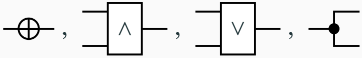
Diagrammatic Reasoning with Control as a Constructor, Applications to Quantum Circuits

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

21st August 2026 - QPL 2026

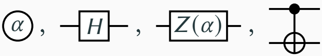
Boolean circuits

are made of simple generators



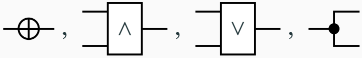
Quantum circuits

are made of simple generators

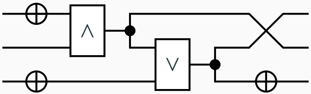


Boolean circuits

are made of simple generators

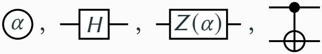


and can be composed to form circuits expressing classical algorithms.

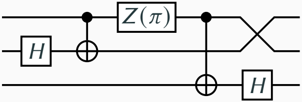


Quantum circuits

are made of simple generators



and can be composed to form circuits expressing quantum algorithms.

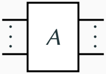


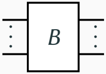
PROP

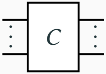
$$\overline{\mathrm{id}_0 : 0 \longrightarrow 0} \qquad \overline{\mathrm{id}_1 : 1 \longrightarrow 1} \qquad \overline{\sigma_{1,1} : 2 \longrightarrow 2}$$

$$\frac{}{\mathrm{id}_0 : 0 \to 0} \qquad \frac{}{\mathrm{id}_1 : 1 \to 1} \qquad \frac{}{\sigma_{1,1} : 2 \to 2}$$

$$\frac{}{A : n_A \to m_A} \qquad \frac{}{B : n_B \to m_B} \qquad \frac{}{C : n_C \to m_C}$$







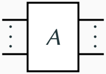
$\cdots$

$$\frac{}{\mathrm{id}_0 : 0 \to 0}$$

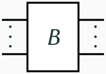
$$\frac{}{\mathrm{id}_1 : 1 \to 1}$$

$$\frac{}{\sigma_{1,1} : 2 \to 2}$$

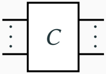
$$\frac{}{A : n_A \to m_A}$$



$$\frac{}{B : n_B \to m_B}$$

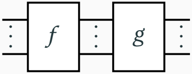


$$\frac{}{C : n_C \to m_C}$$

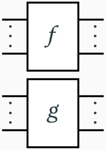


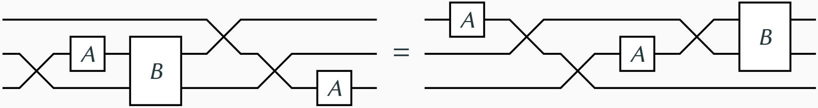
$\cdots$

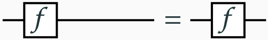
$$\frac{f : n \to p \quad g : p \to m}{f \mathbin{;} g : n \to m}$$

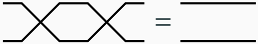


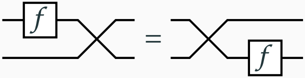
$$\frac{f : n \to m \quad g : p \to q}{f \otimes g : n + p \to m + q}$$

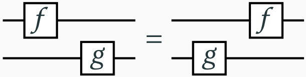



A
B
A
=
A
A
B


f
=
f


=

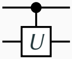

f
=
f

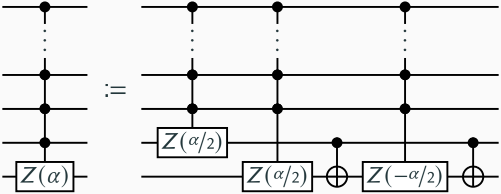

f
g
=
f
g

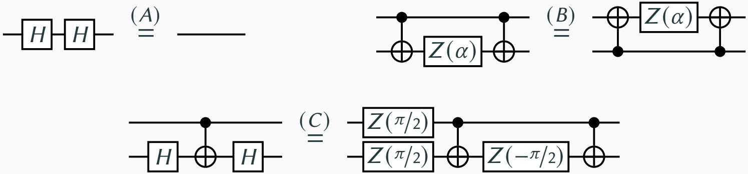
...

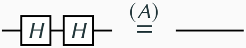
Quantum circuits

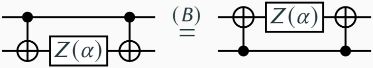

α
Z(α)
H

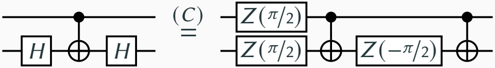
$\llbracket$  $\rrbracket = \left(\begin{array}{c|c} \mathbb{I} & 0 \\ \hline 0 & U \end{array}\right)$

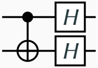

$Z(\alpha)$
$:=$
$Z(\alpha/2)$
$Z(\alpha/2)$
$Z(-\alpha/2)$

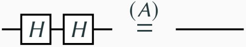

H
H
(A)
=
Z(α)
(B)
=
Z(α)
H
H
(C)
=
Z(π/2)
Z(π/2)
Z(−π/2)

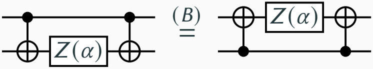

H
H
(A)
=

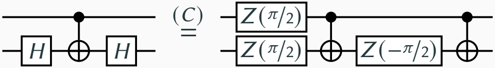

Z(α)
(B)
=
Z(α)

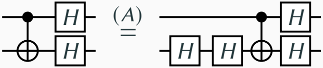

H
H
(C)
=
Z(π/2)
Z(π/2)
Z(−π/2)

