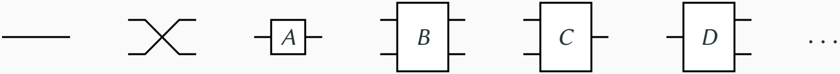
Diagrammatic Reasoning with Control as a Constructor, Applications to Quantum Circuits

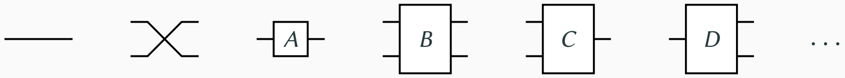
14th April 2026 - FoSSaCS 2026

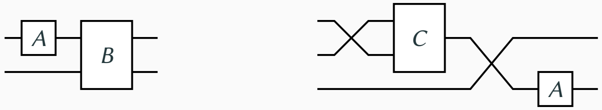
Noé Delorme and Simon Perdrix
Université de Lorraine, CNRS, INRIA, LORIA, Nancy, France

Circuits as generators and compositions

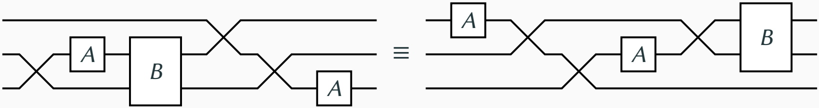


Circuits as generators and compositions



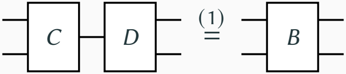


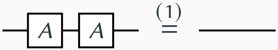
Diagrammatic equivalence



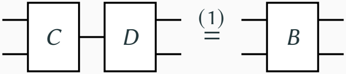
$\equiv$: diagrammatic equivalence

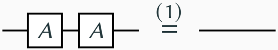
Circuit rewriting

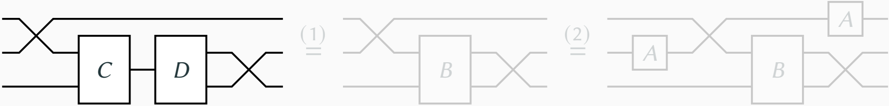


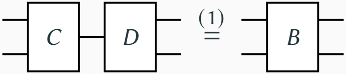


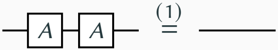
Circuit rewriting

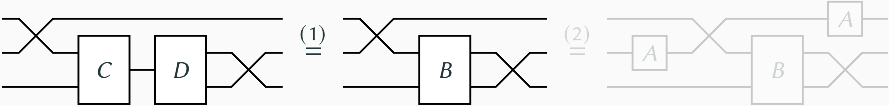


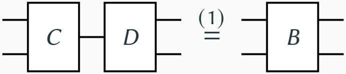


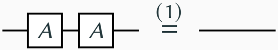


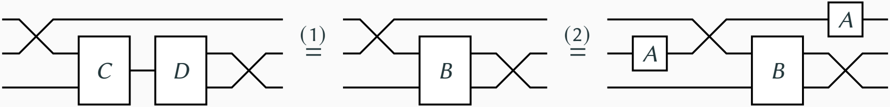

C
D
(1)
B


A
A
(1)


C
D
(1)
B
(2)
A
A
B


C
D
(1)
B

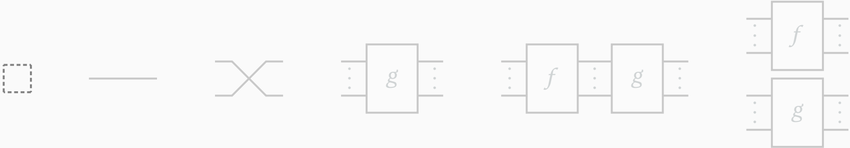

A
A
(1)


C
D
(1)
B
(2)
A
B
A

PROP formalism

$$\frac{}{\mathrm{id}_0 : 0 \to 0} \qquad \frac{}{\mathrm{id}_1 : 1 \to 1} \qquad \frac{}{\sigma : 2 \to 2} \qquad \frac{g \in \Sigma}{g : \mathrm{dom}(g) \to \mathrm{cod}(g)}$$

$$\frac{f : n \to p \quad g : p \to m}{f \mathbin{;} g : n \to m} \qquad \frac{f : n \to m \quad g : p \to q}{f \otimes g : n + p \to m + q}$$



Σ : a set of generators

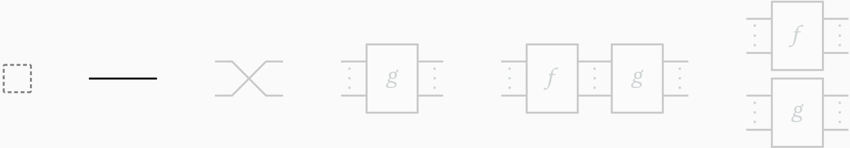
$;$: the sequential composition

$\otimes$: the parallel composition

PROP formalism

$$\frac{}{\mathrm{id}_0 : 0 \to 0} \qquad \frac{}{\mathrm{id}_1 : 1 \to 1} \qquad \frac{}{\sigma : 2 \to 2} \qquad \frac{g \in \Sigma}{g : \mathrm{dom}(g) \to \mathrm{cod}(g)}$$

$$\frac{f : n \to p \quad g : p \to m}{f \,;\, g : n \to m} \qquad \frac{f : n \to m \quad g : p \to q}{f \otimes g : n + p \to m + q}$$



