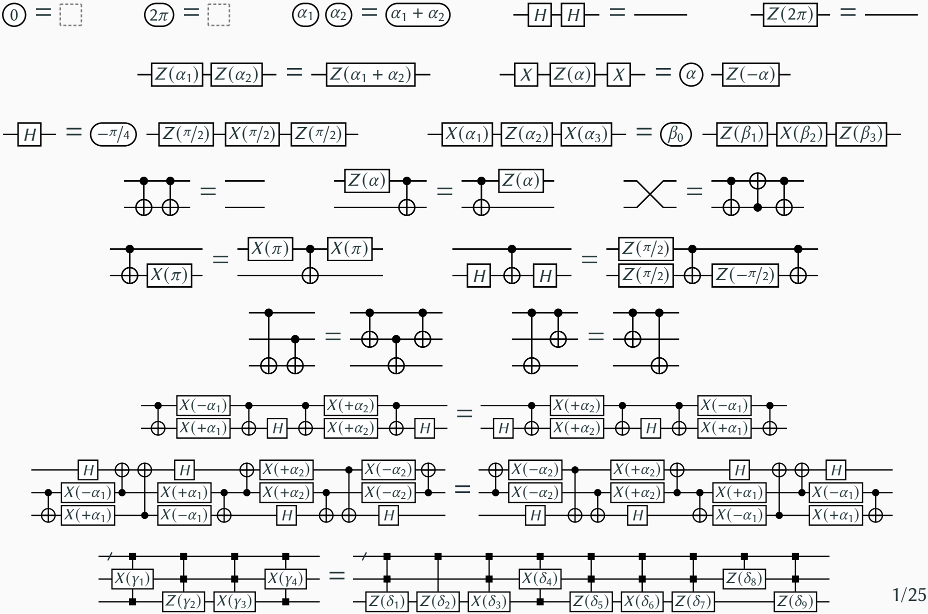
We Improved It, Proved It Minimal, Then Cheated.

9th April 2026 - MOCQUA Seminar

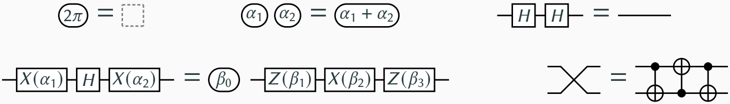
Noé Delorme

Université de Lorraine, CNRS, INRIA, LORIA, Nancy, France

Before



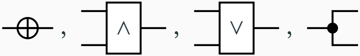
After



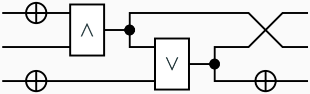
What are quantum circuits?

Boolean circuits

are made of simple generators



and can be composed to form circuits expressing classical algorithms.



Quantum circuits

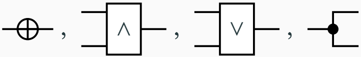
are made of simple generators

and can be composed to form circuits expressing quantum algorithms.

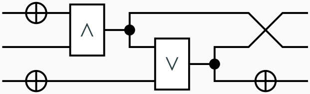
What are quantum circuits?

Boolean circuits

are made of simple generators

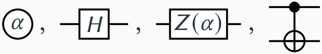


and can be composed to form circuits expressing classical algorithms.

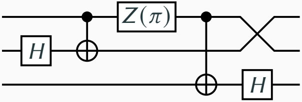


Quantum circuits

are made of simple generators



and can be composed to form circuits expressing quantum algorithms.



Other gates as shorthand notations

Other usual gates can be defined as shorthand notations by compositions of the generators.

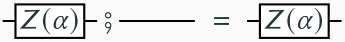
$$-\boxed{X(\alpha)}- \;:=\; -\boxed{H}-\boxed{Z(\alpha)}-\boxed{H}- \qquad -\boxed{Y(\alpha)}- \;:=\; -\boxed{Z(-\pi/2)}-\boxed{X(\alpha)}-\boxed{Z(+\pi/2)}-$$

$$-\boxed{X}- \;:=\; -\boxed{X(\pi)}- \qquad -\boxed{Y}- \;:=\; -\boxed{Y(\pi)}- \qquad -\boxed{Z}- \;:=\; -\boxed{Z(\pi)}-$$

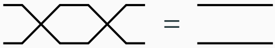
$$-\boxed{S}- \;:=\; -\boxed{Z(\pi/2)}- \qquad -\boxed{T}- \;:=\; -\boxed{Z(\pi/4)}-$$

PROP formalism

Formally, quantum circuits are defined in the PROP formalism, which brings coherence equations such that

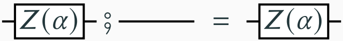


and

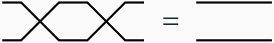


to captures the intuitive behaviour of wires and boxes. Then quantum circuits are defined "up to deformation".

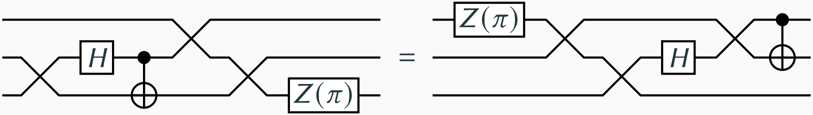
Formally, quantum circuits are defined in the PROP formalism, which brings coherence equations such that



and



to captures the intuitive behaviour of wires and boxes. Then quantum circuits are defined "up to deformation".



Interpretation of quantum circuits

Interpretation

$$\llbracket C_1 \mathbin{;} C_2 \rrbracket = \llbracket C_2 \rrbracket \circ \llbracket C_1 \rrbracket \qquad \llbracket C_1 \otimes C_2 \rrbracket = \llbracket C_1 \rrbracket \otimes \llbracket C_2 \rrbracket$$

$\llbracket$  $\rrbracket = (1)$ $\qquad \llbracket \textcircled{\alpha} \rrbracket = (e^{i\alpha})$

$$\llbracket \text{———} \rrbracket = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \llbracket -\boxed{H}- \rrbracket = {}^1\!/\!\sqrt{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \llbracket -\boxed{Z(\alpha)}- \rrbracket = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$$

$\llbracket$  $\rrbracket = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ $\qquad \llbracket$  $\rrbracket = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

circuits $\neq$ matrices

Interpretation

$$[\![C_1 \fatsemi C_2]\!] = [\![C_2]\!] \circ [\![C_1]\!] \qquad [\![C_1 \otimes C_2]\!] = [\![C_1]\!] \otimes [\![C_2]\!]$$

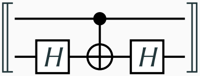
$$[\![\;\boxed{}\;]\!] = (1) \qquad [\![\;\alpha\;]\!] = (e^{i\alpha})$$

$$[\![\;\text{———}\;]\!] = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad [\![\;-\boxed{H}-\;]\!] = {}^1/\sqrt{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad [\![\;-\boxed{Z(\alpha)}-\;]\!] = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$$

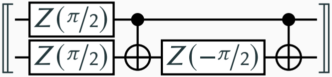
$[\![$  $]\!]$ $= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ $\qquad$ $[\![$  $]\!]$ $= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

circuits $\neq$ matrices

Distinct circuits can have the same interpretation.



=

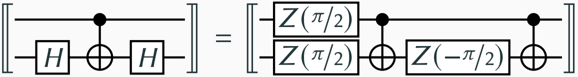


$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

Which circuit is the best? In terms of total number of gates ; in terms of number of fault-tolerant gates ; or to satisfy hardware constraints (for instance topological constraints).

Motivations

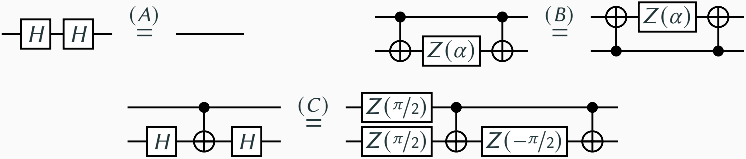
Distinct circuits can have the same interpretation.



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

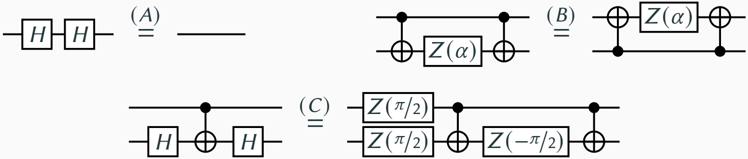
Which circuit is the best? In terms of total number of gates ; in terms of number of fault-tolerant gates ; or to satisfy hardware constraints (for instance topological constraints).