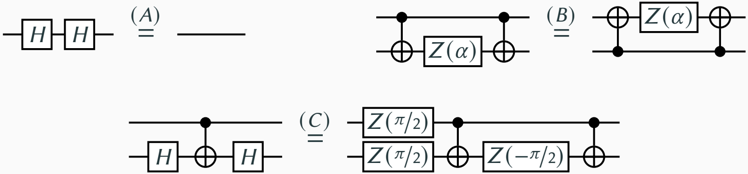

H
H

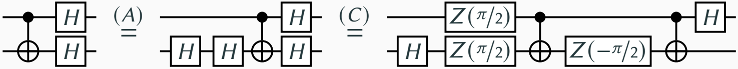

H
H
(A)
=

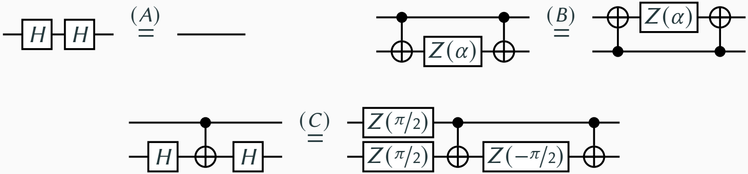

Z(α)
(B)
=
Z(α)

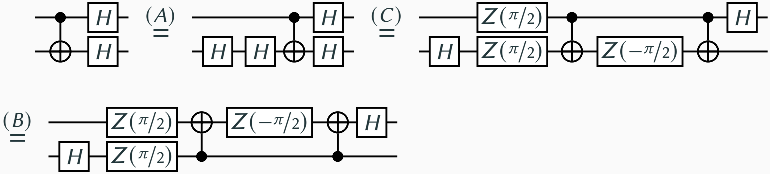

H
H
(C)
=
Z(π/2)
Z(π/2)
Z(−π/2)

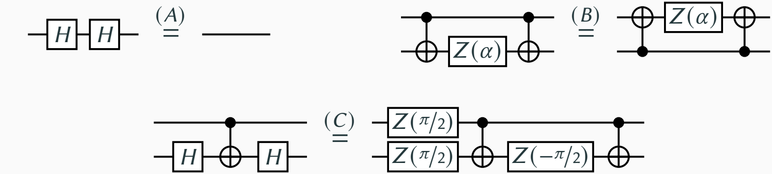

H
H
(A)
=
H
H
H
H

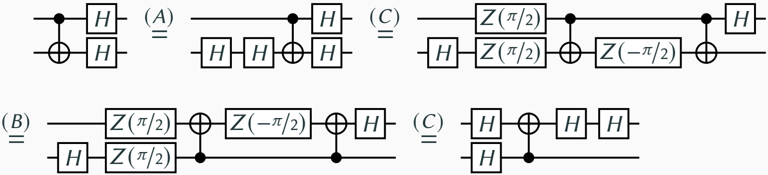

H
H
(A)
Z(α)
(B)
Z(α)
H
H
(C)
Z(π/2)
Z(π/2)
Z(−π/2)

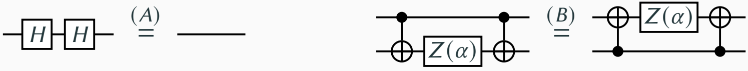

H
H
(A)
H
H
H
H
(C)
Z(π/2)
H
Z(π/2)
Z(−π/2)
H

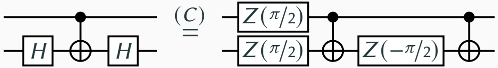

H
H
(A)
Z(α)
(B)
Z(α)
H
H
(C)
Z(π/2)
Z(π/2)
Z(−π/2)

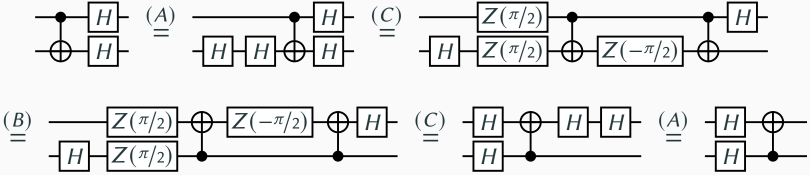

H
H
(A)
H
H
H
H
(C)
Z(π/2)
H
Z(π/2)
Z(−π/2)
H
(B)
Z(π/2)
Z(−π/2)
H
H
Z(π/2)


H
H
(A)
=
Z(α)
(B)
=
Z(α)
H
H
(C)
=
Z(π/2)
Z(π/2)
Z(−π/2)


H
H
(A)
=
H
H
H
H
(C)
=
Z(π/2)
H
Z(π/2)
Z(−π/2)
H
(B)
=
Z(π/2)
H
Z(π/2)
Z(−π/2)
H
(C)
=
H
H
H
H

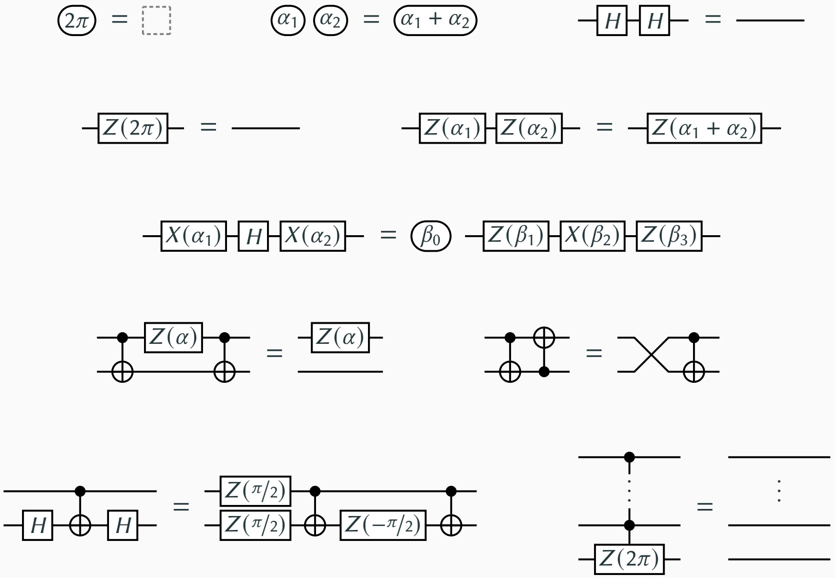

H
H
(A)
(B)
Z(α)
Z(α)


H
H
(C)
Z(π/2)
Z(π/2)
Z(−π/2)


H
(A)
(C)
(B)
Z(π/2)
Z(−π/2)

Definition

An axiomatization is said to be **complete** when any true equation can be derived from its axioms.


