i\} \rightarrow \{e_j\}$  respect comultiplication and counit.

A **comonoid homomorphism**  $(A, \varphi', \varphi) \rightarrow (B, \varphi', \varphi)$  is  $A \xrightarrow{f} B$  with:



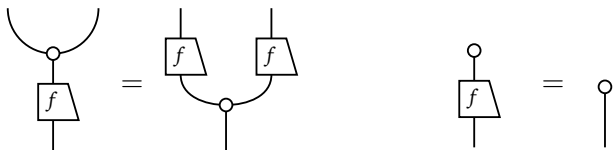
# Homomorphisms

Draw comultiplication as  $\varphi'$ , counit as  $\varphi$ , multiplication as  $\mu$ , unit as  $\eta$ .

Choosing bases  $\{d_i\}$  and  $\{e_j\}$  makes  $H$  and  $K$  in **FHilb** comonoids.

Functions  $\{d_i\} \rightarrow \{e_j\}$  respect comultiplication and counit.

A **comonoid homomorphism**  $(A, \varphi', \varphi) \rightarrow (B, \varphi', \varphi)$  is  $A \xrightarrow{f} B$  with:



Dually: **monoid homomorphism**.

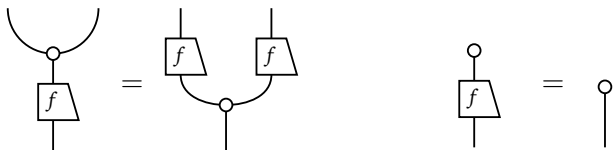
# Homomorphisms

Draw comultiplication as  $\varphi'$ , counit as  $\varphi$ , multiplication as  $\mu$ , unit as  $\eta$ .

Choosing bases  $\{d_i\}$  and  $\{e_j\}$  makes  $H$  and  $K$  in **FHilb** comonoids.

Functions  $\{d_i\} \rightarrow \{e_j\}$  respect comultiplication and counit.

A **comonoid homomorphism**  $(A, \varphi', \varphi) \rightarrow (B, \varphi', \varphi)$  is  $A \xrightarrow{f} B$  with:



Dually: **monoid homomorphism**.

Given monoidal category, can build new category of (co)monoids and homomorphisms.

## Example homomorphisms

- ▶ In **Set**, any function  $A \xrightarrow{f} B$  is a comonoid homomorphism:  
 $(f \times f)(a, a) = (f(a), f(a))$ , and  $f(a) = \bullet$ .

## Example homomorphisms

- ▶ In **Set**, any function  $A \xrightarrow{f} B$  is a comonoid homomorphism:  $(f \times f)(a, a) = (f(a), f(a))$ , and  $f(a) = \bullet$ .
- ▶ In **Rel**, any surjective homomorphism  $G \xrightarrow{f} H$  of groups is a comonoid homomorphism. Preservation of comultiplication: LHS is  $g \sim (h, h^{-1}f(g))$ , RHS is  $g \sim (f(g'), f(g')^{-1}f(g))$ .

$$\begin{array}{ccc}
 g \in G & \xrightarrow{f} & H \ni h \\
 \downarrow & & \downarrow \\
 G \times G & \xrightarrow{f \times f} & H \times H \ni (k, k^{-1}h) \quad \forall k \in H
 \end{array}$$

$$(k, k^{-1}f(g)) \stackrel{?}{=} (f(h), f(h)^{-1}f(g))$$

$\swarrow k=f(g)$

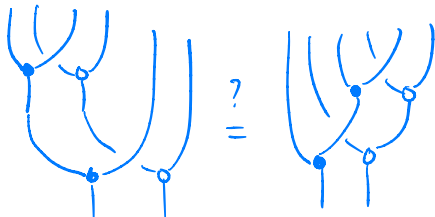
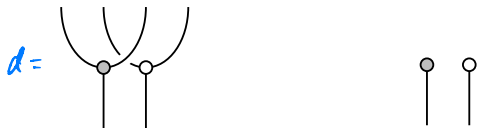


## Example homomorphisms

- ▶ In **Set**, any function  $A \xrightarrow{f} B$  is a comonoid homomorphism:  
 $(f \times f)(a, a) = (f(a), f(a))$ , and  $f(a) = \bullet$ .
- ▶ In **Rel**, any surjective homomorphism  $G \xrightarrow{f} H$  of groups is a comonoid homomorphism. Preservation of comultiplication:  
LHS is  $g \sim (h, h^{-1}f(g))$ , RHS is  $g \sim (f(g'), f(g')^{-1}f(g))$ .
- ▶ In **FHilb**, any function  $\{d_i\} \xrightarrow{f} \{e_j\}$  between bases extends linearly to a comonoid homomorphism:  
 $d(f(d_i)) = f(d_i) \otimes f(d_i)$  and  $e(f(d_j)) = 1 = e(d_j)$ .