Given a set of axioms,

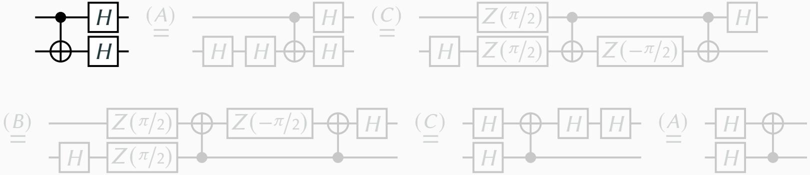


we can derive other equations. For instance,

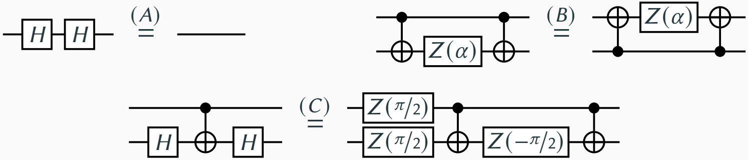
Given a set of axioms,



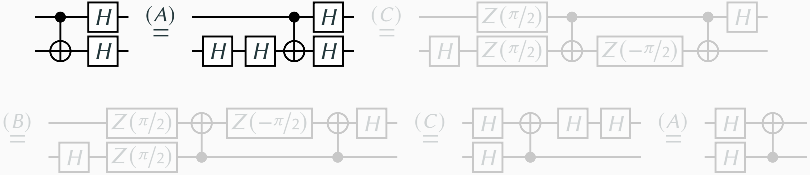
we can derive other equations. For instance,



Given a set of axioms,

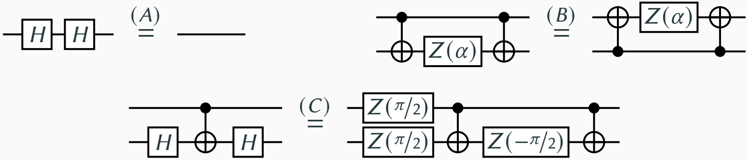


we can derive other equations. For instance,

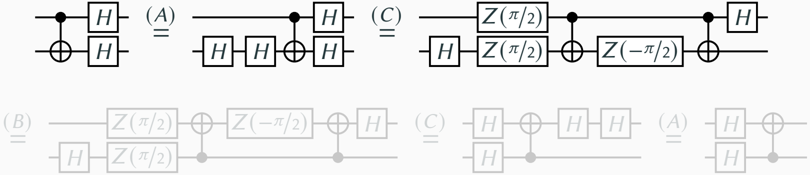


Circuit rewriting

Given a set of axioms,

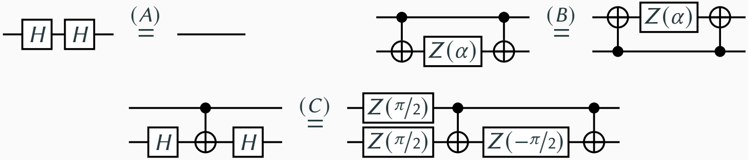


we can derive other equations. For instance,

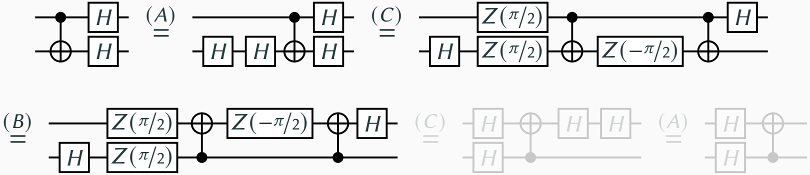


Circuit rewriting

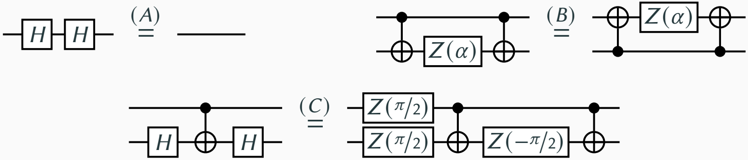
Given a set of axioms,



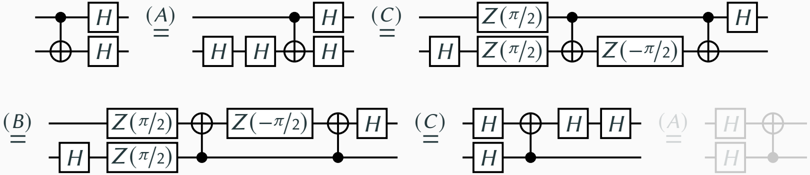
we can derive other equations. For instance,



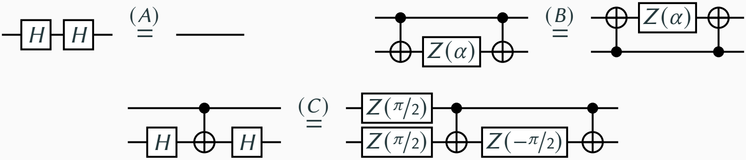
Given a set of axioms,



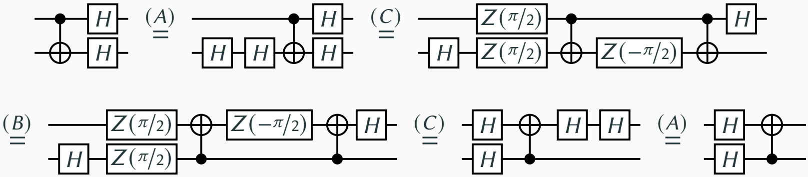
we can derive other equations. For instance,



Given a set of axioms,



we can derive other equations. For instance,



Soundness and completeness

Is there a set of axioms $\mathcal{R}$ from which we can derive any true equation and only true equations in a graphical language $\mathbf{P}$?

Soundness

Any derivable equation is true.

$$\forall C_1, C_2 \quad : \quad \mathbf{P}/\mathcal{R} \vdash C_1 = C_2 \implies \llbracket C_1 \rrbracket = \llbracket C_2 \rrbracket$$

Completeness

Any true equation is derivable.

$$\forall C_1, C_2 \quad : \quad \llbracket C_1 \rrbracket = \llbracket C_2 \rrbracket \implies \mathbf{P}/\mathcal{R} \vdash C_1 = C_2$$

[Clément,Heurtel,Mansfield,Perdrix,Valiron'2023]

The first complete and sound set of axioms for quantum circuits.

Is there a set of axioms $\mathcal{R}$ from which we can derive any true equation and only true equations in a graphical language $\mathbf{P}$?

Soundness

Any derivable equation is true.

$$\forall C_1, C_2 \quad : \quad \mathbf{P}/\mathcal{R} \vdash C_1 = C_2 \implies [\![C_1]\!] = [\![C_2]\!]$$

Completeness

Any true equation is derivable.

$$\forall C_1, C_2 \quad : \quad [\![C_1]\!] = [\![C_2]\!] \implies \mathbf{P}/\mathcal{R} \vdash C_1 = C_2$$

[Clément,Heurtel,Mansfield,Perdrix,Valiron'2023]

The first complete and sound set of axioms for quantum circuits.

Soundness and completeness

Is there a set of axioms $\mathcal{R}$ from which we can derive any true equation and only true equations in a graphical language **P**?

Soundness

Any derivable equation is true.

$$\forall C_1, C_2 \quad : \quad \mathbf{P}/\mathcal{R} \vdash C_1 = C_2 \implies [\![C_1]\!] = [\![C_2]\!]$$

Completeness

Any true equation is derivable.

$$\forall C_1, C_2 \quad : \quad [\![C_1]\!] = [\![C_2]\!] \implies \mathbf{P}/\mathcal{R} \vdash C_1 = C_2$$

[Clément,Heurtel,Mansfield,Perdrix,Valiron'2023]

The first complete and sound set of axioms for quantum circuits.

Soundness and completeness

Is there a set of axioms $\mathcal{R}$ from which we can derive any true equation and only true equations in a graphical language $\mathbf{P}$?

Soundness

Any derivable equation is true.