Σ : a set of generators

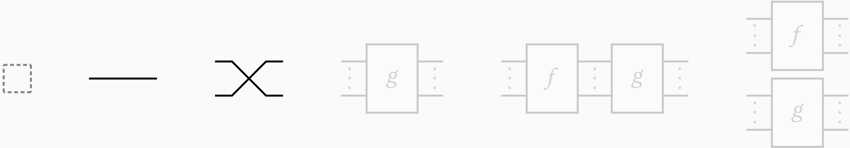
$;$: the sequential composition

$\otimes$: the parallel composition

PROP formalism

$$\frac{}{\mathrm{id}_0 : 0 \to 0} \qquad \frac{}{\mathrm{id}_1 : 1 \to 1} \qquad \frac{}{\sigma : 2 \to 2} \qquad \frac{g \in \Sigma}{g : \mathrm{dom}(g) \to \mathrm{cod}(g)}$$

$$\frac{f : n \to p \quad g : p \to m}{f \fatsemi g : n \to m} \qquad \frac{f : n \to m \quad g : p \to q}{f \otimes g : n + p \to m + q}$$



Σ : a set of generators

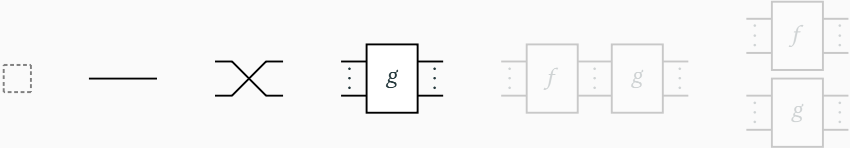
$\fatsemi$: the sequential composition

$\otimes$: the parallel composition

PROP formalism

$$\frac{}{\mathrm{id}_0 : 0 \to 0} \qquad \frac{}{\mathrm{id}_1 : 1 \to 1} \qquad \frac{}{\sigma : 2 \to 2} \qquad \frac{g \in \Sigma}{g : \mathrm{dom}(g) \to \mathrm{cod}(g)}$$

$$\frac{f : n \to p \quad g : p \to m}{f \fatsemi g : n \to m} \qquad \frac{f : n \to m \quad g : p \to q}{f \otimes g : n + p \to m + q}$$



Σ : a set of generators

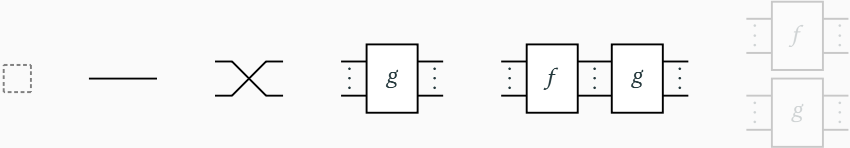
$\fatsemi$: the sequential composition

$\otimes$: the parallel composition

PROP formalism

$$\frac{}{\mathrm{id}_0 : 0 \to 0} \qquad \frac{}{\mathrm{id}_1 : 1 \to 1} \qquad \frac{}{\sigma : 2 \to 2} \qquad \frac{g \in \Sigma}{g : \mathrm{dom}(g) \to \mathrm{cod}(g)}$$

$$\frac{f : n \to p \quad g : p \to m}{f \mathbin{;} g : n \to m} \qquad \frac{f : n \to m \quad g : p \to q}{f \otimes g : n + p \to m + q}$$



Σ : a set of generators

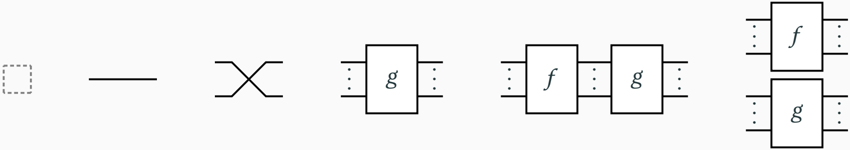
$\mathbin{;}$: the sequential composition

$\otimes$: the parallel composition

PROP formalism

$$\frac{}{\mathrm{id}_0 : 0 \to 0} \qquad \frac{}{\mathrm{id}_1 : 1 \to 1} \qquad \frac{}{\sigma : 2 \to 2} \qquad \frac{g \in \Sigma}{g : \mathrm{dom}(g) \to \mathrm{cod}(g)}$$

$$\frac{f : n \to p \quad g : p \to m}{f \,;\, g : n \to m} \qquad \frac{f : n \to m \quad g : p \to q}{f \otimes g : n + p \to m + q}$$