## Product of monoids

Can combine two (co)monoids to single one using braiding:



## Product of monoids

Can combine two (co)monoids to single one using braiding:



If braiding is symmetry: categorical product.

## Product of monoids

Can combine two (co)monoids to single one using braiding:



If braiding is symmetry: categorical product.

Examples:

- ▶ In **Set**, product comonoid on  $A, B$  is unique comonoid on  $A \times B$ .

## Product of monoids

Can combine two (co)monoids to single one using braiding:



If braiding is symmetry: categorical product.

Examples:

- ▶ In **Set**, product comonoid on  $A, B$  is unique comonoid on  $A \times B$ .
- ▶ In **Rel**, the product comonoid of groups  $G$  and  $H$  is comonoid of  $G \times H$  with multiplication  $(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2)$ .

## Product of monoids

Can combine two (co)monoids to single one using braiding:



If braiding is symmetry: categorical product.

Examples:

- ▶ In **Set**, product comonoid on  $A, B$  is unique comonoid on  $A \times B$ .
- ▶ In **Rel**, the product comonoid of groups  $G$  and  $H$  is comonoid of  $G \times H$  with multiplication  $(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2)$ .
- ▶ In **FHilb**, the product of comonoids on  $H$  and  $K$  that copy bases  $\{d_i\}$  and  $\{e_j\}$  is the comonoid copying basis  $\{d_i \otimes e_j\}$  of  $H \otimes K$ .

# Dagger

Monoidal dagger category has duality between monoids and comonoids:  $(A, d, e)$  is a comonoid if and only if  $(A, d^\dagger, e^\dagger)$  is a monoid.

# Dagger

Monoidal dagger category has duality between monoids and comonoids:  $(A, d, e)$  is a comonoid if and only if  $(A, d^\dagger, e^\dagger)$  is a monoid.

Example:

- ▶ In **Rel**: comultiplication  $g \sim (h, h^{-1}g)$  for group  $G$  turns into multiplication  $(g, h) \sim gh$ .



# Closure

Morphisms transform *input* into *output*.

But sometimes want to transform morphisms into morphisms.

# Closure

Morphisms transform *input* into *output*.

But sometimes want to transform morphisms into morphisms.

Can handle this using names and conames. E.g.:

$$\mathbf{FHilb}(H, K) = \{H \xrightarrow{f} K \mid f \text{ linear}\}$$

is vector space with pointwise operations  $(f + g)(x) = f(x) + g(x)$ ,  
Hilbert space with *trace inner product*  $\langle f | g \rangle = \text{Tr}(f^\dagger \circ g)$ .

To transform morphisms, encode them as vectors in function spaces.

# Matrices

One of most important features of matrices: they can be multiplied.

In other words, linear maps  $\mathbb{C}^n \rightarrow \mathbb{C}^n$  can be composed.

Using closure, can *internalize* this: the vector space  $\mathbb{M}_n$  of matrices is a monoid that lives in the same category as  $\mathbb{C}^n$ .

# Matrices

One of most important features of matrices: they can be multiplied.  
In other words, linear maps  $\mathbb{C}^n \rightarrow \mathbb{C}^n$  can be composed.

Using closure, can *internalize* this: the vector space  $\mathbb{M}_n$  of matrices is a monoid that lives in the same category as  $\mathbb{C}^n$ .

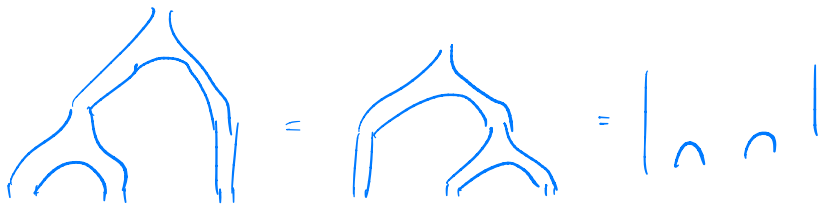
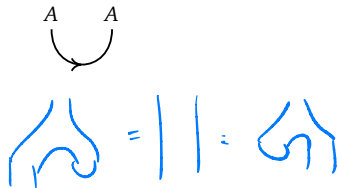
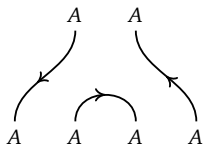
More generally, if an object  $A$  in a monoidal category has a dual  $A^*$ , then operators  $A \xrightarrow{f} A$  correspond bijectively to states  $I \xrightarrow{\lceil f \rceil} A^* \otimes A$ .  
Composition  $A \xrightarrow{g \circ f} A$  of operators transfers to states  $I \xrightarrow{\lceil g \circ f \rceil} A^* \otimes A$ :