$\forall C_1, C_2 \quad : \quad \mathbf{P}/\mathcal{R} \vdash C_1 = C_2 \implies [\![C_1]\!] = [\![C_2]\!]$

Completeness

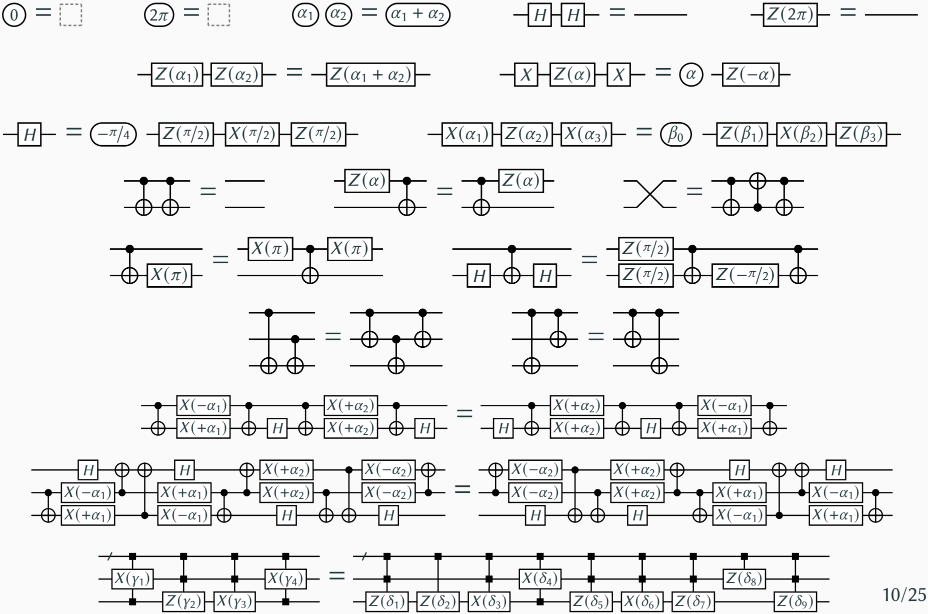
Any true equation is derivable.

$\forall C_1, C_2 \quad : \quad [\![C_1]\!] = [\![C_2]\!] \implies \mathbf{P}/\mathcal{R} \vdash C_1 = C_2$

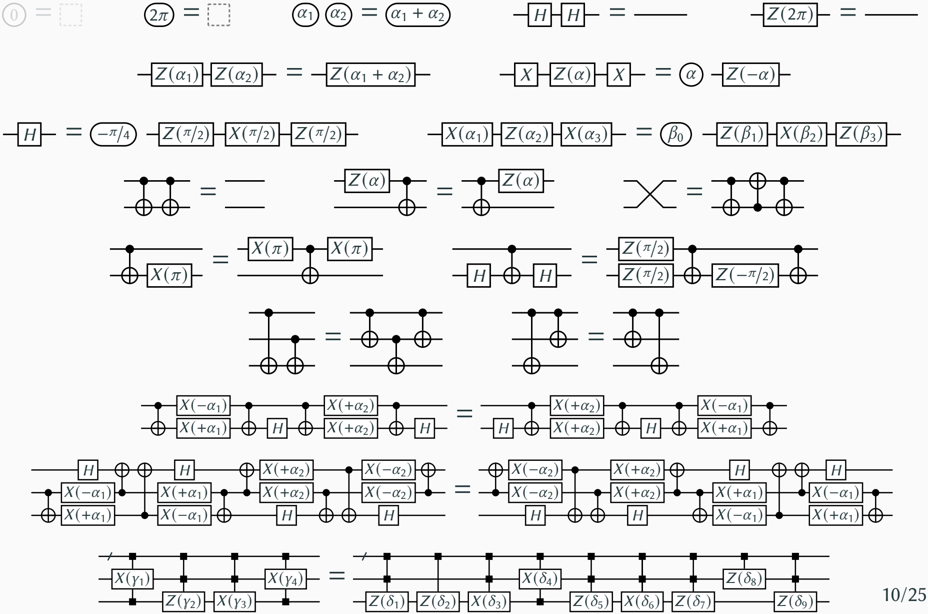
[Clément,Heurtel,Mansfield,Perdrix,Valiron'2023]

The first complete and sound set of axioms for quantum circuits.