Σ : a set of generators

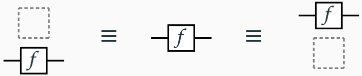
$;$: the sequential composition

$\otimes$: the parallel composition

PROP formalism

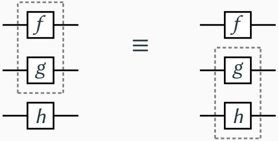
$$\sigma \fatsemi \sigma \equiv \mathrm{id}_1 \otimes \mathrm{id}_1$$

$$\mathrm{id}_0 \otimes f \equiv f \equiv f \otimes \mathrm{id}_0$$

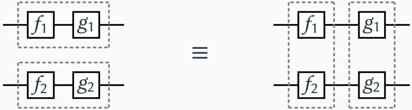


$$(f \fatsemi g) \fatsemi h \equiv f \fatsemi (g \fatsemi g)$$

$$(f \otimes g) \otimes h \equiv f \otimes (g \otimes h)$$



$$(f_1 \fatsemi g_2) \otimes (f_2 \fatsemi g_2) \equiv (f_1 \otimes f_2) \fatsemi (g_1 \otimes g_2)$$



$\ldots$

PROP formalism

$$\frac{f \equiv g}{\mathbf{P}/\mathcal{R} \vdash f = g} \qquad \frac{(L = R) \in \mathcal{R}}{\mathbf{P}/\mathcal{R} \vdash L = R}$$

$$\frac{\mathbf{P}/\mathcal{R} \vdash f = g}{\mathbf{P}/\mathcal{R} \vdash h \fatsemi f = h \fatsemi g} \qquad \frac{\mathbf{P}/\mathcal{R} \vdash f = g}{\mathbf{P}/\mathcal{R} \vdash f \fatsemi h = g \fatsemi h}$$

$$\frac{\mathbf{P}/\mathcal{R} \vdash f = g}{\mathbf{P}/\mathcal{R} \vdash h \otimes f = h \otimes g} \qquad \frac{\mathbf{P}/\mathcal{R} \vdash f = g}{\mathbf{P}/\mathcal{R} \vdash f \otimes h = g \otimes h}$$

$\equiv$: diagrammatic equivalence

$\mathbf{P}$: a PROP

$\mathcal{R}$: a set of rewrite equations

$\mathbf{P}/\mathcal{R} \vdash \cdot = \cdot$: the equivalence relation

PROP formalism

$$\frac{f \equiv g}{\mathbf{P}/\mathcal{R} \vdash f = g} \qquad \frac{(L = R) \in \mathcal{R}}{\mathbf{P}/\mathcal{R} \vdash L = R}$$

$$\frac{\mathbf{P}/\mathcal{R} \vdash f = g}{\mathbf{P}/\mathcal{R} \vdash h \,⨟\, f = h \,⨟\, g} \qquad \frac{\mathbf{P}/\mathcal{R} \vdash f = g}{\mathbf{P}/\mathcal{R} \vdash f \,⨟\, h = g \,⨟\, h}$$

$$\frac{\mathbf{P}/\mathcal{R} \vdash f = g}{\mathbf{P}/\mathcal{R} \vdash h \otimes f = h \otimes g} \qquad \frac{\mathbf{P}/\mathcal{R} \vdash f = g}{\mathbf{P}/\mathcal{R} \vdash f \otimes h = g \otimes h}$$

$\equiv$: diagrammatic equivalence

$\mathbf{P}$: a PROP

$\mathcal{R}$: a set of rewrite equations

$\mathbf{P}/\mathcal{R} \vdash \cdot = \cdot$: the equivalence relation

PROP formalism

$$\frac{f \equiv g}{\mathbf{P}/\mathcal{R} \vdash f = g} \qquad \frac{(L = R) \in \mathcal{R}}{\mathbf{P}/\mathcal{R} \vdash L = R}$$

$$\frac{\mathbf{P}/\mathcal{R} \vdash f = g}{\mathbf{P}/\mathcal{R} \vdash h \,⨟\, f = h \,⨟\, g} \qquad \frac{\mathbf{P}/\mathcal{R} \vdash f = g}{\mathbf{P}/\mathcal{R} \vdash f \,⨟\, h = g \,⨟\, h}$$

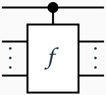
$$\frac{\mathbf{P}/\mathcal{R} \vdash f = g}{\mathbf{P}/\mathcal{R} \vdash h \otimes f = h \otimes g} \qquad \frac{\mathbf{P}/\mathcal{R} \vdash f = g}{\mathbf{P}/\mathcal{R} \vdash f \otimes h = g \otimes h}$$

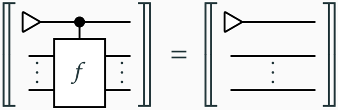
$\equiv$: diagrammatic equivalence

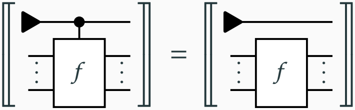
$\mathbf{P}$: a PROP

$\mathcal{R}$: a set of rewrite equations

$\mathbf{P}/\mathcal{R} \vdash \cdot = \cdot$: the equivalence relation





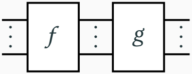


▷— : initialization of state 0

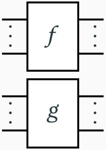
▶— : initialization of state 1

Controlled PROP

$$\frac{f : n \to p \quad g : p \to m}{f \fatsemi g : n \to m}$$



$$\frac{f : n \to m \quad g : p \to q}{f \otimes g : n + p \to m + q}$$

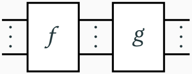


NEW!