$$\begin{array}{c} \curvearrowleft \\ \lceil g \rceil \\ \square \\ \curvearrowright \end{array} \quad \begin{array}{c} \curvearrowleft \\ \lceil f \rceil \\ \square \\ \curvearrowright \end{array} = \begin{array}{c} \downarrow \quad \uparrow \\ \lceil g \circ f \rceil \\ \square \end{array}$$

So  $A^* \otimes A$  canonically becomes monoid.

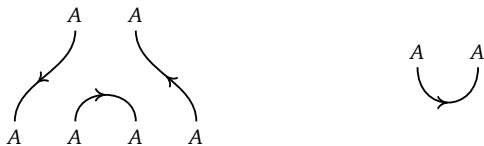
# Pair of pants

If  $A \dashv A^*$  in monoidal category, then  $A^* \otimes A$  is a monoid:

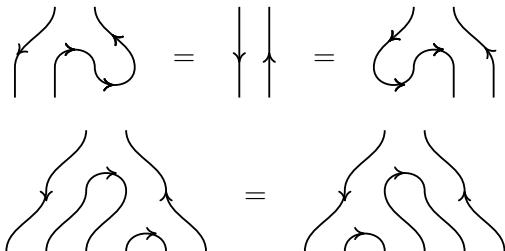


## Pair of pants

If  $A \dashv A^*$  in monoidal category, then  $A^* \otimes A$  is a monoid:



**Proof.**



# Matrix algebras

Example: pair of pants on  $\mathbb{C}^n$  in **FHilb** is the algebra  $\mathbb{M}_n$  of  $n$ -by- $n$  matrices under matrix multiplication.

## Matrix algebras

Example: pair of pants on  $\mathbb{C}^n$  in **FHilb** is the algebra  $\mathbb{M}_n$  of  $n$ -by- $n$  matrices under matrix multiplication.

Proof: Fix basis  $\{|i\rangle\}$  for  $A = \mathbb{C}^n$ , so  $A^* \otimes A$  has basis  $\{\langle j| \otimes |i\rangle\}$ .



# Matrix algebras

Example: pair of pants on  $\mathbb{C}^n$  in **FHilb** is the algebra  $\mathbb{M}_n$  of  $n$ -by- $n$  matrices under matrix multiplication.

Proof: Fix basis  $\{|i\rangle\}$  for  $A = \mathbb{C}^n$ , so  $A^* \otimes A$  has basis  $\{\langle j| \otimes |i\rangle\}$ .

Define map  $A^* \otimes A \rightarrow \mathbb{M}_n$  by mapping  $\langle j| \otimes |i\rangle$  to the matrix  $e_{ij}$  with a single entry 1 on row  $i$  and column  $j$  and zeroes elsewhere.

# Matrix algebras

Example: pair of pants on  $\mathbb{C}^n$  in **FHilb** is the algebra  $\mathbb{M}_n$  of  $n$ -by- $n$  matrices under matrix multiplication.

Proof: Fix basis  $\{|i\rangle\}$  for  $A = \mathbb{C}^n$ , so  $A^* \otimes A$  has basis  $\{\langle j| \otimes |i\rangle\}$ .

Define map  $A^* \otimes A \rightarrow \mathbb{M}_n$  by mapping  $\langle j| \otimes |i\rangle$  to the matrix  $e_{ij}$  with a single entry 1 on row  $i$  and column  $j$  and zeroes elsewhere.

This bijection respects multiplication:

$$\begin{array}{c} \curvearrowright \quad \curvearrowleft \\ i \quad j \quad k \quad l \end{array} = \begin{bmatrix} \langle i| \otimes |l\rangle & \text{if } j = k \\ 0 & \text{if } j \neq k \end{bmatrix} \mapsto \begin{bmatrix} e_{il} & \text{if } j = k \\ 0 & \text{if } j \neq k \end{bmatrix} = e_{ij}e_{kl}$$

## Pair of pants are universal

Cayley: any group  $G$  is a subgroup of a symmetric one.