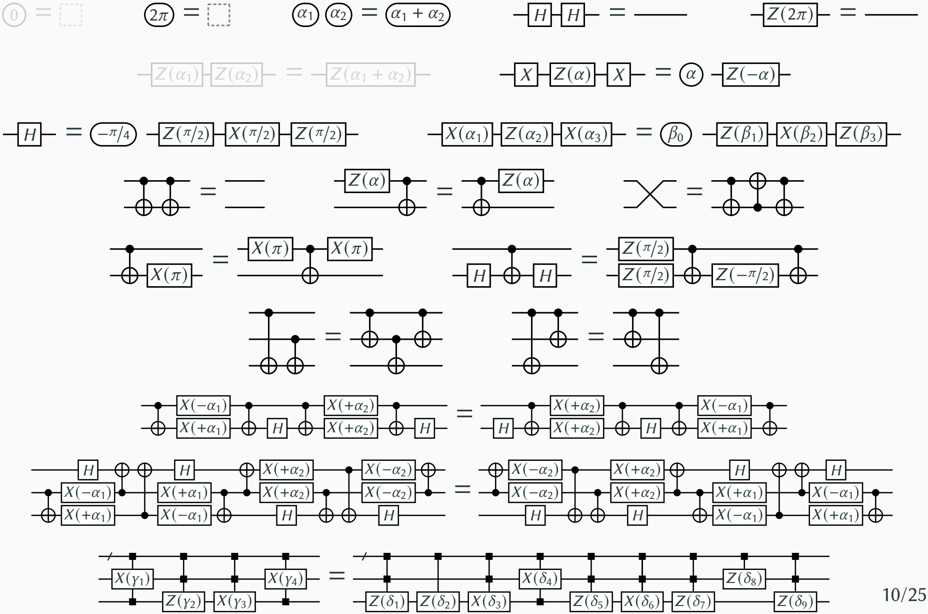
Complete and sound set of axioms



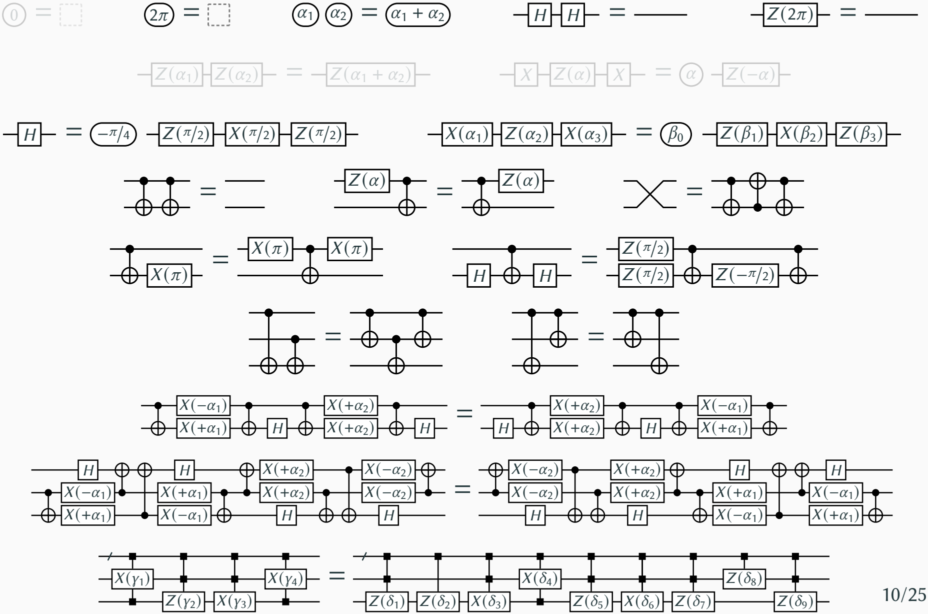
Complete and sound set of axioms



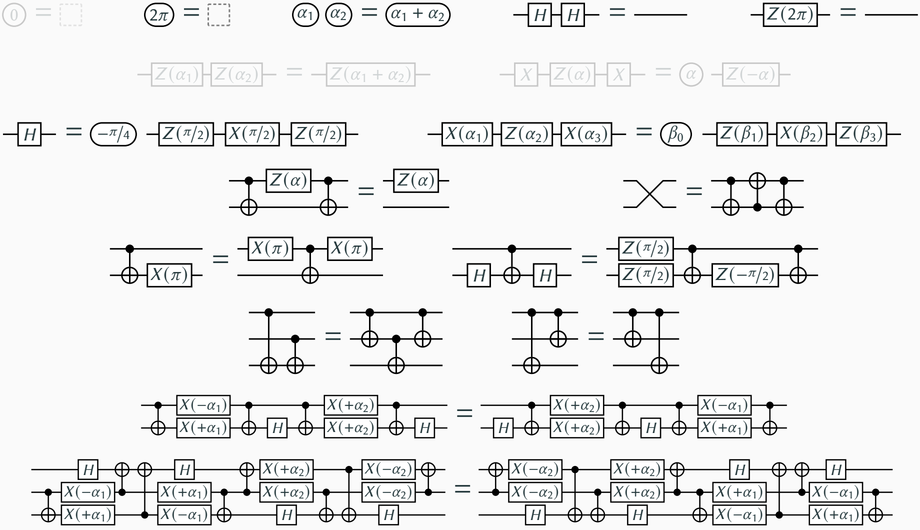
Complete and sound set of axioms

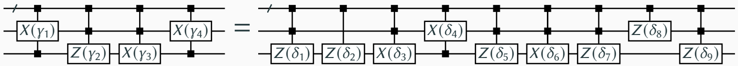


Complete and sound set of axioms

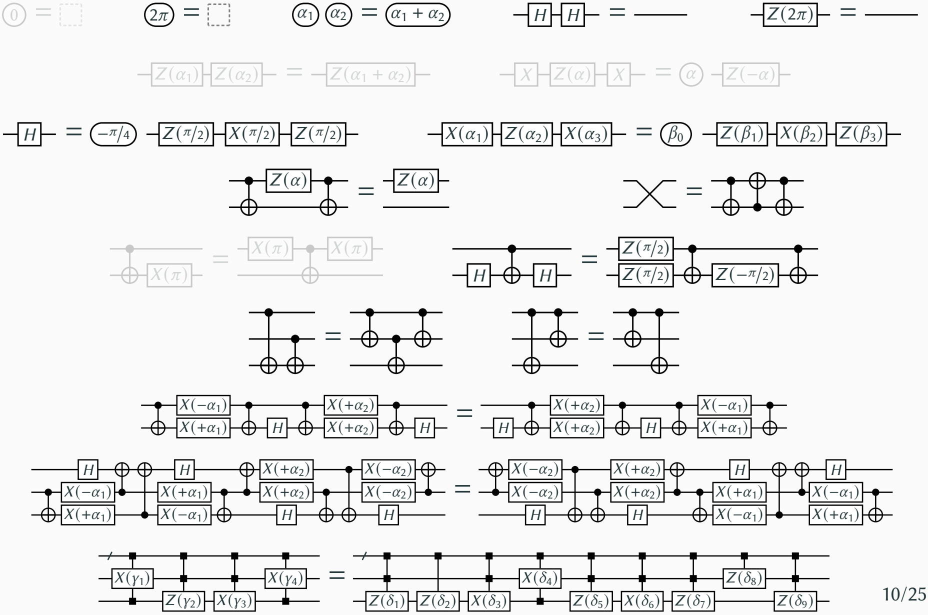


Complete and sound set of axioms

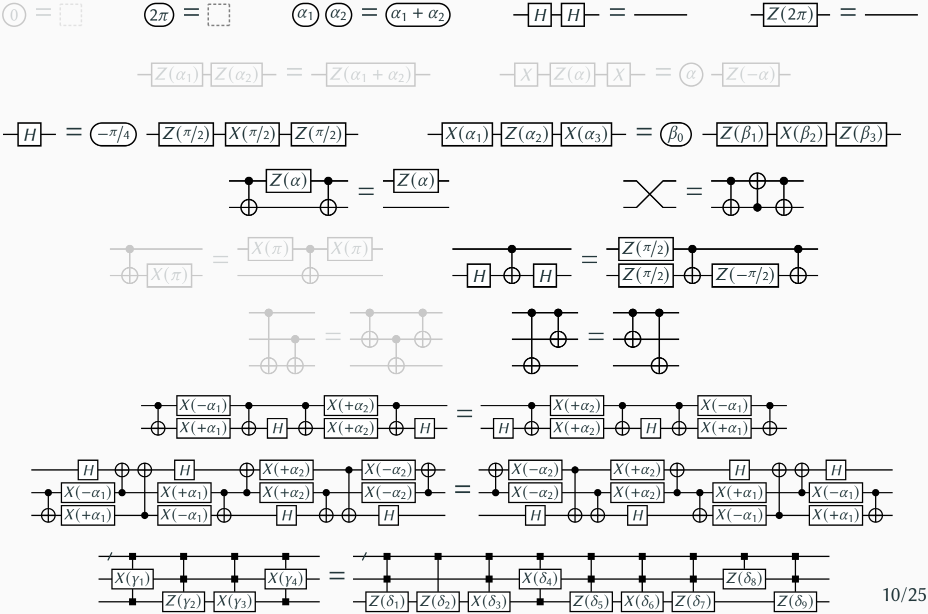




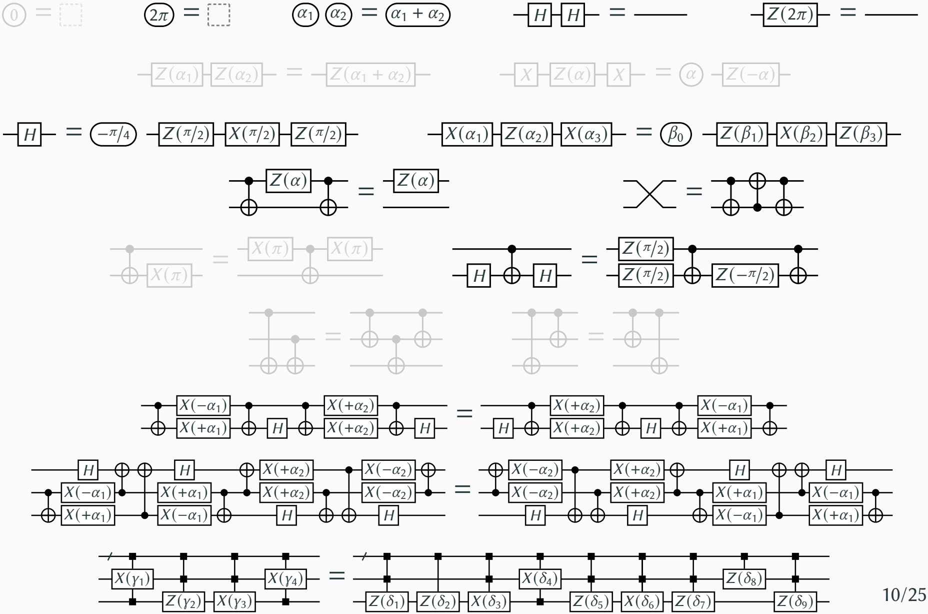
Complete and sound set of axioms

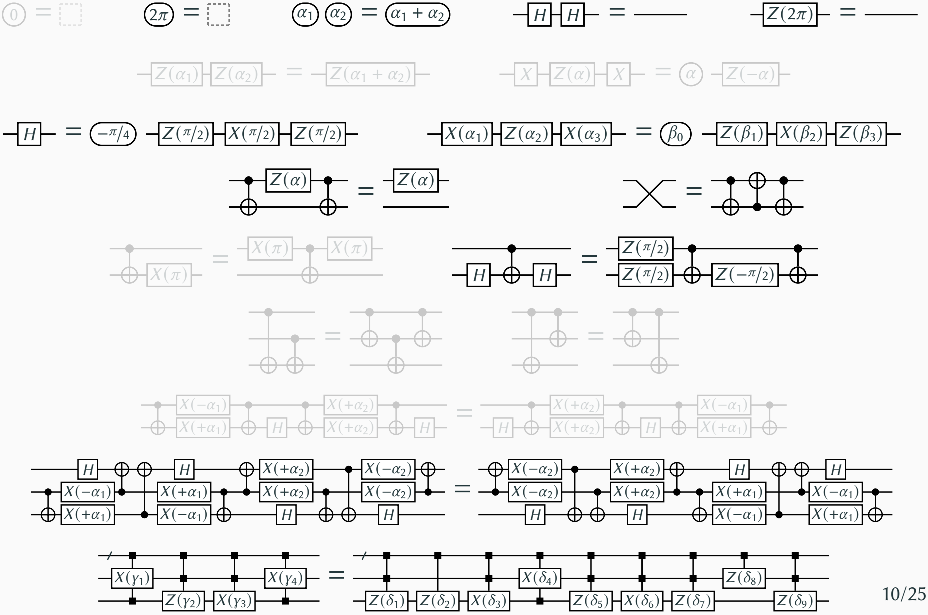


Complete and sound set of axioms

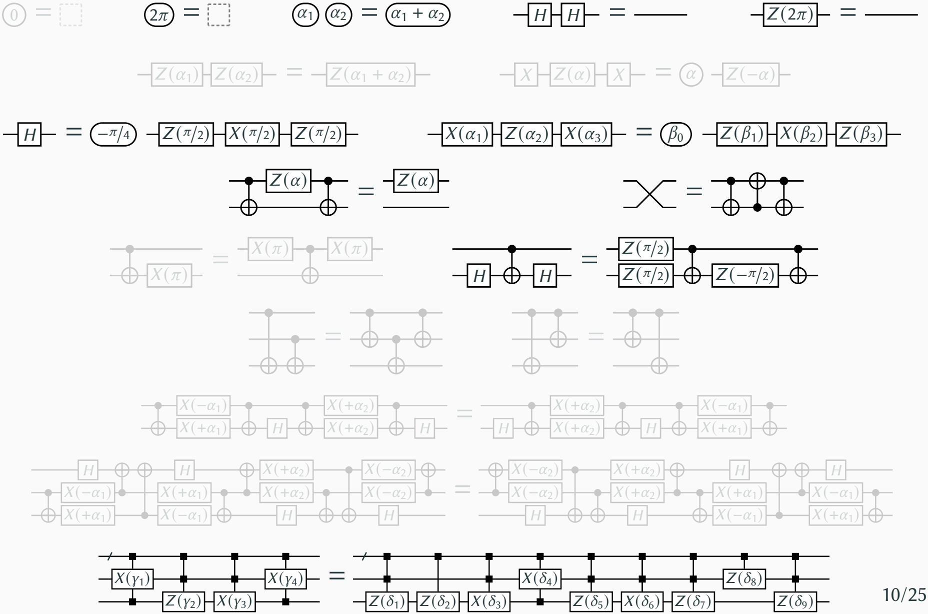


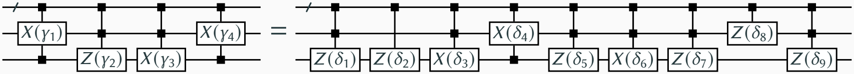
Complete and sound set of axioms




0 =
2π =
α1 α2 = α1 + α2
H H =
Z(2π) =
Z(α1) Z(α2) = Z(α1 + α2)
X Z(α) X = α Z(−α)
H = −π/4 Z(π/2) X(π/2) Z(π/2)
X(α1) Z(α2) X(α3) = β0 Z(β1) X(β2) Z(β3)
Z(α) = Z(α)
=
X(π) = X(π) X(π)
H H = Z(π/2) Z(π/2) Z(−π/2)
=
=
X(−α1) X(+α1) H X(+α2) X(+α2) H = H X(+α2) X(+α2) H X(−α1) X(+α1)
H X(−α1) X(+α1) H X(+α1) X(−α1) X(+α2) X(+α2) H X(−α2) X(−α2) H = X(−α2) X(−α2) H X(+α2) X(+α2) H H X(+α1) X(−α1) H X(−α1) X(+α1)
