Minimal Equational Theories for Quantum Circuits

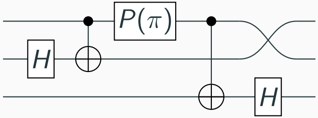
LICS'24 39th Annual ACM/IEEE Symposium on Logic in Computer Science

Alexandre Clément*, Noé Delorme† and Simon Perdrix†

*Université Paris-Saclay, ENS Paris-Saclay, CNRS, Inria, LMF, 91190, Gif-sur-Yvette, France
†Université de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, France

What is it all about?

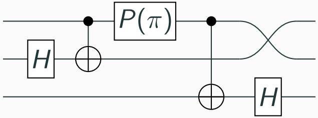
Quantum circuits are a rigourous graphical language used to represent quantum algorithms.



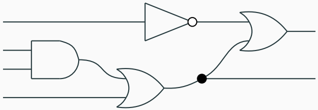
Just like boolean circuits are a rigourous graphical language used to represent classical algorithms.

What is it all about?

Quantum circuits are a rigourous graphical language used to represent quantum algorithms.



Just like boolean circuits are a rigourous graphical language used to represent classical algorithms.



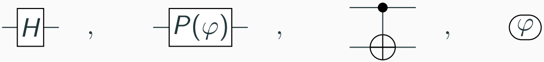
Quantum circuits as a graphical language

Quantum circuits are generated by

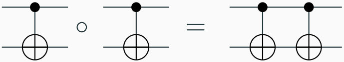
and can be composed sequentially with $\circ$ and in parallel with $\otimes$ as

to form new circuits.

Quantum circuits are generated by



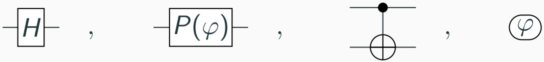
and can be composed sequentially with $\circ$ and in parallel with $\otimes$ as



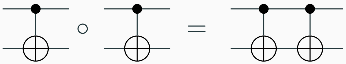
and

to form new circuits.

Quantum circuits are generated by

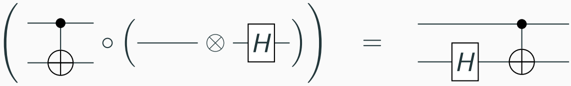


and can be composed sequentially with $\circ$ and in parallel with $\otimes$ as



and

to form new circuits.



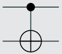
Standard interpretation of quantum circuits

Interpretation

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

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

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

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

circuits $\neq$ matrices

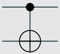
Standard interpretation of quantum circuits

Interpretation

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

$$[\![\ \square\ ]\!] = (1) \qquad [\![\ \varphi\ ]\!] = (e^{i\varphi})$$

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

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

circuits $\neq$ matrices

Quantum circuits as a graphical language

Formally, quantum circuits are defined as a symmetric monoidal category, which ensure some deformation equations such that

or

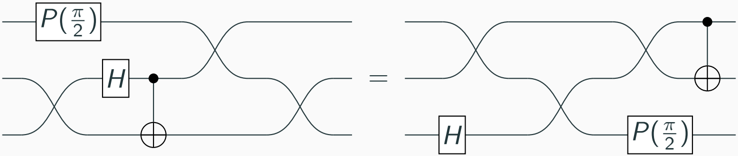
This framework captures the intuitive behaviour of wires by ensuring that circuits are defined "up to deformation".

Quantum circuits as a graphical language

Formally, quantum circuits are defined as a symmetric monoidal category, which ensure some deformation equations such that

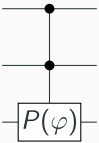
or

This framework captures the intuitive behaviour of wires by ensuring that circuits are defined "up to deformation".



Controlled gates as shortcut notations

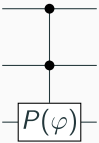
We use the standard bullet notation for controlled gates.



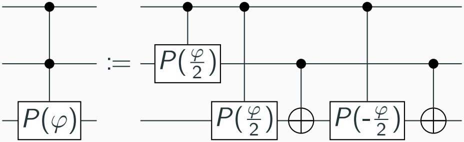
Controlled gates can be constructed inductively. The $(n + 1)$-controlled gate is a shortcut containing several instances of n-controlled gates.