## Pair of pants are universal

Cayley: any group  $G$  is a subgroup of a symmetric one.

*Symmetric group*  $\text{Sym}(A)$ : bijections  $A \rightarrow A$  under composition.

Embedding  $R: G \rightarrow \text{Sym}(G)$  is *regular representation*  $g \mapsto R_g$ .

$$R_g(h) = g \cdot h$$

## Pair of pants are universal

Cayley: any group  $G$  is a subgroup of a symmetric one.

*Symmetric group*  $\text{Sym}(A)$ : bijections  $A \rightarrow A$  under composition.

Embedding  $R: G \rightarrow \text{Sym}(G)$  is *regular representation*  $g \mapsto R_g$ .

$$R_g(h) = g \cdot h$$

Already works for monoids: any  $M$  is submonoid of  $\mathbf{Set}(M, M)$ .

## Pair of pants are universal

Cayley: any group  $G$  is a subgroup of a symmetric one.

*Symmetric group*  $\text{Sym}(A)$ : bijections  $A \rightarrow A$  under composition.

Embedding  $R: G \rightarrow \text{Sym}(G)$  is *regular representation*  $g \mapsto R_g$ .

$$R_g(h) = g \cdot h$$

Already works for monoids: any  $M$  is submonoid of  $\mathbf{Set}(M, M)$ .

Closure: instead of injective homomorphism  $M \xrightarrow{R} \mathbf{Set}(M, M)$ , consider relation  $M \rightarrow M^* \times M$  (latter with pair of pants).

## Pair of pants are universal

Cayley: any group  $G$  is a subgroup of a symmetric one.

Symmetric group  $\text{Sym}(A)$ : bijections  $A \rightarrow A$  under composition.

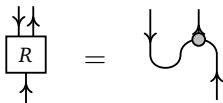
Embedding  $R: G \rightarrow \text{Sym}(G)$  is *regular representation*  $g \mapsto R_g$ .

$$R_g(h) = g \cdot h$$

Already works for monoids: any  $M$  is submonoid of  $\mathbf{Set}(M, M)$ .

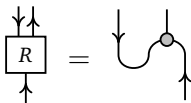
Closure: instead of injective homomorphism  $M \xrightarrow{R} \mathbf{Set}(M, M)$ , consider relation  $M \rightarrow M^* \times M$  (latter with pair of pants).

Abstract embedding of  $(M, \circ, \circ, \circ)$  into  $M \dashv M^*$ :



## Cayley's theorem

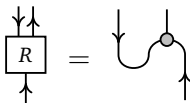
Any monoid  $(A, \cdot, \circ)$  in a monoidal category with  $A \dashv A^*$  has monoid homomorphism to  $(A^* \otimes A, /, \backslash, \cup)$  with right inverse.



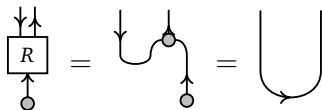


## Cayley's theorem

Any monoid  $(A, \cdot, \circ)$  in a monoidal category with  $A \dashv A^*$  has monoid homomorphism to  $(A^* \otimes A, \wedge, \vee)$  with right inverse.


$$\boxed{R} = \text{dot with two outputs and one input}$$

**Proof.**  $R$  preserves units:


$$\boxed{R} \text{ applied to unit} = \text{dot with two outputs and one input} = \text{U-shaped wire}$$

## Cayley's theorem

Any monoid  $(A, \otimes, \oplus)$  in a monoidal category with  $A \dashv A^*$  has monoid homomorphism to  $(A^* \otimes A, \wedge, \vee)$  with right inverse.

$$\boxed{R} = \text{wavy line with dot}$$

**Proof.**  $R$  preserves units:

$$\boxed{R} = \text{wavy line with dot} = \text{U-shaped line}$$

$R$  preserves multiplication:

$$\boxed{R} = \text{wavy line with dot} = \text{wavy line with dot} = \text{wavy line with dot} = \boxed{R} \boxed{R}$$

*associativity*

*R*

Finally,  $R$  has a right inverse  $\varphi$ .

## Uniform deleting

Counit  $A \xrightarrow{e} I$  tells us we can 'delete'  $A$  if we want to.

What does it mean to have deletion *systematically* on every object?

## Uniform deleting

Counit  $A \xrightarrow{e} I$  tells us we can ‘delete’  $A$  if we want to.

What does it mean to have deletion *systematically* on every object?