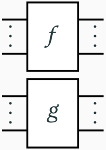
$$\frac{f : n \to n}{\mathrm{C}(f) : 1 + n \to 1 + n}$$

Controlled PROP

$$\frac{f : n \to p \quad g : p \to m}{f \mathbin{;} g : n \to m}$$

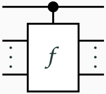


$$\frac{f : n \to m \quad g : p \to q}{f \otimes g : n + p \to m + q}$$



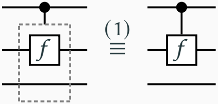
NEW!

$$\frac{f : n \to n}{\mathrm{C}(f) : 1 + n \to 1 + n}$$



Controlled PROP

NEW!

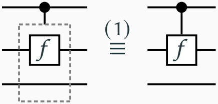


NEW!

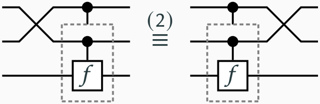
NEW!

Controlled PROP

NEW!

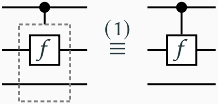


NEW!

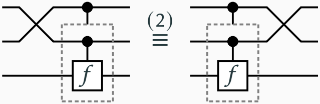


NEW!

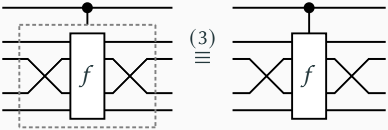
NEW!



NEW!



NEW!



Controlled PROP

Definition

A control functor maps any endocircuit $f : n \to n$ to the endocircuit $C(f) : (1+n) \to (1+n)$ while satisfying (1), (2), and (3).

Definition

A controlled PROP is a PROP equipped with a control functor.

Controlled PROP

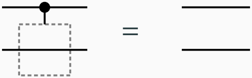
Definition

A control functor maps any endocircuit $f : n \to n$ to the endocircuit $C(f) : (1+n) \to (1+n)$ while satisfying (1), (2), and (3).

Definition

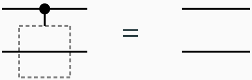
A controlled PROP is a PROP equipped with a control functor.

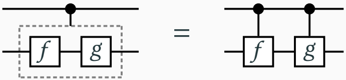
$$C(\mathrm{id}_1) = \mathrm{id}_1 \otimes \mathrm{id}_1 \qquad C(f \mathbin{;} g) = C(f) \mathbin{;} C(g)$$



Notice however that $C(f \otimes g) \neq C(f) \otimes C(g)$, instead we have

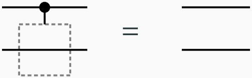
$$C(\mathrm{id}_1) = \mathrm{id}_1 \otimes \mathrm{id}_1 \qquad\qquad C(f \mathbin{;} g) = C(f) \mathbin{;} C(g)$$

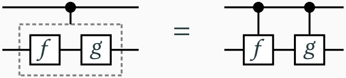




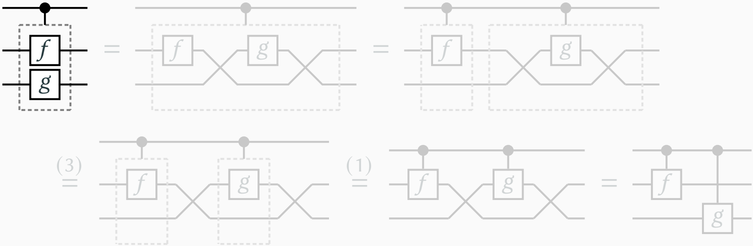
Notice however that $C(f \otimes g) \neq C(f) \otimes C(g)$, instead we have

$\mathrm{C}(\mathrm{id}_1) = \mathrm{id}_1 \otimes \mathrm{id}_1$ $\qquad$ $\mathrm{C}(f \fatsemi g) = \mathrm{C}(f) \fatsemi \mathrm{C}(g)$



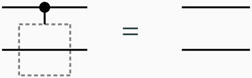


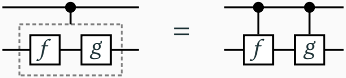
Notice however that $\mathrm{C}(f \otimes g) \neq \mathrm{C}(f) \otimes \mathrm{C}(g)$, instead we have



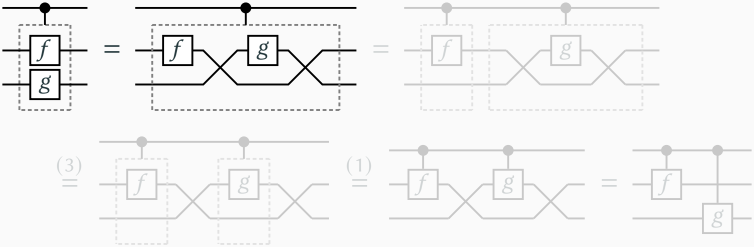
Controlled PROP

$\mathrm{C}(\mathrm{id}_1) \quad = \quad \mathrm{id}_1 \otimes \mathrm{id}_1$ $\qquad\qquad$ $\mathrm{C}(f \fatsemi g) \quad = \quad \mathrm{C}(f) \fatsemi \mathrm{C}(g)$