Controlled gates as shortcut notations

We use the standard bullet notation for controlled gates.

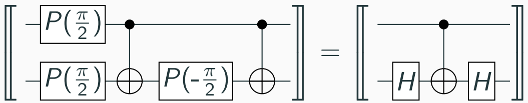


Controlled gates can be constructed inductively. The $(n+1)$-controlled gate is a shortcut containing several instances of n-controlled gates.



Motivations

Distinct circuits can have the same interpretation.



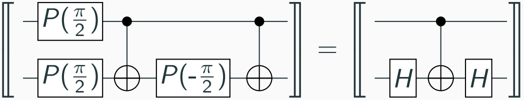
$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

Given a quantum algorithm, which circuit is the best?

Motivations:

- Resource optimisation (for instance the number of gates).
- Hardware-constraint satisfaction (for instance topological constraints).
- Verification, circuit equivalence testing.

Distinct circuits can have the same interpretation.



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

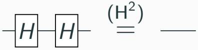
Given a quantum algorithm, which circuit is the best?

Motivations:

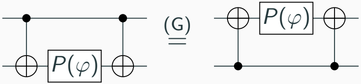
- Resource optimisation (for instance the number of gates).
- Hardware-constraint satisfaction (for instance topological constraints).
- Verification, circuit equivalence testing.