A monoidal category has **uniform deleting** if there is a natural transformation  $A \xrightarrow{e_A} I$  with  $e_I = \text{id}_I$ , such that:

$$\begin{array}{ccc} & A \otimes B & \\ e_A \otimes e_B \swarrow & & \searrow e_{A \otimes B} \\ I \otimes I & \xrightarrow{\lambda_I} & I \end{array}$$

## Uniform deleting

Counit  $A \xrightarrow{e} I$  tells us we can ‘delete’  $A$  if we want to.

What does it mean to have deletion *systematically* on every object?

A monoidal category has **uniform deleting** if there is a natural transformation  $A \xrightarrow{e_A} I$  with  $e_I = \text{id}_I$ , such that:

$$\begin{array}{ccc} & A \otimes B & \\ e_A \otimes e_B \swarrow & & \searrow e_{A \otimes B} \\ I \otimes I & \xrightarrow{\lambda_I} & I \end{array}$$

Uniform deleting possible if and only if  $I$  is terminal.

# Uniform deleting

Counit  $A \xrightarrow{e} I$  tells us we can 'delete'  $A$  if we want to.

What does it mean to have deletion *systematically* on every object?

A monoidal category has **uniform deleting** if there is a natural transformation  $A \xrightarrow{e_A} I$  with  $e_I = \text{id}_I$ , such that:

$$\begin{array}{ccc} A & \xrightarrow{e_A} & I \\ f \downarrow & & \parallel \\ B & \xrightarrow{e_B} & I \end{array}$$

$$\begin{array}{ccc} & A \otimes B & \\ e_A \otimes e_B \swarrow & & \searrow e_{A \otimes B} \\ I \otimes I & \xrightarrow{\lambda_I} & I \end{array}$$

$$\begin{array}{ccc} A & \xrightarrow{e_A} & I \\ f \downarrow & & \parallel \\ I & \xrightarrow{e_I} & I \end{array}$$

Uniform deleting possible if and only if  $I$  is terminal.

**Proof.** Uniform deleting gives a morphism  $A \xrightarrow{e_A} I$  for each object  $A$ . Naturality and  $e_I = \text{id}_I$  then show any morphism  $A \xrightarrow{f} I$  equals  $e_A$ . Conversely, if  $I$  is terminal, choose  $e_A : A \rightarrow I$  uniquely. □

## No-deleting theorem

A **preorder** is a category that has at most one morphism  $A \rightarrow B$  for any pair of objects  $A, B$ .

Preorders are degenerate, with only process of each type.

## No-deleting theorem

A **preorder** is a category that has at most one morphism  $A \rightarrow B$  for any pair of objects  $A, B$ .

Preorders are degenerate, with only process of each type.

**Theorem:** if a monoidal category with duals has uniform deleting, then it is a preorder.



## No-deleting theorem

A **preorder** is a category that has at most one morphism  $A \rightarrow B$  for any pair of objects  $A, B$ .

Preorders are degenerate, with only process of each type.

**Theorem:** if a monoidal category with duals has uniform deleting, then it is a preorder.

**Proof.** Let  $A \xrightarrow{f, g} B$  be morphisms. Naturality of  $e$  gives:

$$\begin{array}{ccc} A \otimes B^* & \xrightarrow{e_{A \otimes B^*}} & I \\ \lrcorner f \lrcorner \downarrow & & \downarrow \text{id}_I \\ I & \xrightarrow{e_I = \text{id}_I} & I \end{array}$$

So  $\lrcorner f \lrcorner = e_{A \otimes B^*}$ , and similarly  $\lrcorner g \lrcorner = e_{A \otimes B^*}$ . Hence  $f = g$ . □

## Uniform copying

Question: what does it mean to *copy* objects *systematically*?

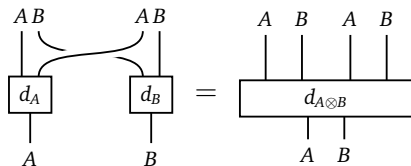
Answer: copying must respect composition, tensor products.

## Uniform copying

Question: what does it mean to *copy* objects *systematically*?

Answer: copying must respect composition, tensor products.