X(γ1) Z(γ2) X(γ3) X(γ4) = Z(δ1) Z(δ2) X(δ3) X(δ4) Z(δ5) X(δ6) Z(δ7) Z(δ8) Z(δ9)

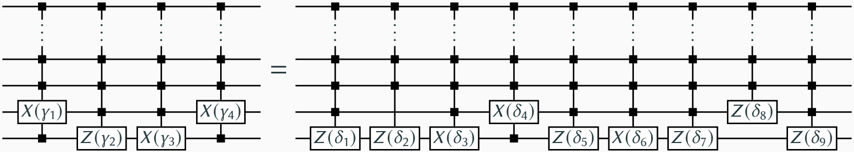
Complete and sound set of axioms



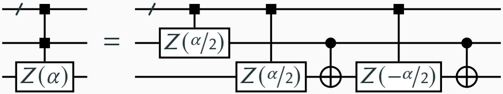


There is an instance of this axiom for any number of wires $n \geq 2$, and all gates are shorthand notations implementing controlled operations. For instance, the controlled version of $\boxed{Z(\alpha)}$ is defined as follows.

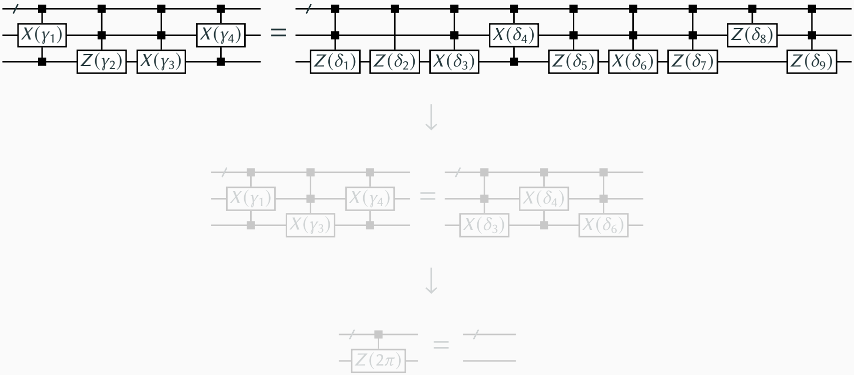
The huge and ugly axiom



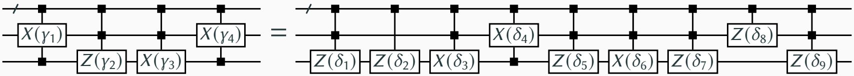
There is an instance of this axiom for any number of wires $n \geq 2$, and all gates are shorthand notations implementing controlled operations. For instance, the controlled version of $\boxed{Z(\alpha)}$ is defined as follows.



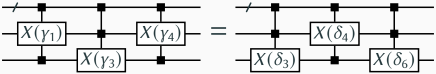
Huge, ugly, and useless...



Huge, ugly, and useless...

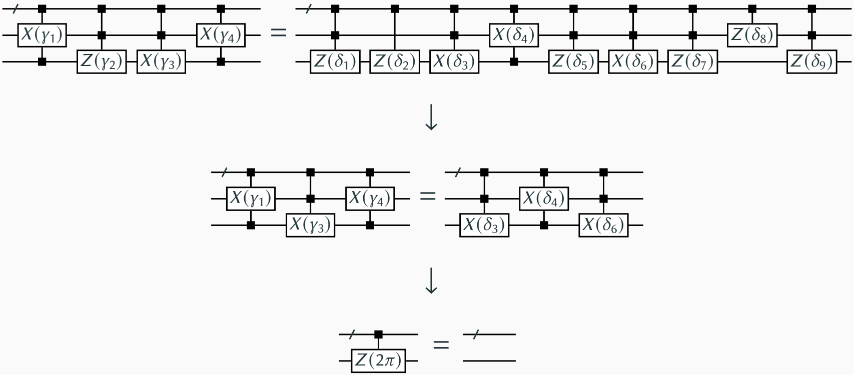


$\downarrow$

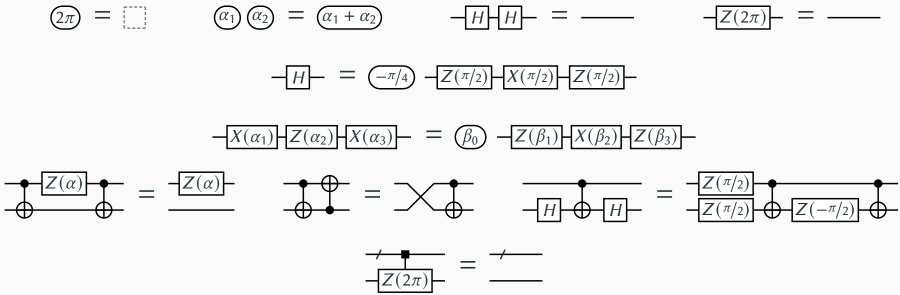


$\downarrow$

Huge, ugly, and useless...



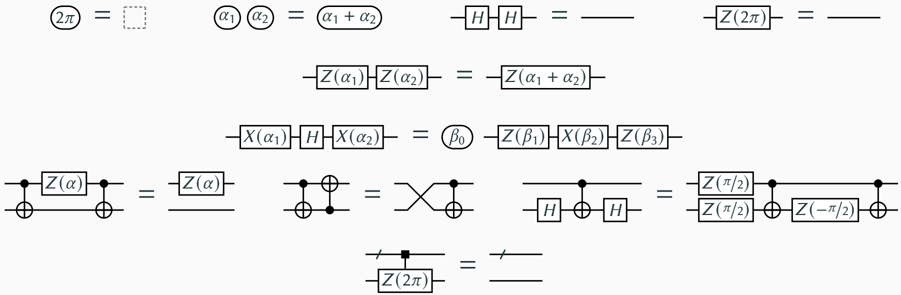
New set of axioms



Theorem

The axioms are independents.