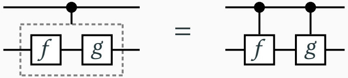


Notice however that $\mathrm{C}(f \otimes g) \neq \mathrm{C}(f) \otimes \mathrm{C}(g)$, instead we have

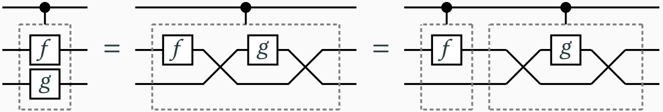


Controlled PROP

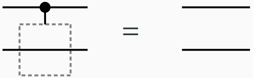
$C(\mathrm{id}_1) = \mathrm{id}_1 \otimes \mathrm{id}_1$ $\qquad$ $C(f \,⨾\, g) = C(f) \,⨾\, C(g)$



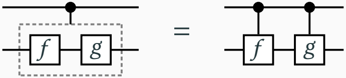
Notice however that $C(f \otimes g) \neq C(f) \otimes C(g)$, instead we have



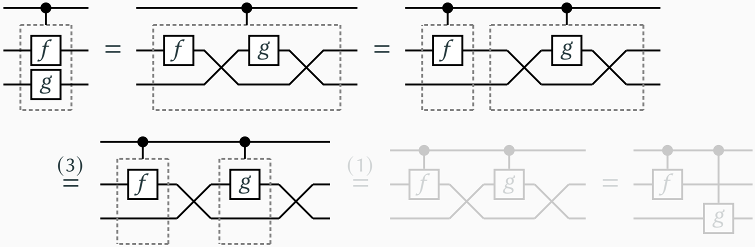
$$\mathrm{C}(\mathrm{id}_1) \quad = \quad \mathrm{id}_1 \otimes \mathrm{id}_1$$



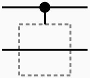
$$\mathrm{C}(f \fatsemi g) \quad = \quad \mathrm{C}(f) \fatsemi \mathrm{C}(g)$$

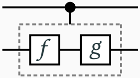
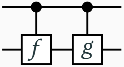


Notice however that $\mathrm{C}(f \otimes g) \neq \mathrm{C}(f) \otimes \mathrm{C}(g)$, instead we have

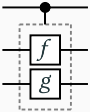
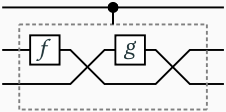
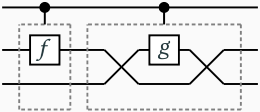


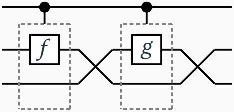
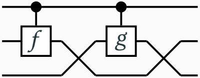
$$C(\mathrm{id}_1) = \mathrm{id}_1 \otimes \mathrm{id}_1 \qquad C(f \mathbin{;} g) = C(f) \mathbin{;} C(g)$$

 = 

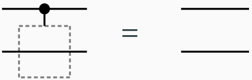
 = 

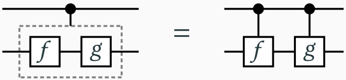
Notice however that $C(f \otimes g) \neq C(f) \otimes C(g)$, instead we have

 =  = 

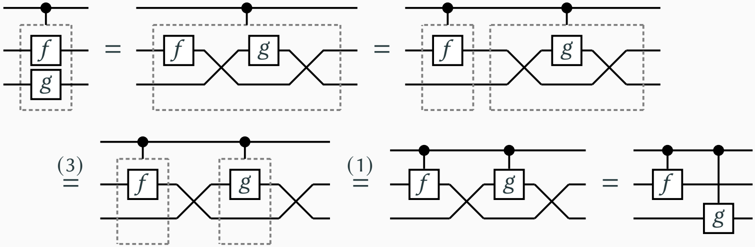
$\overset{(3)}{=}$  $\overset{(1)}{=}$  =

$$\mathrm{C}(\mathrm{id}_1) \quad = \quad \mathrm{id}_1 \otimes \mathrm{id}_1 \qquad\qquad \mathrm{C}(f \fatsemi g) \quad = \quad \mathrm{C}(f) \fatsemi \mathrm{C}(g)$$





Notice however that $\mathrm{C}(f \otimes g) \neq \mathrm{C}(f) \otimes \mathrm{C}(g)$, instead we have



Controlled PROP

$$\frac{\mathbf{P}/\mathcal{R} \vdash f = g}{\mathbf{P}/\mathcal{R} \vdash \mathrm{C}(f) = \mathrm{C}(g)}$$ **NEW!**

Example

Let **CNot** be the controlled PROP generated by with the following rewrite equations.

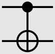
Then, is not a generator. It is the circuit C( ).