A braided monoidal category has **uniform copying** if there is a natural transformation  $A \xrightarrow{d_A} A \otimes A$  with  $d_I = \rho_I$ , satisfying cocommutativity and coassociativity, and:

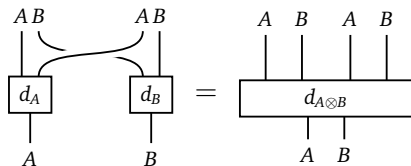


## Uniform copying

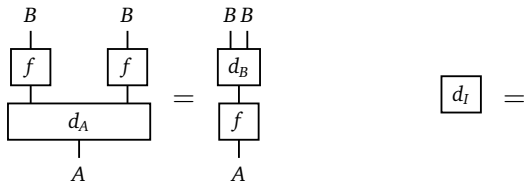
Question: what does it mean to *copy* objects *systematically*?

Answer: copying must respect composition, tensor products.

A braided monoidal category has **uniform copying** if there is a natural transformation  $A \xrightarrow{d_A} A \otimes A$  with  $d_I = \rho_I$ , satisfying cocommutativity and coassociativity, and:



Naturality and  $d_I = \rho_I$  look like this for arbitrary  $A \xrightarrow{f} B$ :



## Copying states

Example: **Set** has uniform copying maps  $a \mapsto (a, a)$ :

$$d_1(\bullet) = (\bullet, \bullet) = \rho_1(\bullet)$$

both maps  $A \times B \rightarrow A \times B \times A \times B$  are  $(a, b) \mapsto (a, b, a, b)$

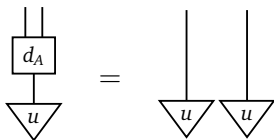
## Copying states

Example: **Set** has uniform copying maps  $a \mapsto (a, a)$ :

$$d_1(\bullet) = (\bullet, \bullet) = \rho_1(\bullet)$$

both maps  $A \times B \rightarrow A \times B \times A \times B$  are  $(a, b) \mapsto (a, b, a, b)$

In a braided monoidal category, a state  $I \xrightarrow{u} A$  is **copyable** with respect to a map  $A \xrightarrow{d_A} A \otimes A$  when:



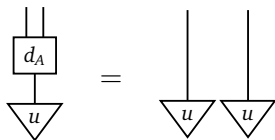
## Copying states

Example: **Set** has uniform copying maps  $a \mapsto (a, a)$ :

$$d_1(\bullet) = (\bullet, \bullet) = \rho_1(\bullet)$$

both maps  $A \times B \rightarrow A \times B \times A \times B$  are  $(a, b) \mapsto (a, b, a, b)$

In a braided monoidal category, a state  $I \xrightarrow{u} A$  is **copyable** with respect to a map  $A \xrightarrow{d_A} A \otimes A$  when:



In braided monoidal category with uniform copying, any state is copyable.

## Copying states

Example: **Set** has uniform copying maps  $a \mapsto (a, a)$ :

$$d_1(\bullet) = (\bullet, \bullet) = \rho_1(\bullet)$$

both maps  $A \times B \rightarrow A \times B \times A \times B$  are  $(a, b) \mapsto (a, b, a, b)$

In a braided monoidal category, a state  $I \xrightarrow{u} A$  is **copyable** with respect to a map  $A \xrightarrow{d_A} A \otimes A$  when:

$$\begin{array}{c} \parallel \\ \square d_A \\ \downarrow \\ \triangle u \end{array} = \begin{array}{cc} \downarrow & \downarrow \\ \triangle u & \triangle u \end{array}$$

In braided monoidal category with uniform copying, any state is copyable.

**Proof.** If there is uniform copying, then, by naturality of the copying maps, we have  $d_A \circ u = (u \otimes u) \circ \rho_I$  for each state  $I \xrightarrow{u} A$ . □



## Duals vs copying

If a braided monoidal category with duals has uniform copying:

$$\begin{array}{c} A^* \quad A \\ \cup \end{array} \quad \begin{array}{c} A^* \quad A \\ \cup \end{array} = \begin{array}{c} A^* \quad A \quad A^* \quad A \\ \cup \quad \cup \\ \quad \cup \end{array}$$

## Duals vs copying

If a braided monoidal category with duals has uniform copying:

$$\begin{array}{c} A^* \quad A \\ \frown \\ \phantom{A^*} \end{array} \quad \begin{array}{c} A^* \quad A \\ \frown \\ \phantom{A^*} \end{array} = \begin{array}{c} A^* \quad A \quad A^* \quad A \\ \bigcup \\ \text{\textcircled{0}} \\ \bigcup \end{array}$$