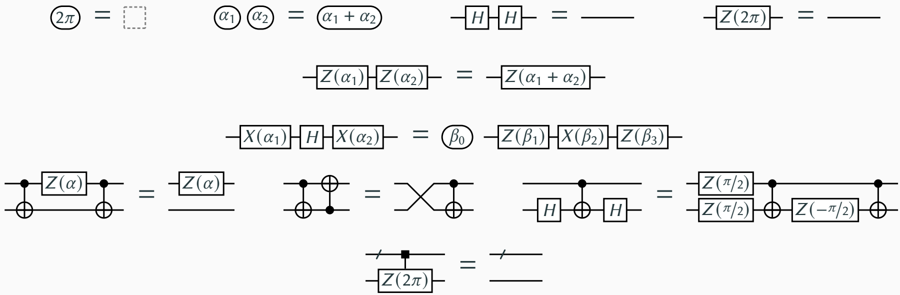
New set of axioms



Theorem

The axioms are independents.

New set of axioms



Theorem

The axioms are independents.

Really?

- What about the last axiom?
- Every instance is necessary. Every single of them.
- And what about Euler's axiom?
- You need at least uncountably many instances of Euler's axiom.
- And with a different set of generators?
- Same issue. I told you, we can no longer improve it. It's over!
- Isn't that sad?
- That's the way it is.
- ...
- ...
- Let's cheat!

Really?

- What about the last axiom?
- Every instance is necessary. Every single of them.
- And what about Euler's axiom?
- You need at least uncountably many instances of Euler's axiom.
- And with a different set of generators?
- Same issue. I told you, we can no longer improve it. It's over!
- Isn't that sad?
- That's the way it is.
- ...
- ...
- Let's cheat!

Really?

- What about the last axiom?
- Every instance is necessary. Every single of them.
- And what about Euler's axiom?
- You need at least uncountably many instances of Euler's axiom.
- And with a different set of generators?
- Same issue. I told you, we can no longer improve it. It's over!
- Isn't that sad?
- That's the way it is.
- ...
- ...
- Let's cheat!

Really?

- What about the last axiom?
- Every instance is necessary. Every single of them.
- And what about Euler’s axiom?
- You need at least uncountably many instances of Euler’s axiom.
- And with a different set of generators?
- Same issue. I told you, we can no longer improve it. It’s over!
- Isn’t that sad?
- That’s the way it is.
- ...
- ...
- Let’s cheat!

Really?

- What about the last axiom?
- Every instance is necessary. Every single of them.
- And what about Euler's axiom?
- You need at least uncountably many instances of Euler's axiom.
- And with a different set of generators?
- Same issue. I told you, we can no longer improve it. It's over!
- Isn't that sad?
- That's the way it is.
- ...
- ...
- Let's cheat!

Really?

- What about the last axiom?
- Every instance is necessary. Every single of them.
- And what about Euler's axiom?
- You need at least uncountably many instances of Euler's axiom.
- And with a different set of generators?
- Same issue. I told you, we can no longer improve it. It's over!
- Isn't that sad?
- That's the way it is.
- ...
- ...
- Let's cheat!

Really?

- What about the last axiom?
- Every instance is necessary. Every single of them.
- And what about Euler's axiom?
- You need at least uncountably many instances of Euler's axiom.
- And with a different set of generators?
- Same issue. I told you, we can no longer improve it. It's over!
- Isn't that sad?
- That's the way it is.
- ...
- ...
- Let's cheat!

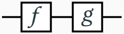
“If the game is impossible, then change the rules.”

Generators

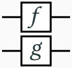
id_0 $\qquad$ id_1 $\qquad$ σ $\qquad$ a $\qquad$ b

Composition operators

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



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

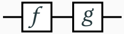


NEW!

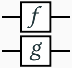
$$\frac{f : n \to n}{\mathrm{C}(f) : 1 + n \to 1 + n}$$

Composition operators

$$\frac{f : n \longrightarrow p \qquad g : p \longrightarrow m}{f \fatsemi g : n \longrightarrow m}$$

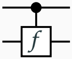


$$\frac{f : n \longrightarrow m \qquad g : p \longrightarrow q}{f \otimes g : n + p \longrightarrow m + q}$$

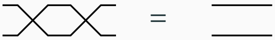


NEW!

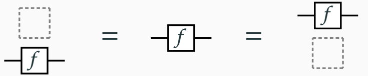
$$\frac{f : n \longrightarrow n}{\mathrm{C}(f) : 1 + n \longrightarrow 1 + n}$$



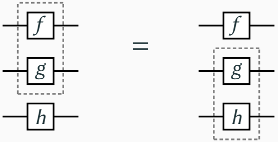
$$\sigma \fatsemi \sigma \quad = \quad \mathrm{id}_1 \otimes \mathrm{id}_1$$



$$\mathrm{id}_0 \otimes f \quad = \quad f \quad = \quad f \otimes \mathrm{id}_0$$



$$(f \otimes g) \otimes h \quad = \quad f \otimes (g \otimes h)$$

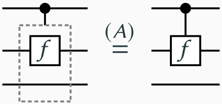


$$(f \fatsemi g) \fatsemi h \quad = \quad f \fatsemi (g \fatsemi g)$$

$$(f_1 \fatsemi g_2) \otimes (f_2 \fatsemi g_2) \quad = \quad (f_1 \otimes f_2) \fatsemi (g_1 \otimes g_2)$$

. . .

NEW!

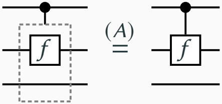


NEW!

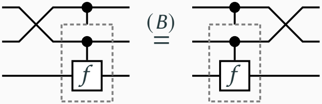
NEW!

Coherence equations

NEW!



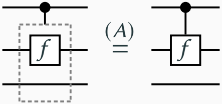
NEW!



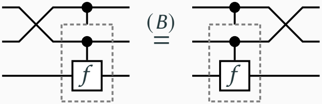
NEW!

Coherence equations

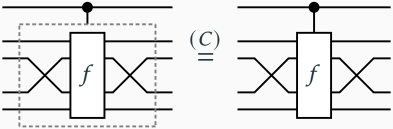
NEW!



NEW!



NEW!



Controlled PROPs

Definition

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

Definition

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

Controlled PROPs

Definition

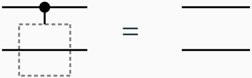
A control functor maps any endocircuit $f : n \to n$ to the endocircuit $C(f) : (1+n) \to (1+n)$ while satisfying (A), (B), and (C).

Definition

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

Controlled PROPs

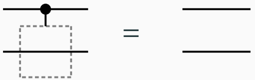
$$\mathrm{C}(\mathrm{id}_1) = \mathrm{id}_1 \otimes \mathrm{id}_1$$

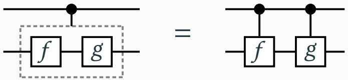


$$\mathrm{C}(f \mathbin{;} g) = \mathrm{C}(f) \mathbin{;} \mathrm{C}(g)$$

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

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

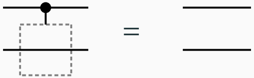


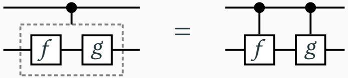


Notice however that $C(f \otimes g) \neq C(f) \otimes C(g)$, instead we have

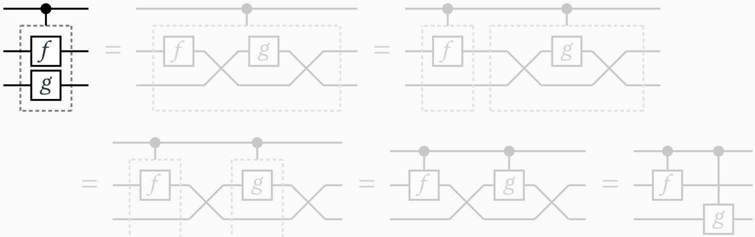
Controlled PROPs

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



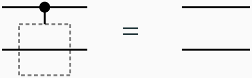


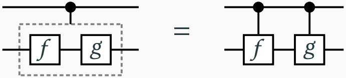
Notice however that $C(f \otimes g) \neq C(f) \otimes C(g)$, instead we have