2π =
α1 α2 = α1 + α2
H H =
Z(2π) =
Z(α1) Z(α2) = Z(α1 + α2)
X(α1) H X(α2) = β0 Z(β1) X(β2) Z(β3)
Z(α) = Z(α)
=
H H = Z(π/2) Z(π/2) Z(−π/2)
Z(2π) =

Theorem [CHMPV2023, CDP2024]

The axiomatization is **complete**, meaning that any true equation can be derived from its axioms.

Theorem [CHMPV2023, CDP2024]

The axiomatization is **complete**, meaning that any true equation can be derived from its axioms.

Theorem [CDP2024]

The axiomatization is **minimal**, meaning that none of its axiom can be removed without loosing completeness.

Theorem [CHMPV2023, CDP2024]

The axiomatization is **complete**, meaning that any true equation can be derived from its axioms.

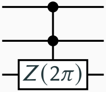
Theorem [CDP2024]

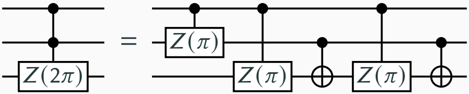
The axiomatization is **minimal**, meaning that none of its axiom can be removed without loosing completeness.

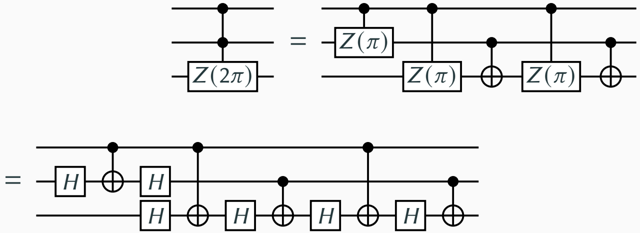
Theorem [CDP2024]

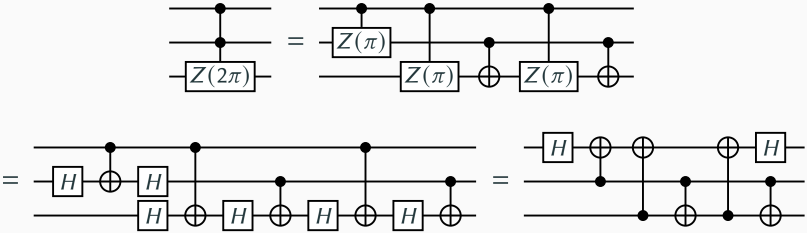
Any complete axiomatization must contain **at least one axiom involving n qubits** for any $n \in \mathbb{N}$.

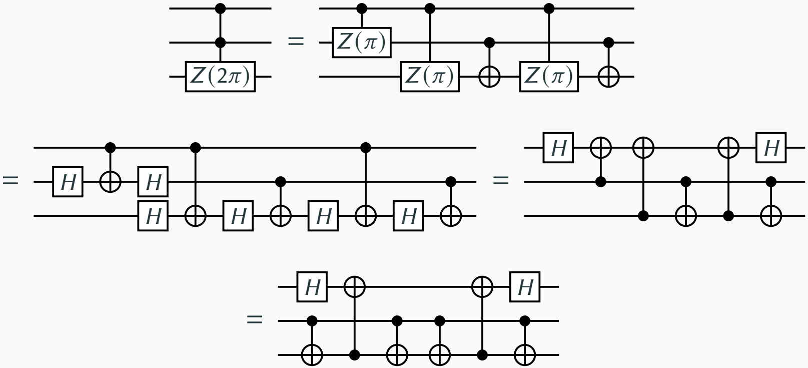
Controlled gates are everywhere.


$Z(2\pi)$

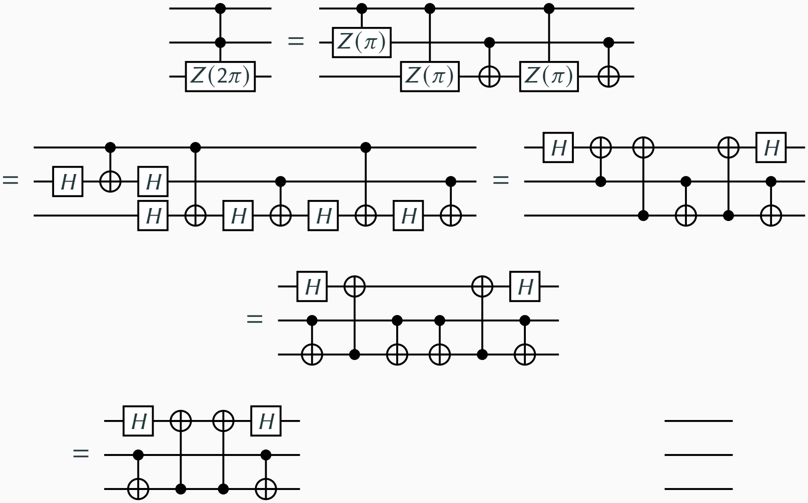

Z(2π)
=
Z(π)
Z(π)
Z(π)