Using equations to transform circuits

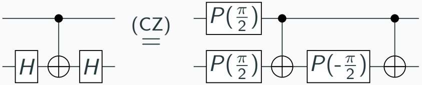
We can use simple equations such that,



,



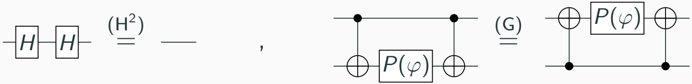
and



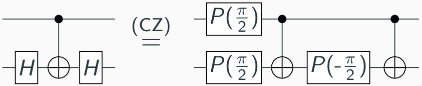
to derive new equations. For instance,

Using equations to transform circuits

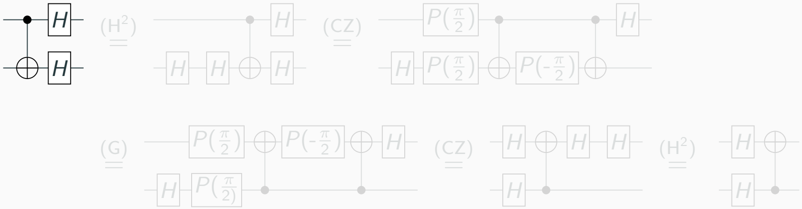
We can use simple equations such that,



and

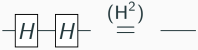


to derive new equations. For instance,

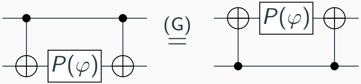


Using equations to transform circuits

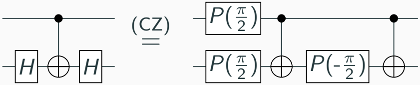
We can use simple equations such that,



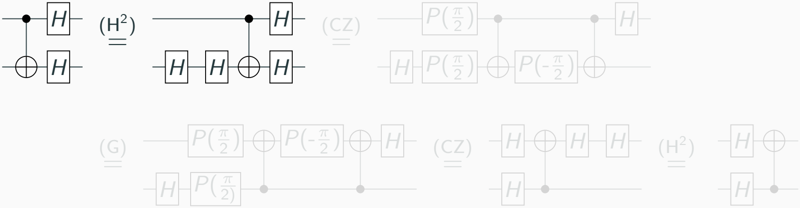
,



and

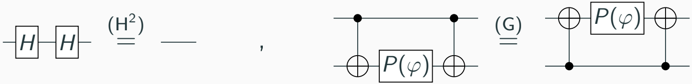


to derive new equations. For instance,

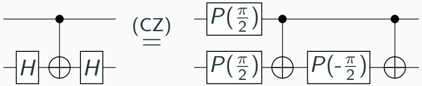


Using equations to transform circuits

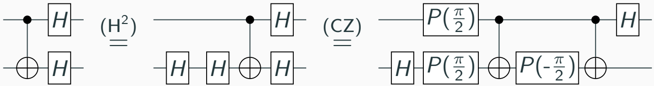
We can use simple equations such that,



and

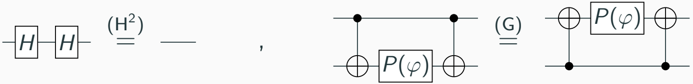


to derive new equations. For instance,

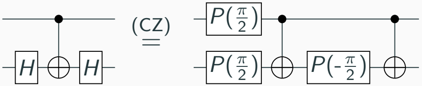


Using equations to transform circuits

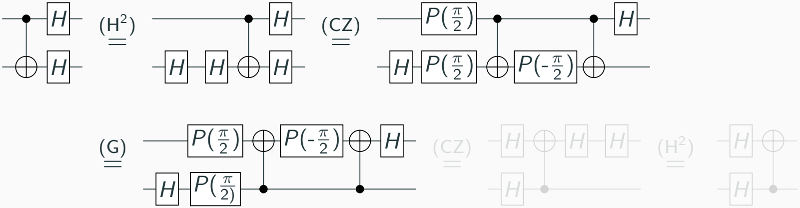
We can use simple equations such that,



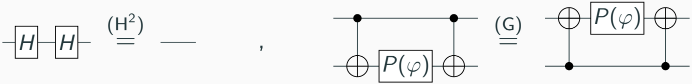
and



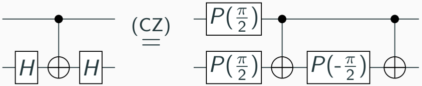
to derive new equations. For instance,



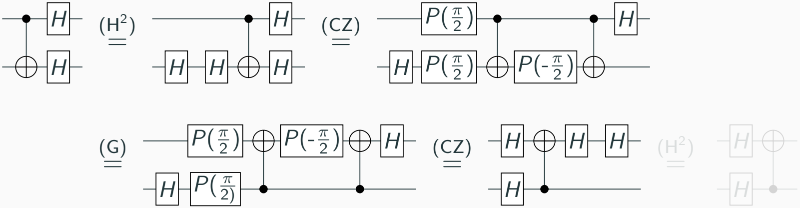
We can use simple equations such that,



and

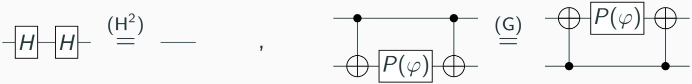


to derive new equations. For instance,

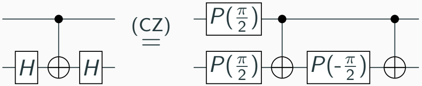


Using equations to transform circuits

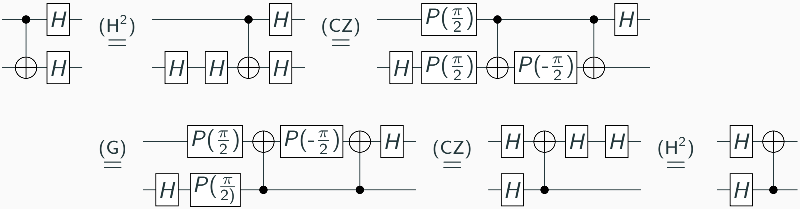
We can use simple equations such that,



and



to derive new equations. For instance,



Complete and sound equational theory

Is there an equational theory (i.e. a set of axioms) Γ from which we can derive any true equation and only true equations?

Soundness

Any derivable equation is true.

$$\forall C_1, C_2 \quad : \quad \Gamma \vdash C_1 = C_2 \implies [\![C_1]\!] = [\![C_2]\!]$$

Completeness

Any true equation is derivable.

$$\forall C_1, C_2 \quad : \quad [\![C_1]\!] = [\![C_2]\!] \implies \Gamma \vdash C_1 = C_2$$

Previous work [Clément,Heurtel,Mansfield,Perdrix,Valiron LICS'23]:

The first complete and sound equational theory.