**Proof.** First, consider the following equality (\*):

$$\begin{array}{c} A^* \quad A \\ \frown \\ \phantom{A^*} \end{array} \quad \begin{array}{c} A^* \quad A \\ \frown \\ \phantom{A^*} \end{array} = \begin{array}{c} A^* \quad A \\ \frown \\ \phantom{A^*} \end{array} \quad \boxed{d_I} \quad \begin{array}{c} A^* \quad A \\ \frown \\ \phantom{A^*} \end{array} = \begin{array}{c} \text{---} \text{---} \text{---} \text{---} \\ \boxed{d_{A^* \otimes A}} \\ \text{---} \text{---} \end{array} = \begin{array}{c} \text{---} \text{---} \\ \boxed{d_{A^*}} \quad \boxed{d_A} \\ \text{---} \text{---} \end{array}$$

# Duals vs copying

If a braided monoidal category with duals has uniform copying:

$$\begin{array}{c} A^* \quad A \end{array} \quad \begin{array}{c} A^* \quad A \end{array} = \begin{array}{c} A^* \quad A \quad A^* \quad A \\ \text{U} \end{array}$$

**Proof.** First, consider the following equality (\*):

$$\begin{array}{c} A^* \quad A \end{array} \quad \begin{array}{c} A^* \quad A \end{array} = \begin{array}{c} A^* \quad A \quad A^* \quad A \\ \text{d}_I \end{array} = \begin{array}{c} \text{d}_{A^* \otimes A} \end{array} = \begin{array}{c} \text{d}_{A^*} \quad \text{d}_A \end{array}$$

Then:

$$\begin{array}{c} A^* \quad A \end{array} \quad \begin{array}{c} A^* \quad A \end{array} \stackrel{(*)}{=} \begin{array}{c} \text{d}_{A^*} \quad \text{d}_A \end{array} \stackrel{(*)}{=} \begin{array}{c} \text{d}_{A^*} \quad \text{d}_A \end{array} \stackrel{(*)}{=} \begin{array}{c} A^* \quad A \quad A^* \quad A \\ \text{U} \end{array}$$

## Duals vs copying

In a braided monoidal category with duals and uniform copying:

$$\begin{array}{c} A & A \\ \diagdown & / \\ & \diagup & \diagdown \\ A & A \end{array} = \begin{array}{c} A & A \\ | & | \\ A & A \end{array}$$

## Duals vs copying

In a braided monoidal category with duals and uniform copying:

$$\begin{array}{c} A & A \\ \diagdown & / \\ & \\ / & \diagdown \\ A & A \end{array} = \begin{array}{c} A & A \\ | & | \\ A & A \end{array}$$

**Proof.**

$$\begin{array}{c} A & A \\ \diagdown & / \\ & \\ / & \diagdown \\ A & A \end{array} = \begin{array}{c} \text{---} \\ \diagdown & / \\ \text{---} \\ / & \diagdown \\ \text{---} & \text{---} \\ | & | \\ A & A \end{array} = \begin{array}{c} \text{---} \\ \diagdown & / \\ \text{---} \\ / & \diagdown \\ \text{---} & \text{---} \\ | & | \\ A & A \end{array} \stackrel{\text{iso}}{=} \begin{array}{c} A & A \\ | & | \\ A & A \end{array}$$

## No-cloning theorem

If a braided monoidal category with duals has uniform copying, every endomorphism is a multiple of the identity,  $f = \text{Tr}(f) \bullet \text{id}$ :

The diagram shows an equality between two expressions. On the left, a vertical line with a square box labeled  $f$  in the middle. On the right, a vertical line with a square box labeled  $f$  on the left side, and a loop on the right side that starts from the top of the line, goes up, loops around, and goes back down to the bottom of the line. An equals sign is placed between the two expressions.

# No-cloning theorem

If a braided monoidal category with duals has uniform copying, every endomorphism is a multiple of the identity,  $f = \text{Tr}(f) \bullet \text{id}$ :

$$\begin{array}{c} \square f \\ | \end{array} = \begin{array}{c} | \\ \square f \\ | \end{array}$$

**Proof.**

$$\begin{array}{c} \square f \\ | \end{array} = \begin{array}{c} A \\ | \\ \square f \\ | \\ A \end{array} \stackrel{\text{iso}}{=} \begin{array}{c} \square f \\ | \\ A \end{array} = \begin{array}{c} | \\ \square f \\ | \end{array} = \begin{array}{c} \square f \\ | \end{array}$$

*(Handwritten blue annotations show the equivalence between the last two diagrams in the proof sequence.)*

## Products

The following are equivalent for a symmetric monoidal category:

- ▶ tensor products are products and the tensor unit is terminal
- ▶ it has uniform copying and deleting, satisfying counitality



## Products

The following are equivalent for a symmetric monoidal category:

- ▶ tensor products are products and the tensor unit is terminal
- ▶ it has uniform copying and deleting, satisfying counitality

**Proof.** If cartesian, unique  $A \xrightarrow{e_A} I$  and  $d_A = \begin{pmatrix} \text{id}_A \\ \text{id}_A \end{pmatrix}$  provide uniform copying and deleting.