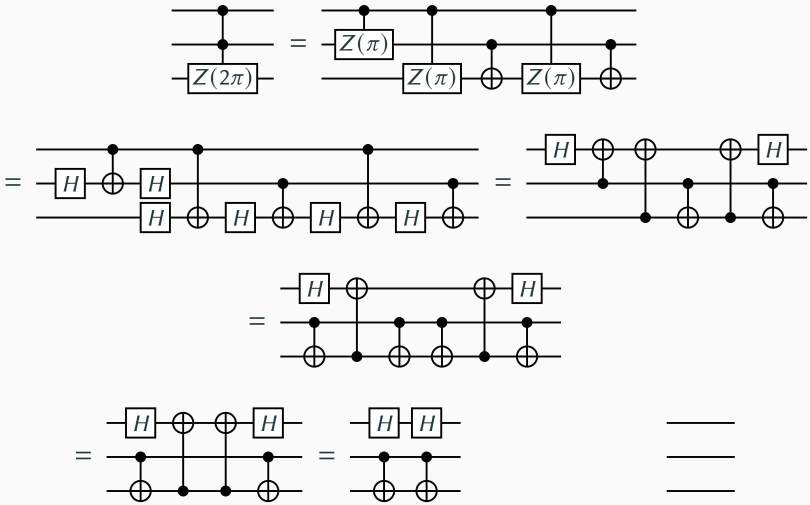

$Z(2\pi)$
=
$Z(\pi)$
$Z(\pi)$
$Z(\pi)$
=
H
H
H
H
H
H


Z(2π)
=
Z(π)
Z(π)
Z(π)
=
H
H
H
H
H
H
=
H
H

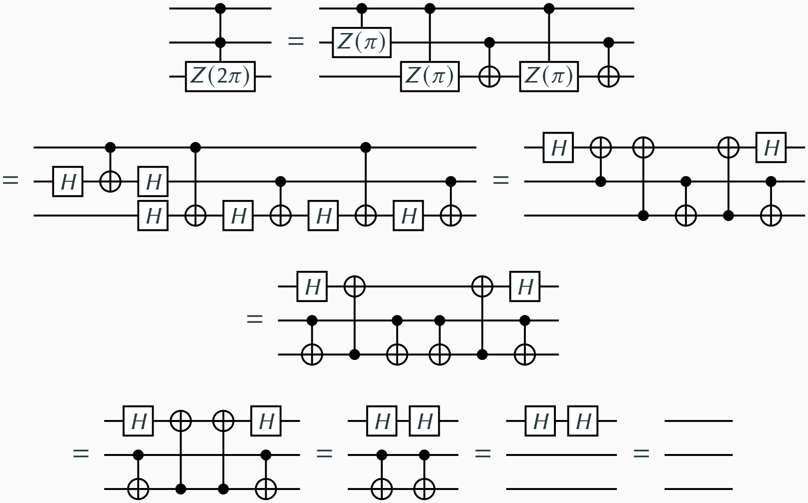


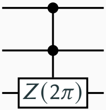
Z(2π)
=
Z(π)
Z(π)
Z(π)
=
H
H
H
H
H
H
=
H
H
=
H
H

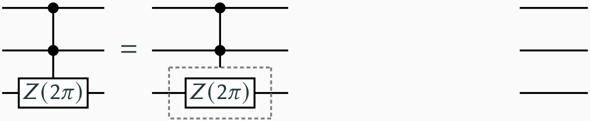

Z(2π)
=
Z(π)
Z(π)
Z(π)
=
H
H
H
H
H
H
=
H
H
=
H
H
=
H
H

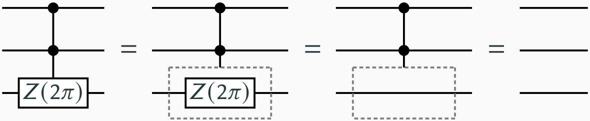


$Z(2\pi)$
$Z(\pi)$
$Z(\pi)$
$Z(\pi)$
H


Z(2π)
=
Z(π)
Z(π)
Z(π)
=
H
H
H
H
H
H
=
H
H
=
H
H
=
H
H
=
H
H
=
H
H
=


$Z(2\pi)$


Z(2π)
=
Z(2π)

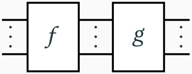

$Z(2\pi)$
=
$Z(2\pi)$
=
=

Controlled PROP

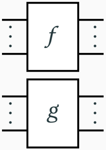
Definition

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

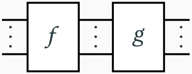
$$\frac{f : n \to p \quad g : p \to m}{f \mathbin{;} g : n \to m}$$



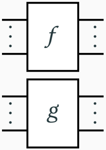
$$\frac{f : n \to m \quad g : p \to q}{f \otimes g : n + p \to m + q}$$



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

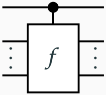


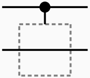
$$\frac{f : n \to m \quad g : p \to q}{f \otimes g : n + p \to m + q}$$

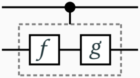


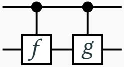
NEW!

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



$C(\mathrm{id}_1) =$  $=$  $= \mathrm{id}_2$

$C(f \fatsemi g) =$ 

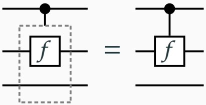
$=$ 

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

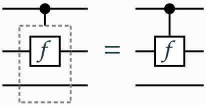
However, control functors are not monoidal.

$$C(f \otimes g) \neq C(f) \otimes C(g)$$

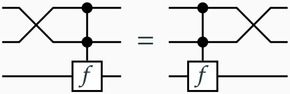
NEW!