Complete and sound equational theory

Is there an equational theory (i.e. a set of axioms) Γ from which we can derive any true equation and only true equations?

Soundness

Any derivable equation is true.

$\forall C_1, C_2 \quad : \quad \Gamma \vdash C_1 = C_2 \implies [\![C_1]\!] = [\![C_2]\!]$

Completeness

Any true equation is derivable.

$\forall C_1, C_2 \quad : \quad [\![C_1]\!] = [\![C_2]\!] \implies \Gamma \vdash C_1 = C_2$

Previous work [Clément,Heurtel,Mansfield,Perdrix,Valiron LICS'23]:

The first complete and sound equational theory.

Complete and sound equational theory

Is there an equational theory (i.e. a set of axioms) Γ from which we can derive any true equation and only true equations?

Soundness

Any derivable equation is true.
$\forall C_1, C_2 \quad : \quad \Gamma \vdash C_1 = C_2 \implies [\![C_1]\!] = [\![C_2]\!]$

Completeness

Any true equation is derivable.
$\forall C_1, C_2 \quad : \quad [\![C_1]\!] = [\![C_2]\!] \implies \Gamma \vdash C_1 = C_2$

Previous work [Clément,Heurtel,Mansfield,Perdrix,Valiron LICS'23]:
The first complete and sound equational theory.

Complete and sound equational theory

Is there an equational theory (i.e. a set of axioms) Γ from which we can derive any true equation and only true equations?

Soundness

Any derivable equation is true.

$\forall C_1, C_2 \quad : \quad \Gamma \vdash C_1 = C_2 \implies [\![C_1]\!] = [\![C_2]\!]$

Completeness

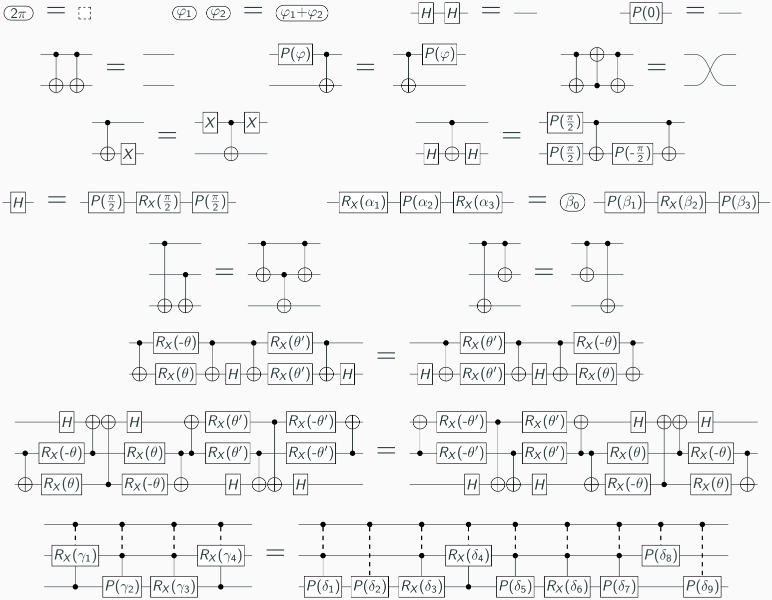
Any true equation is derivable.

$\forall C_1, C_2 \quad : \quad [\![C_1]\!] = [\![C_2]\!] \implies \Gamma \vdash C_1 = C_2$