## Products

The following are equivalent for a symmetric monoidal category:

- ▶ tensor products are products and the tensor unit is terminal
- ▶ it has uniform copying and deleting, satisfying counitality

**Proof.** If cartesian, unique  $A \xrightarrow{e_A} I$  and  $d_A = \begin{pmatrix} \text{id}_A \\ \text{id}_A \end{pmatrix}$  provide uniform copying and deleting.

For converse, need to prove  $A \otimes B$  is product of  $A, B$ .

For  $C \xrightarrow{f} A$  and  $C \xrightarrow{g} B$ , define

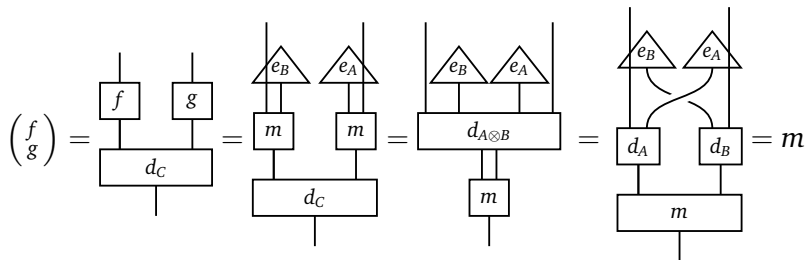
$$\begin{pmatrix} f \\ g \end{pmatrix} = (f \otimes g) \circ d$$

$$p_A = \rho_A \circ (\text{id}_A \otimes e_B): A \otimes B \rightarrow A$$

$$p_B = \lambda_B \circ (e_A \otimes \text{id}_B): A \otimes B \rightarrow B$$

**Proof.** Suppose  $C \xrightarrow{m} A \otimes B$  satisfies  $p_A \circ m = f$  and  $p_B \circ m = g$ .

**Proof.** Suppose  $C \xrightarrow{m} A \otimes B$  satisfies  $p_A \circ m = f$  and  $p_B \circ m = g$ . Then:



Hence mediating morphisms, if they exist, are unique.

**Proof.** Suppose  $C \xrightarrow{m} A \otimes B$  satisfies  $p_A \circ m = f$  and  $p_B \circ m = g$ . Then:

$$\left( \begin{array}{c} f \\ g \end{array} \right) = \begin{array}{c} \boxed{f} \quad \boxed{g} \\ | \quad | \\ \boxed{d_C} \\ | \end{array} = \begin{array}{c} \triangle_{e_B} \quad \triangle_{e_A} \\ | \quad | \\ \boxed{m} \quad \boxed{m} \\ | \quad | \\ \boxed{d_C} \\ | \end{array} = \begin{array}{c} \triangle_{e_B} \quad \triangle_{e_A} \\ | \quad | \\ \boxed{d_{A \otimes B}} \\ | \\ \boxed{m} \\ | \end{array} = \begin{array}{c} \triangle_{e_B} \quad \triangle_{e_A} \\ | \quad | \\ \boxed{d_A} \quad \boxed{d_B} \\ | \quad | \\ \boxed{m} \\ | \end{array} = m$$

Hence mediating morphisms, if they exist, are unique.

Finally, we show the universal morphism has the right properties:

$$p_B \circ \left( \begin{array}{c} f \\ g \end{array} \right) = \begin{array}{c} \triangle_{e_A} \\ | \\ \boxed{f} \quad \boxed{g} \\ | \quad | \\ \boxed{d_C} \\ | \end{array} = \begin{array}{c} \triangle_{e_C} \\ | \\ \boxed{d_C} \\ | \\ \boxed{g} \\ | \end{array} = \begin{array}{c} \boxed{g} \\ | \end{array}$$

A similar result holds for  $g$ .

# Summary

- ▶ Monoids: multiplication on states
- ▶ Comonoids: 'copying' of states
- ▶ Closure: operators form monoids
- ▶ Cloning: no-cloning and no-deleting
- ▶ Products: characterize when tensor product is product

Next week: interaction between monoids and comonoids