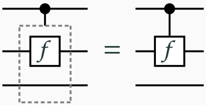
NEW!



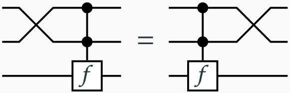
NEW!



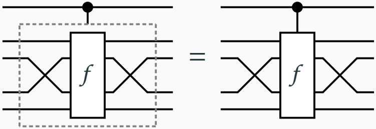
NEW!

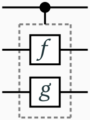


NEW!

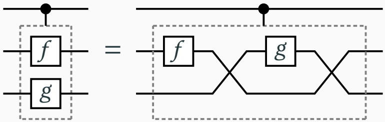


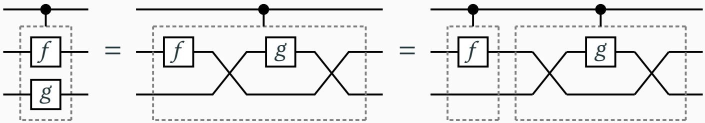
NEW!

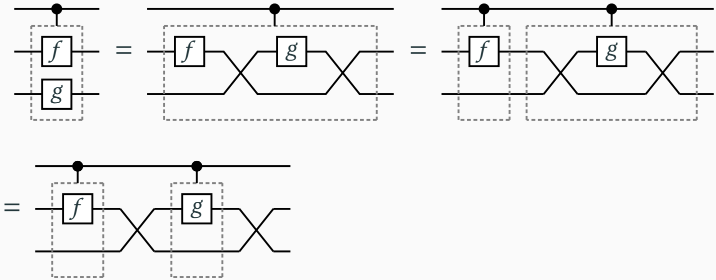


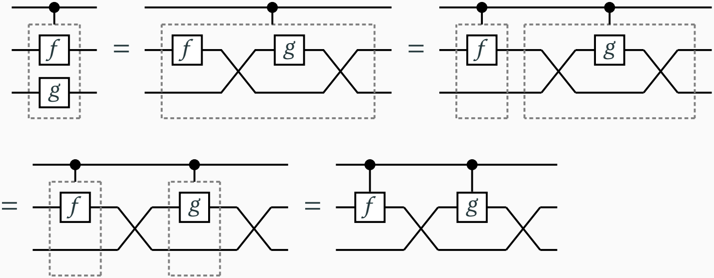


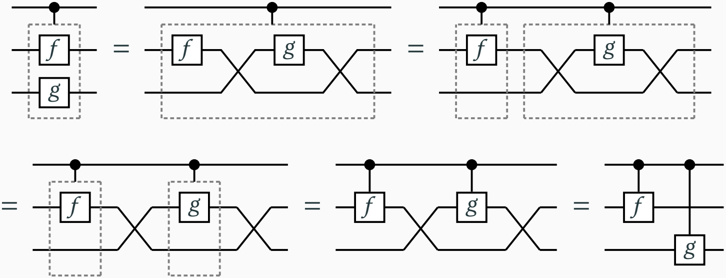
f
g

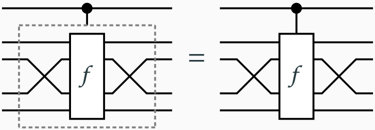

f
g
=
f
g

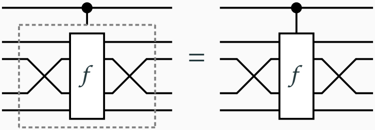

f
g
=
f
g
=
f
g


f
g
=
f
g
=
f
g
=
f
g


f
g
=
f
g
=
f
g
=
f
g
=
f
g

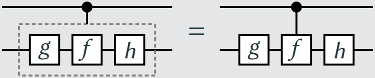

f
g
=
f
g
=
f
g
=
f
g
=
f
g
=
f
g

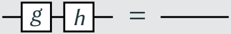

f
=
f



Definition

A **conjugated controlled PROP** is a controlled PROP satisfying the equation



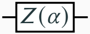
whenever 

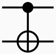
.

Controllable quantum circuits


α

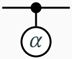

H

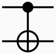

Z(α)