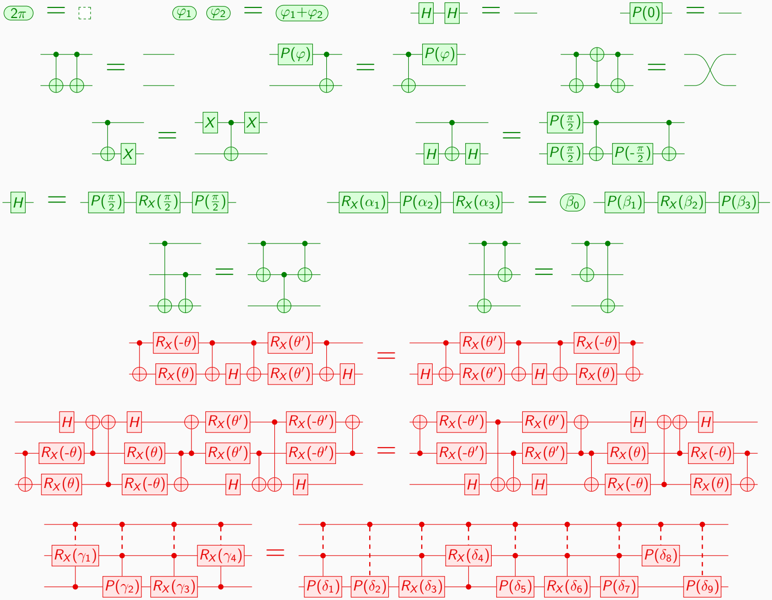
Previous work [Clément,Heurtel,Mansfield,Perdrix,Valiron LICS'23]:

The first complete and sound equational theory.

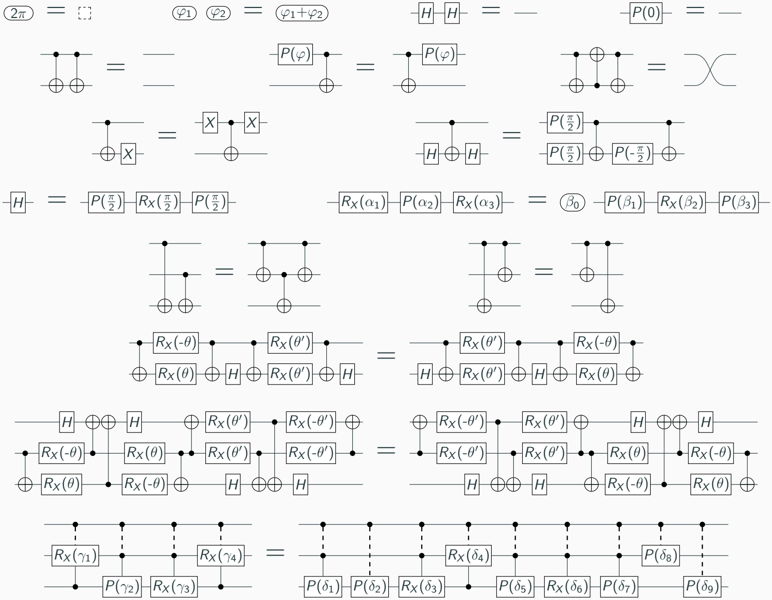
Complete and sound equational theory [CHMPV LICS'23]