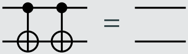
Moreover, the equations is derivable.

$$\frac{\mathbf{P}/\mathcal{R} \vdash f = g}{\mathbf{P}/\mathcal{R} \vdash \mathrm{C}(f) = \mathrm{C}(g)} \quad \textbf{NEW!}$$

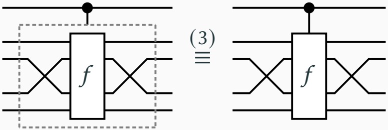
Example

Let **CNot** be the controlled PROP generated by  with the following rewrite equations.

Then,  is not a generator. It is the circuit C().

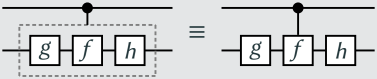
Moreover, the equations  is derivable.

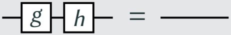
Conjugated PROP



Definition

A conjugated PROP is a controlled PROP such that

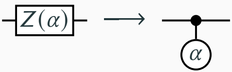


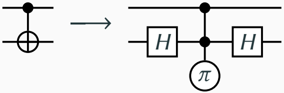
is satisfied whenever $\mathbf{P}/\mathcal{R} \vdash$  .

Applications to Quantum Circuits

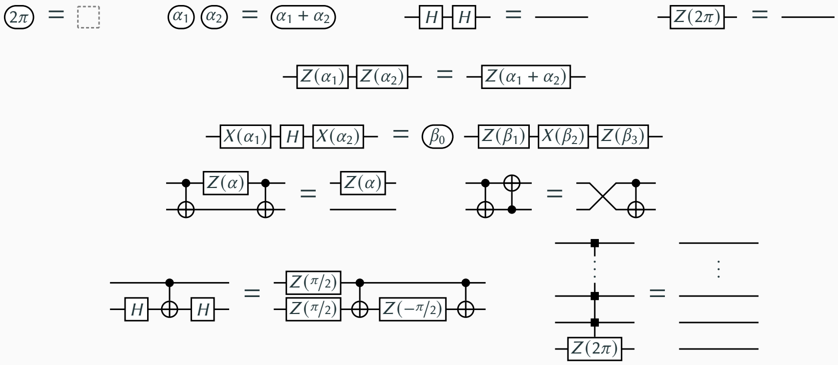
Quantum circuits

Quantum circuits





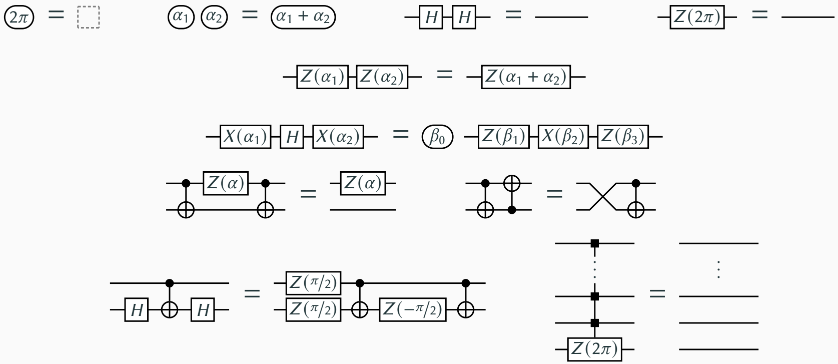
Quantum circuits



Theorem

This minimal set of rewrite equations is complete.