α

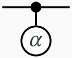

H

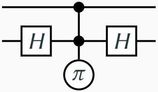

α



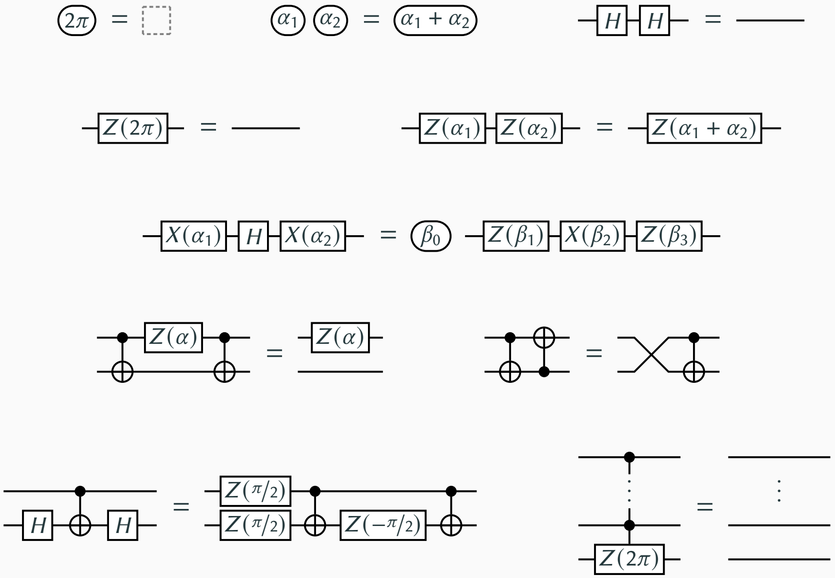

α

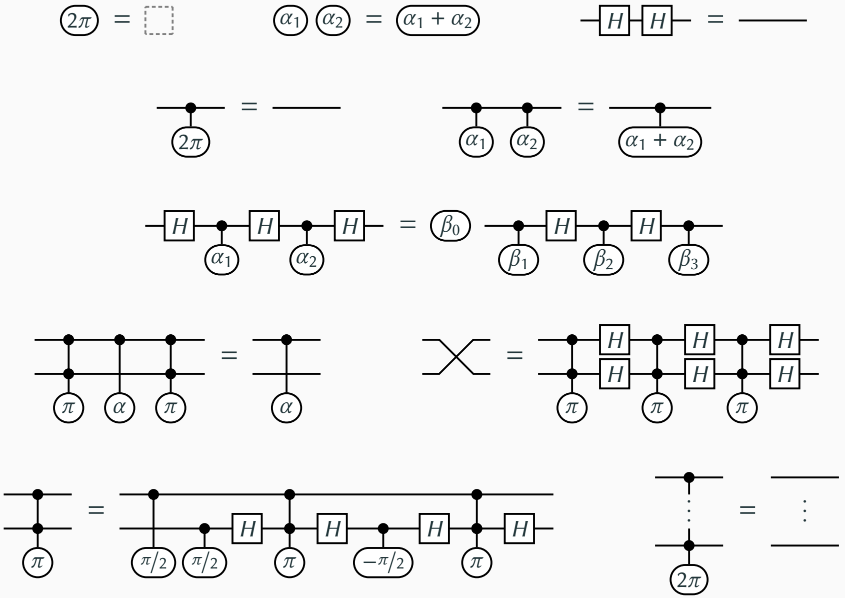

H


α

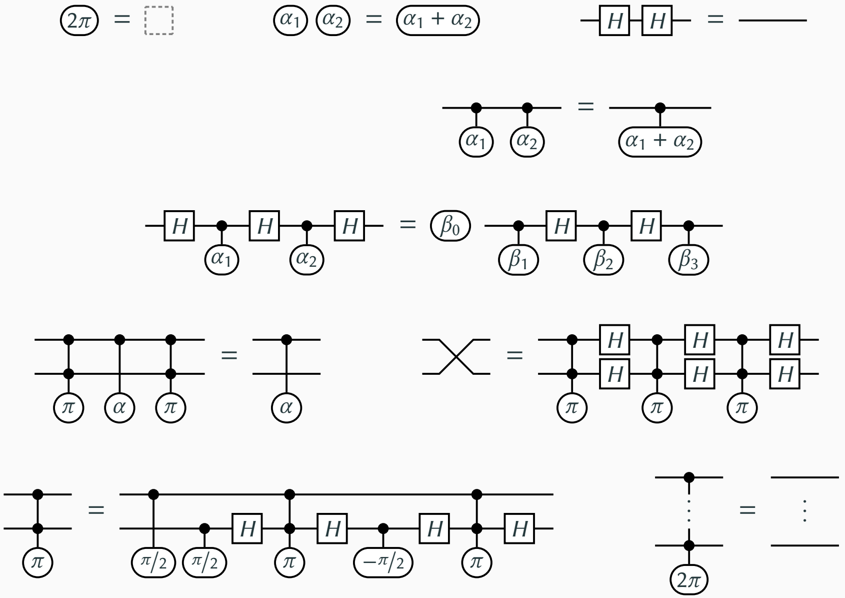

H
π
H

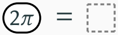
α $\quad\quad$ $-\boxed{H}-$

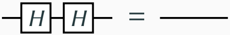

2π
α1 α2 α1 + α2
H H
Z(2π)
Z(α1) Z(α2) Z(α1 + α2)
X(α1) H X(α2) β0 Z(β1) X(β2) Z(β3)
Z(α) Z(α)
H H Z(π/2) Z(π/2) Z(−π/2)
Z(2π)

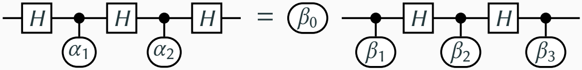


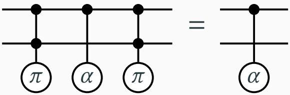
2π =
α1 α2 = α1 + α2
H H =
2π =
α1 α2 = α1 + α2
H α1 H α2 H = β0 β1 H β2 H β3
π α π = α
= π H H π H H π H H
π = π/2 π/2 H π H −π/2 H π H
2π =