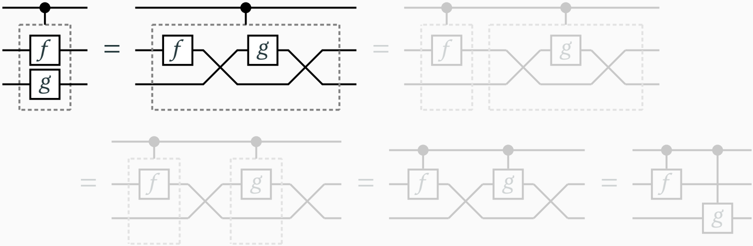
Controlled PROPs

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

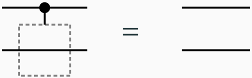


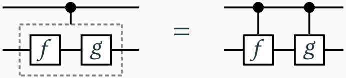


Notice however that $C(f \otimes g) \neq C(f) \otimes C(g)$, instead we have

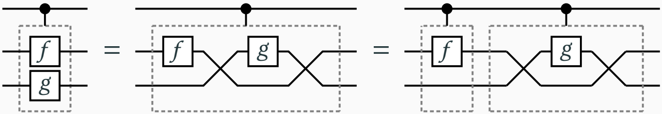


$$\mathrm{C}(\mathrm{id}_1) = \mathrm{id}_1 \otimes \mathrm{id}_1 \qquad \mathrm{C}(f \fatsemi g) = \mathrm{C}(f) \fatsemi \mathrm{C}(g)$$



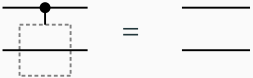


Notice however that $\mathrm{C}(f \otimes g) \neq \mathrm{C}(f) \otimes \mathrm{C}(g)$, instead we have

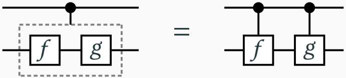


Controlled PROPs

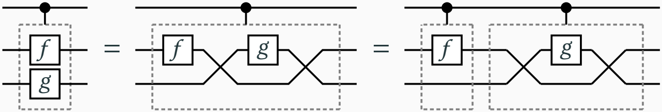
$$C(\mathrm{id}_1) \quad = \quad \mathrm{id}_1 \otimes \mathrm{id}_1$$

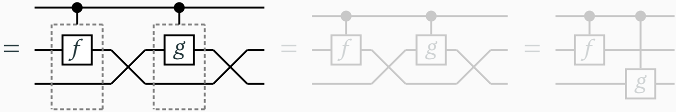


$$C(f \fatsemi g) \quad = \quad C(f) \fatsemi C(g)$$

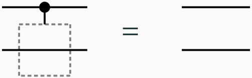


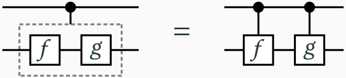
Notice however that $C(f \otimes g) \neq C(f) \otimes C(g)$, instead we have



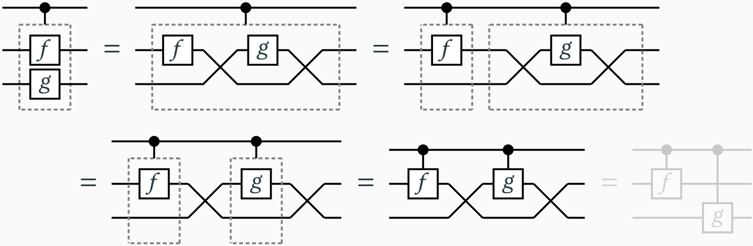


$$\mathrm{C}(\mathrm{id}_1) = \mathrm{id}_1 \otimes \mathrm{id}_1 \qquad \mathrm{C}(f \mathbin{;} g) = \mathrm{C}(f) \mathbin{;} \mathrm{C}(g)$$



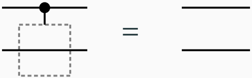


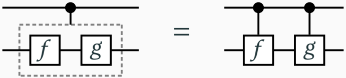
Notice however that $\mathrm{C}(f \otimes g) \neq \mathrm{C}(f) \otimes \mathrm{C}(g)$, instead we have



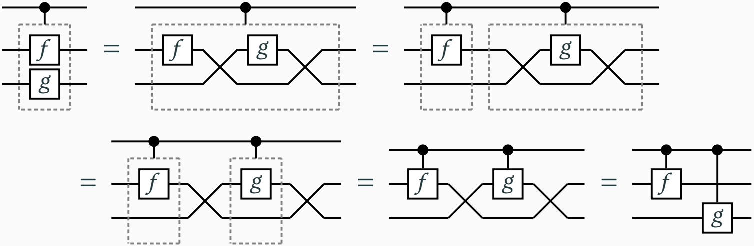
Controlled PROPs

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





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



$$\mathbf{P}/\mathcal{R} \vdash C_1 = C_2 \implies \mathbf{P}/\mathcal{R} \vdash \mathrm{C}(C_1) = \mathrm{C}(C_2) \quad \textbf{NEW!}$$

Example

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

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

Moreover, the equations is = is derivable.

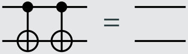
Does anyone actually read the headlines anyway?

$$\mathbf{P}/\mathcal{R} \vdash C_1 = C_2 \implies \mathbf{P}/\mathcal{R} \vdash \mathrm{C}(C_1) = \mathrm{C}(C_2) \quad \textbf{NEW!}$$

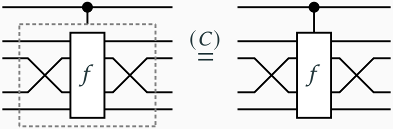
Example

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

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

Moreover, the equations is  is derivable.