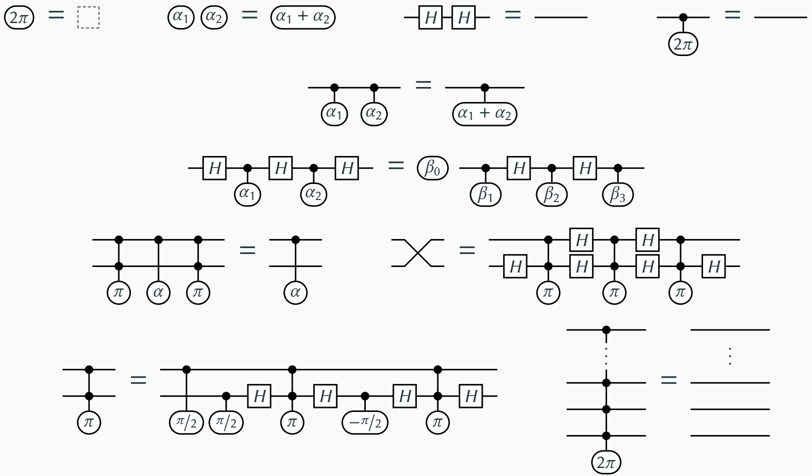
Quantum circuits



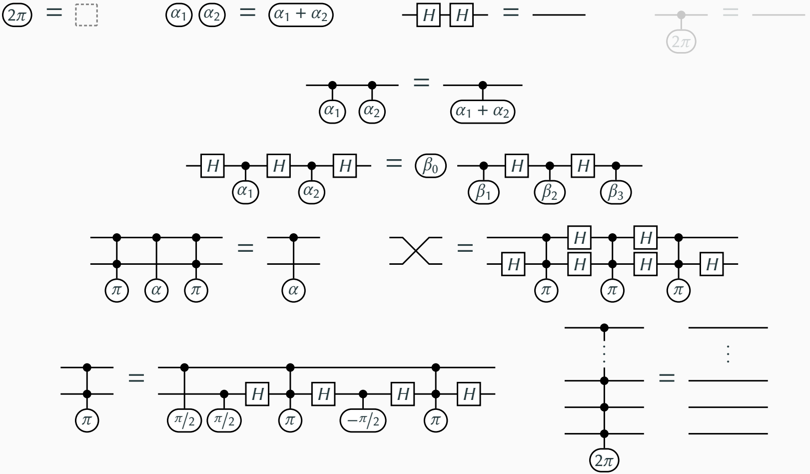
Theorem

This minimal set of rewrite equations is complete.