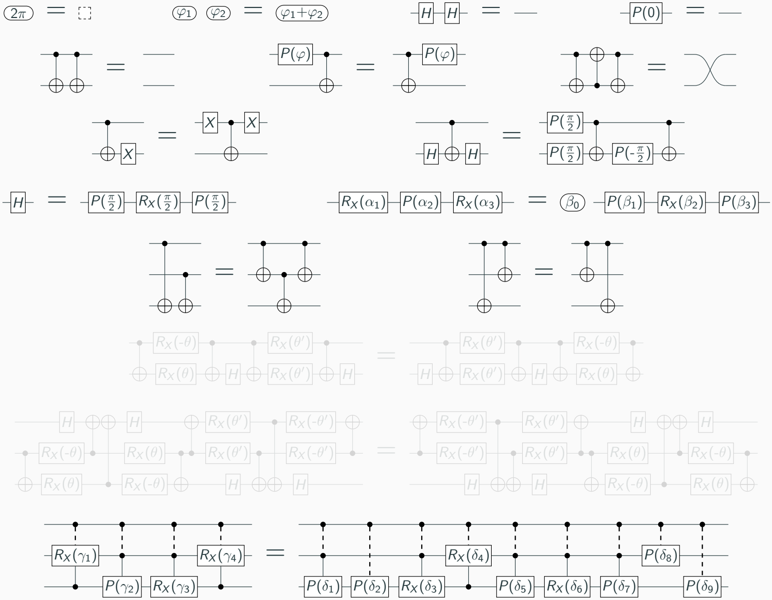
Some easy and some intricate equations



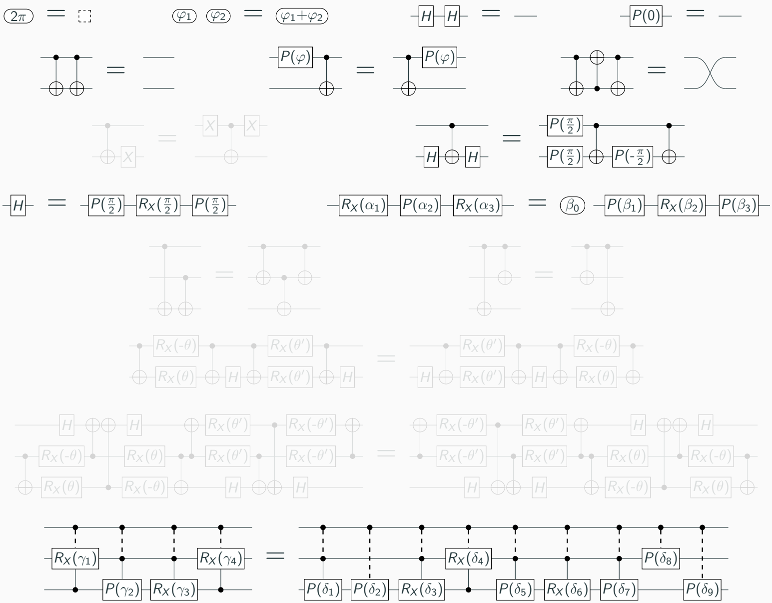
Simplifications [CDPV CSL'24 , CDP LICS'24]



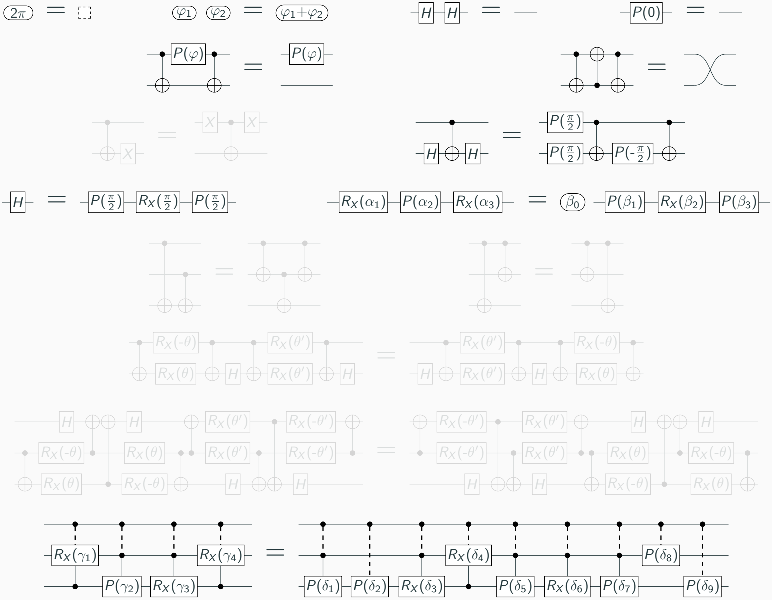
Simplifications [CDPV CSL'24 , CDP LICS'24]