Conjugated PROP



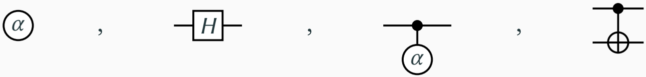
Definition

A conjugated PROP is a controlled PROP such that

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

Simpler generators

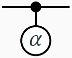
Simpler generators



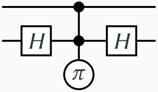
Simpler generators

,

,

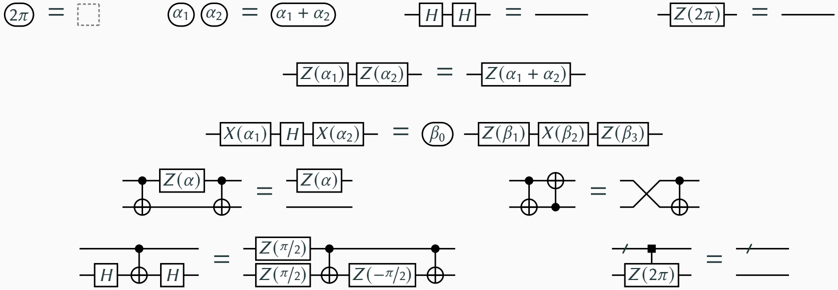


,

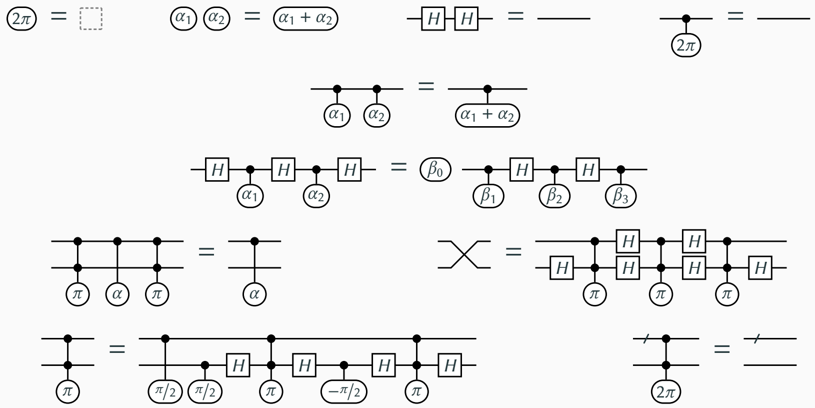


Simpler generators

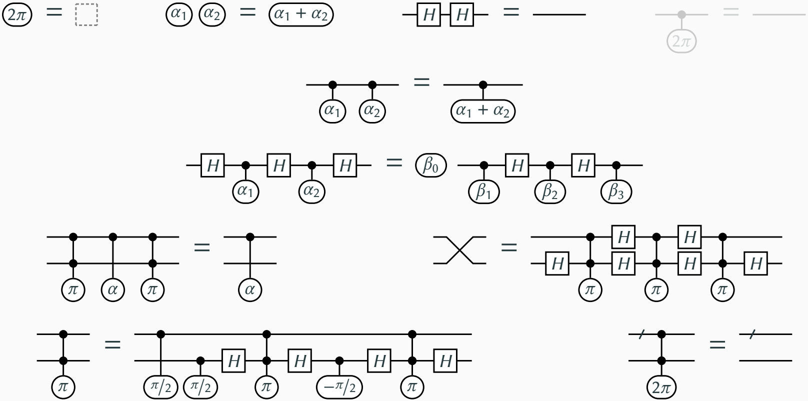
Simpler axioms

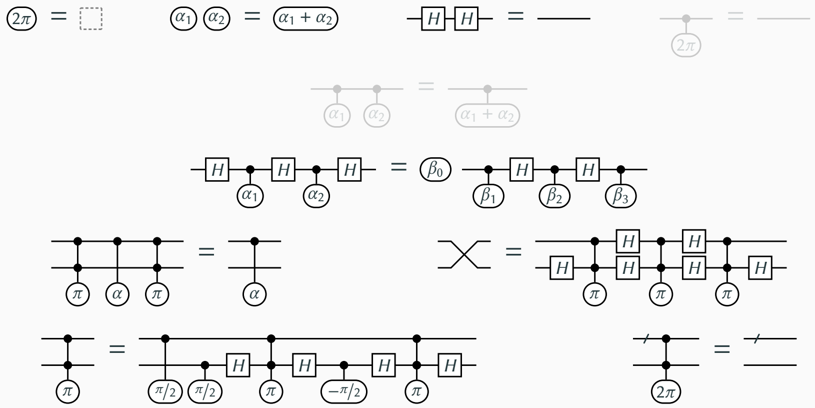


Simpler axioms

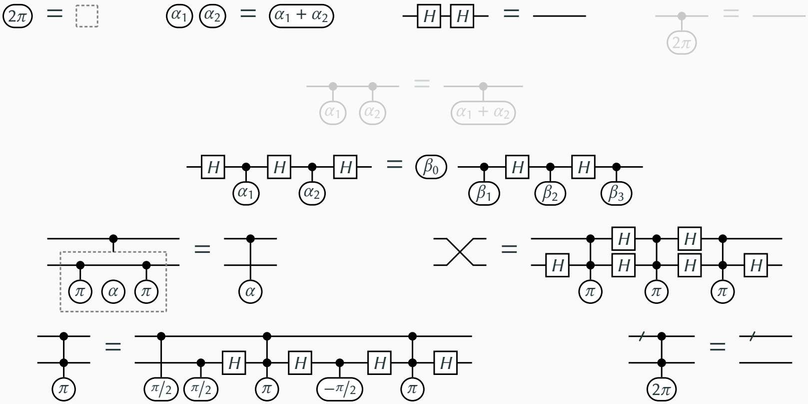


Simpler axioms

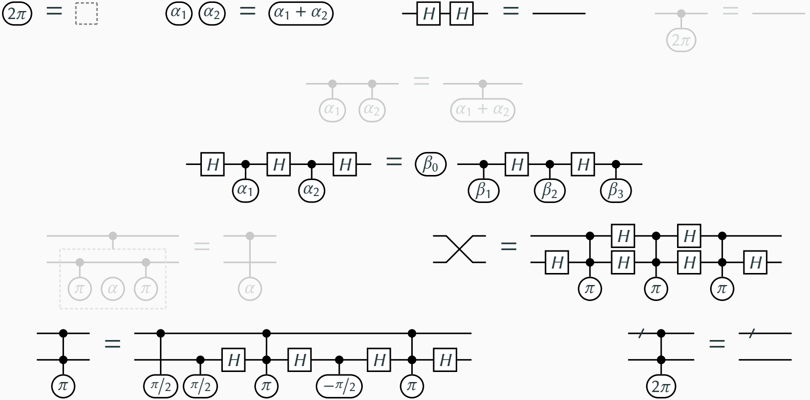



2π
α1 α2
α1 + α2
H H
2π
α1 α2
α1 + α2
H H H
β0
H H
α1 α2
β1 β2 β3
π α π
α
H H H H H
π π π
H H H H
π/2 π/2 π −π/2 π
π
2π

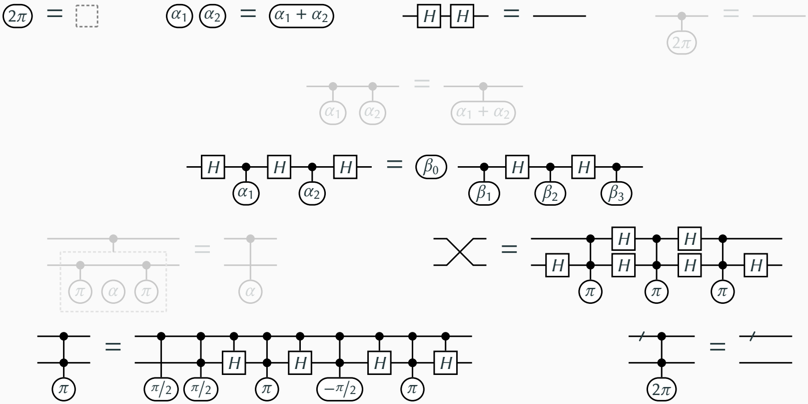
Simpler axioms



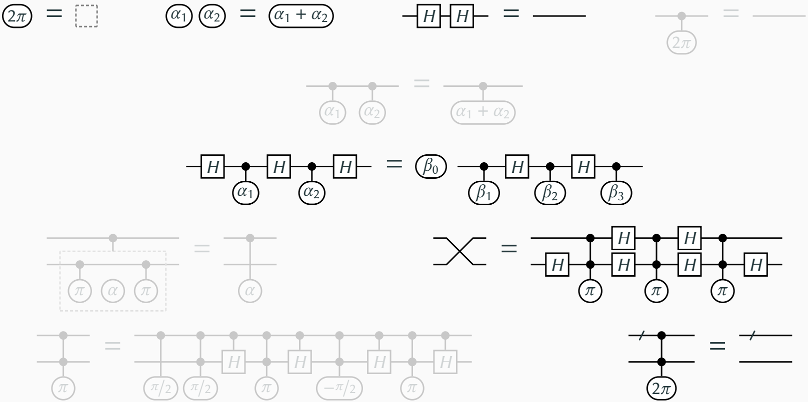
Simpler axioms



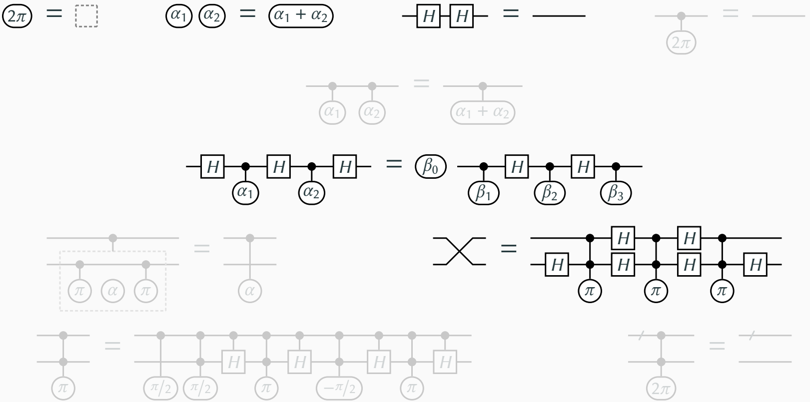
Simpler axioms



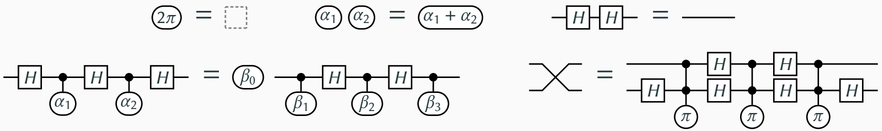
Simpler axioms



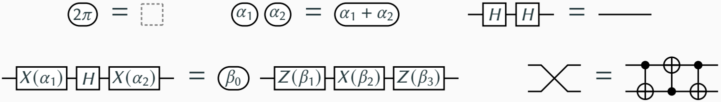
Simpler axioms



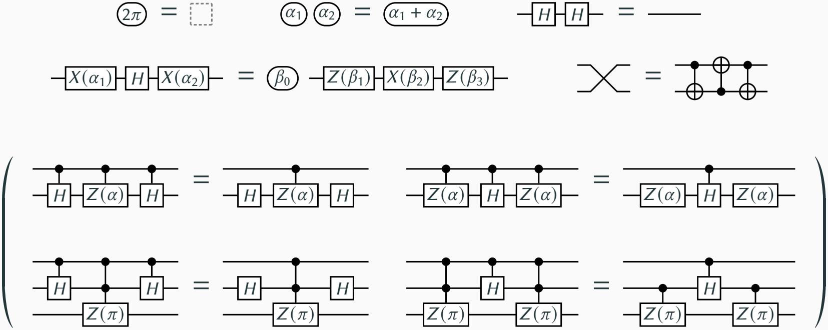
Final set of axioms using controlled PROPs



Final set of axioms using controlled PROPs



Final set of axioms using controlled PROPs



Thanks

(arXiv:2508.21756)

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