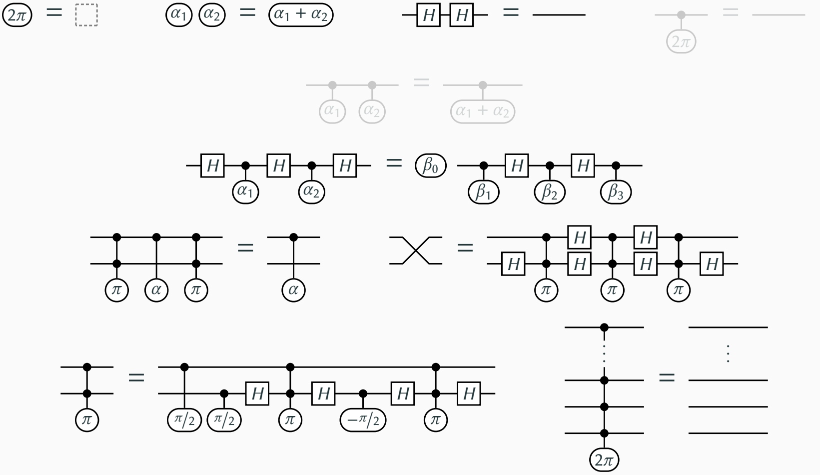
Quantum circuits



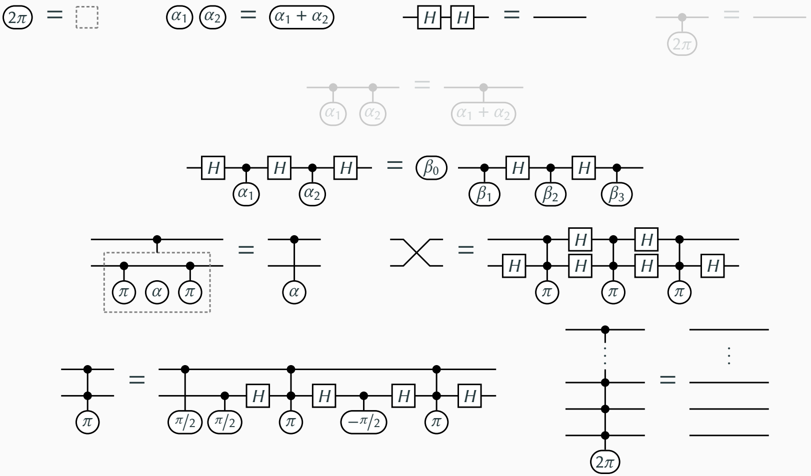
Quantum circuits



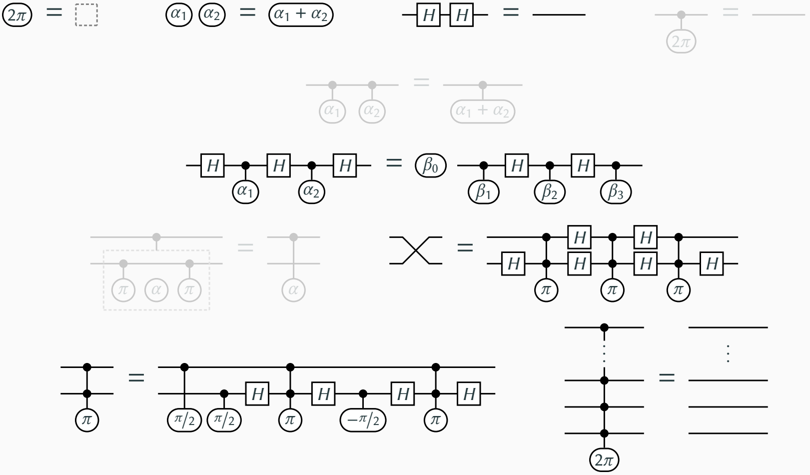
Quantum circuits



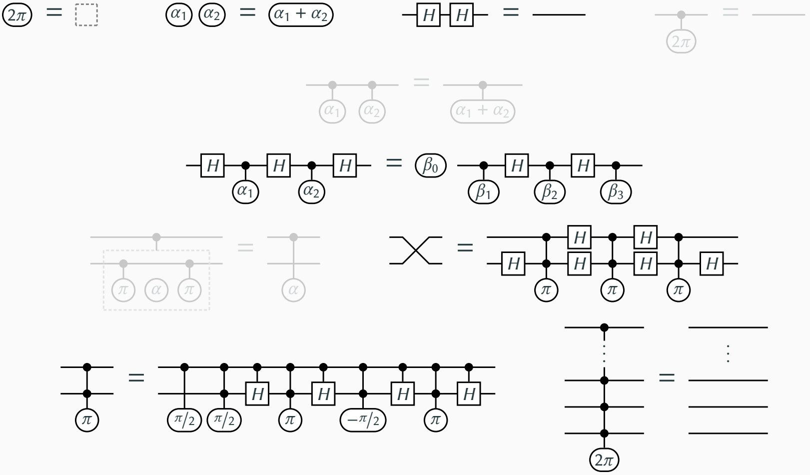
Quantum circuits



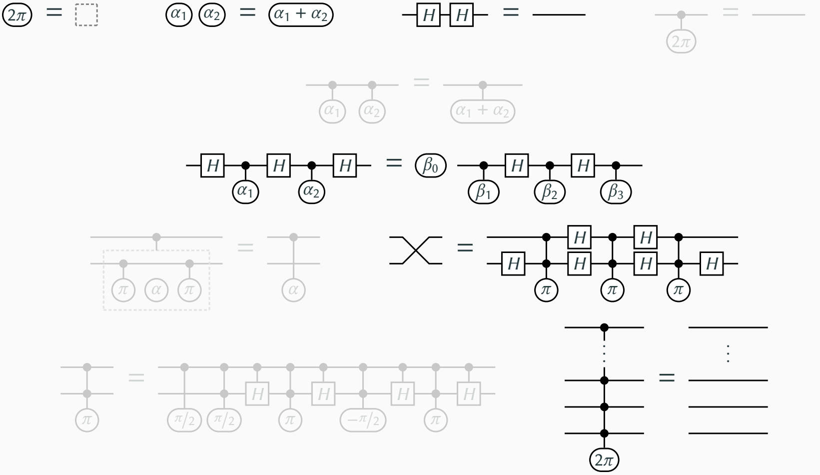
Quantum circuits

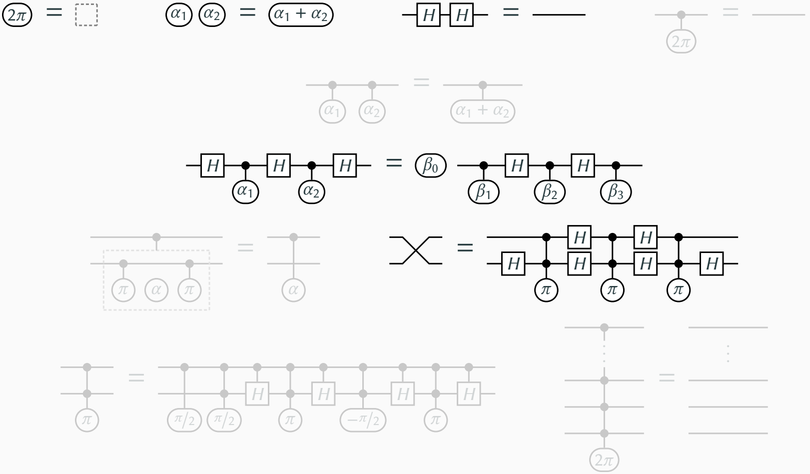


Quantum circuits

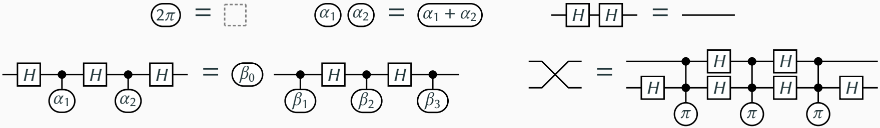


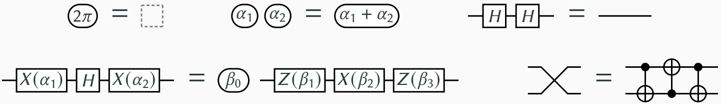
Quantum circuits




2π =
α1 α2 = α1 + α2
H H =
= 2π
α1 α2 = α1 + α2
H H H = β0 β1 H β2 H β3
α1 α2
π α π = α
= H H H H H H
π π π
π = π/2 π/2 H π H −π/2 H π H
= 2π

Quantum circuits




2π =
α_1 α_2 = $\alpha_1 + \alpha_2$
H H =
$X(\alpha_1)$ H $X(\alpha_2)$ = β_0 $Z(\beta_1)$ $X(\beta_2)$ $Z(\beta_3)$
=

To go beyond

Polycontrolled PROPs.

Applications to reversible classical circuits.

Compilation of quantum circuits.

Thanks

(arXiv:2508.21756)

Diagrammatic Reasoning with Control as a Constructor, Applications to Quantum Circuits