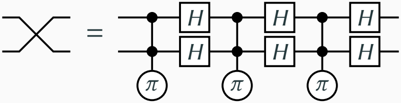


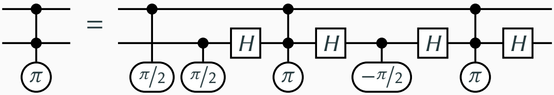


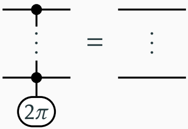


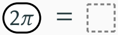




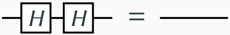


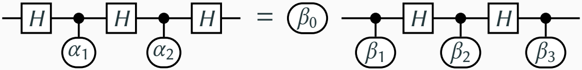


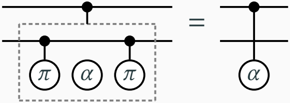


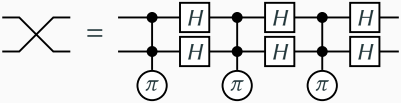

2π
=

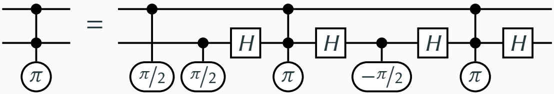

α1
α2
=
α1 + α2

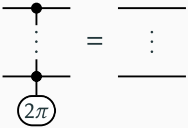

H
H
=

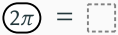

H
α1
H
α2
H
=
β0
β1
H
β2
H
β3

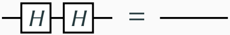

π
α
π
=
α

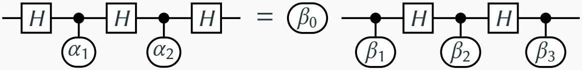

=
H
H
π
H
H
π
H
H
π

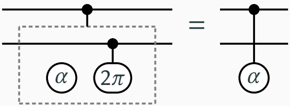

π
=
π/2
π/2
H
π
H
−π/2
H
π
H

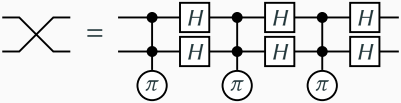

2π
=

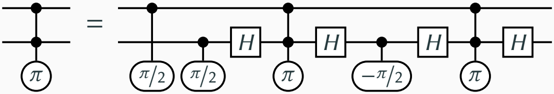


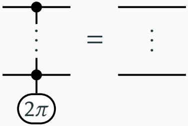


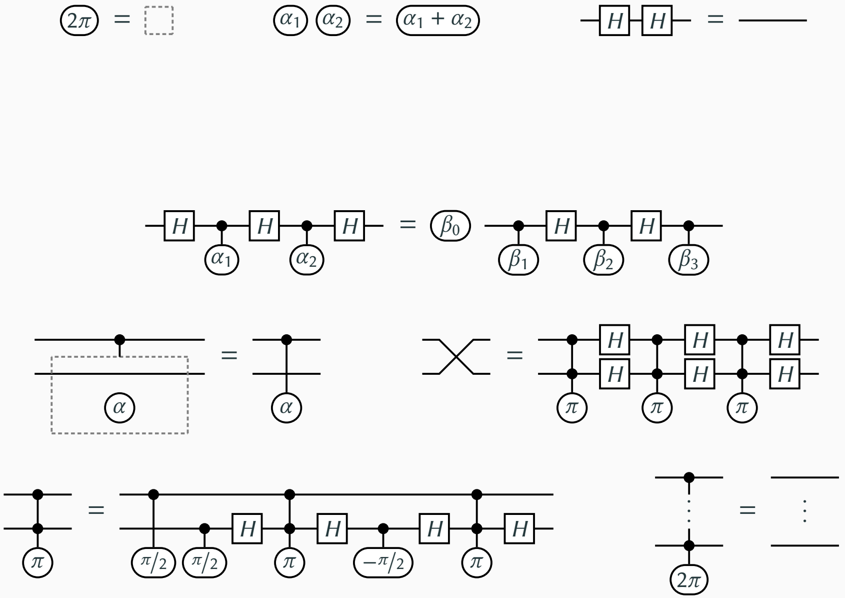




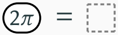




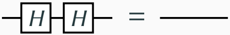


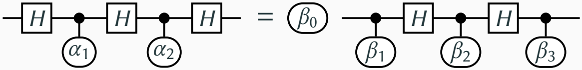


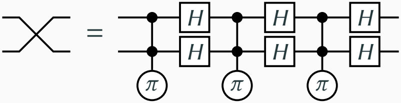
2π =
α_1 α_2 = $\alpha_1 + \alpha_2$
H H =
H α_1 H α_2 H = β_0 β_1 H β_2 H β_3
α = α
= π H H π H H π H H
π = $\pi/2$ $\pi/2$ H π H $-\pi/2$ H π H
2π =

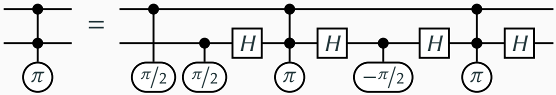

2π
=

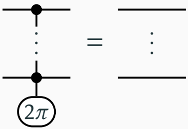

α1
α2
=
α1 + α2

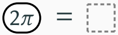

H
H
=


H
α1
H
α2
H
=
β0
β1
H
β2
H
β3

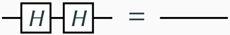

=
H
H
π
H
H
π
H
H
π

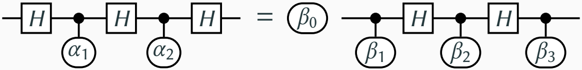

π
=
π/2
π/2
H
π
H
−π/2
H
π
H

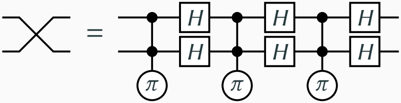

2π
=

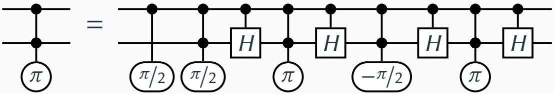

2π
=

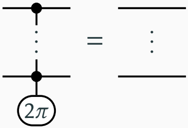

α1
α2
=
α1 + α2


H
H
=


H
α1
H
α2
H
=
β0
β1
H
β2
H
β3

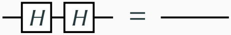

=
π
H
H
π
H
H
π
H
H

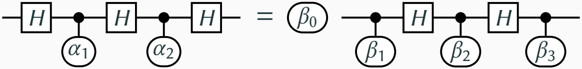

π
=
π/2
π/2
H
π
H
−π/2
H
π
H

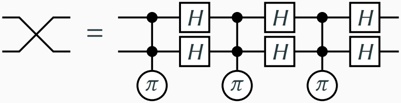

2π
=

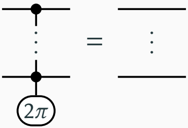

2π
=

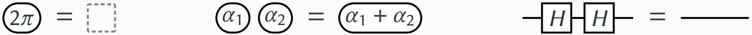

α1
α2
=
α1 + α2

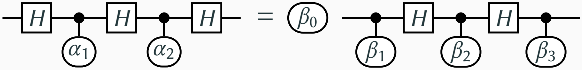

H
H
=

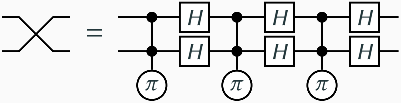

H
α1
H
α2
H
=
β0
β1
H
β2
H
β3


=
H
H
H
H
H
H
π
π
π

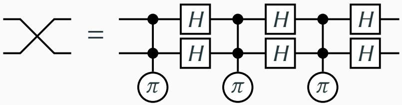

2π
=

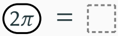


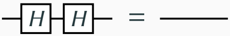


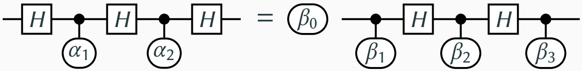


Complete axiomatization for quantum circuits defined as a conjugated controlled PROP.

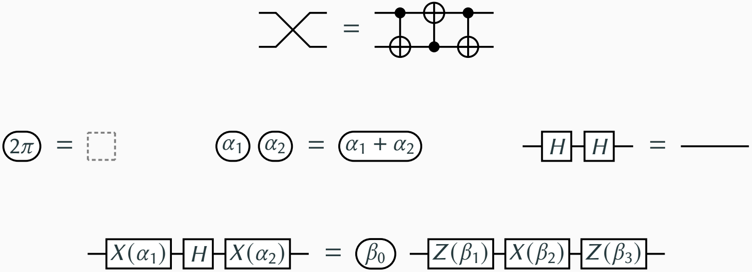




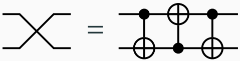


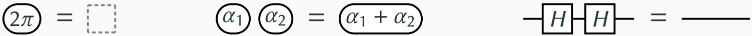


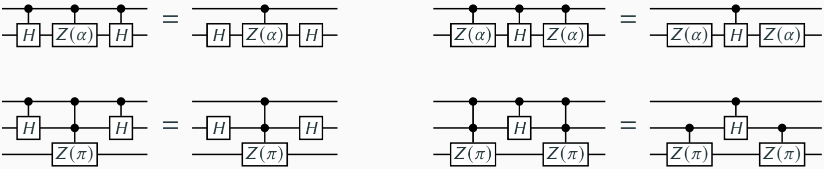
Complete axiomatization for quantum circuits defined as a conjugated controlled PROP.



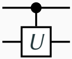
Complete axiomatization for quantum circuits defined as a controlled PROP.



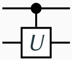




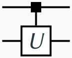
Versatility of the formalism

$[\![$  $]\!]$

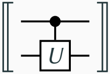
$$= \left(\begin{array}{c|c} \mathbb{I} & 0 \\ \hline 0 & U \end{array}\right)$$



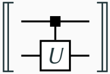
$$[\![\ \cdot\ ]\!] = \left(\begin{array}{c|c} \mathbb{I} & 0 \\ \hline 0 & U \end{array}\right)$$



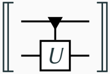
$$[\![\ \cdot\ ]\!] = \left(\begin{array}{c|c} U & 0 \\ \hline 0 & VUV^{\dagger} \end{array}\right)$$



$$= \left(\begin{array}{c|c} \mathbb{I} & 0 \\ \hline 0 & U \end{array}\right)$$

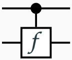
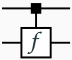


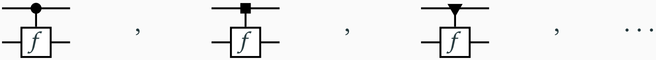
$$= \left(\begin{array}{c|c} U & 0 \\ \hline 0 & VUV^\dagger \end{array}\right)$$

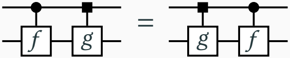


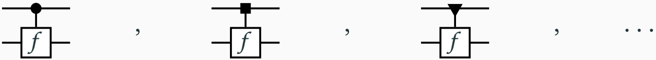
$$= \frac{1}{2}\left(\begin{array}{c|c} \mathbb{I}+U & \mathbb{I}-U \\ \hline \mathbb{I}-U & \mathbb{I}+U \end{array}\right)$$

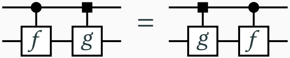
$\dots$

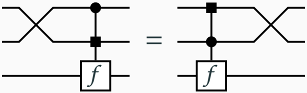
 ,  ,  , $\cdots$

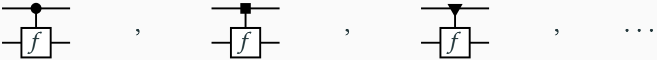

f
f
f

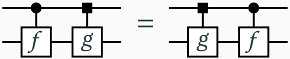

f
g
=
g
f

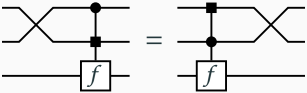

f
,
f
,
f
,
. . .

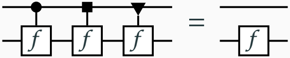

f
g
=
g
f


f
=
f









Controlled PROPs are a **clean** and **versatile** formalism

Controlled PROPs are a **clean** and **versatile** formalism featuring **control as a constructor**.

Controlled PROPs are a **clean** and **versatile** formalism featuring **control as a constructor**. Feel free to use them to express any kind of graphical language!

Controlled PROPs are a **clean** and **versatile** formalism featuring **control as a constructor**. Feel free to use them to express any kind of graphical language!

(arXiv:2508.21756)