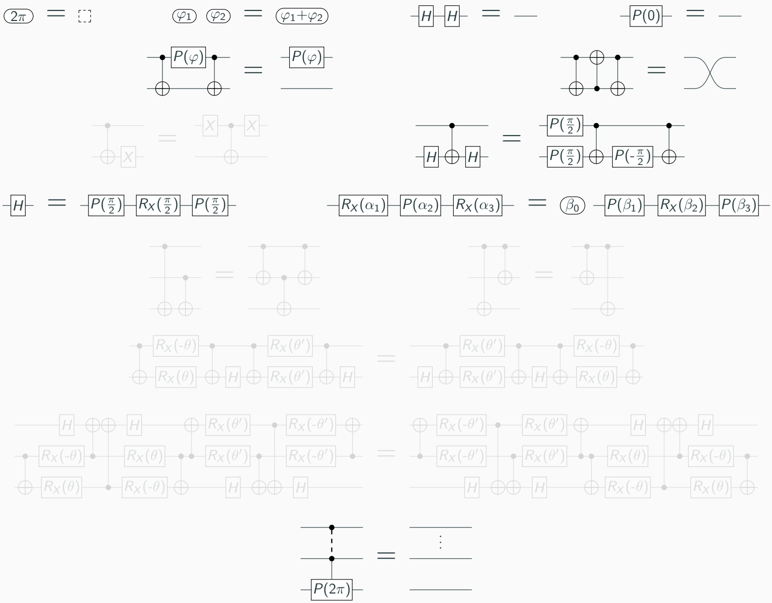
Simplifications [CDPV CSL'24 , CDP LICS'24]



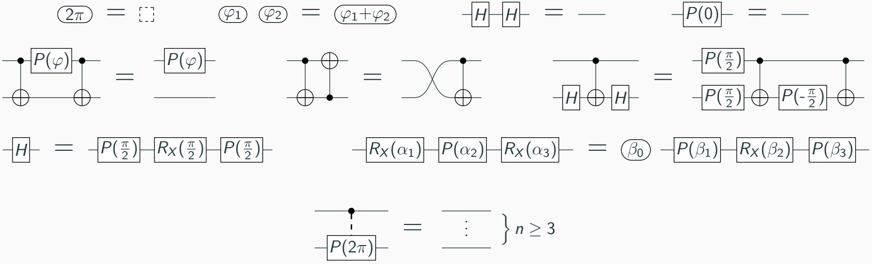
Simplifications [CDPV CSL'24 , CDP LICS'24]



Simplifications [CDPV CSL'24 , CDP LICS'24]



Towards the limit of simplifications



Question: Can we simplify the equational theory even more?

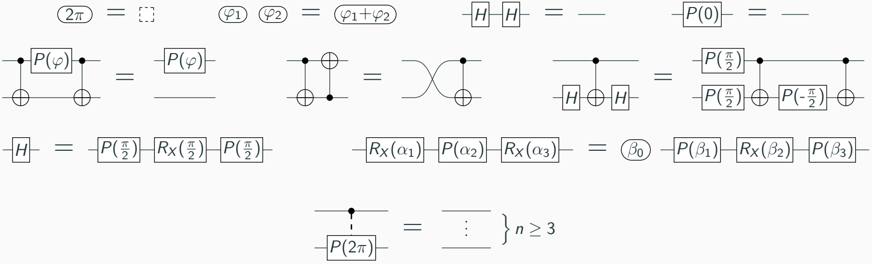
Theorem

This equational theory is complete, sound and minimal.

Minimality

All equations are independents.

$\forall (C_1 = C_2) \in \Gamma \quad : \quad \Gamma \backslash \{C_1 = C_2\} \nvdash C_1 = C_2$



Question: Can we simplify the equational theory even more?

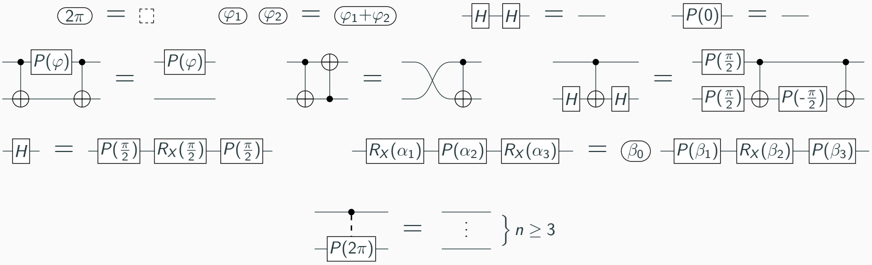
Theorem

This equational theory is complete, sound and minimal.

Minimality

All equations are independents.

$$\forall (C_1 = C_2) \in \Gamma \quad : \quad \Gamma \backslash \{C_1 = C_2\} \nvdash C_1 = C_2$$



Question: Can we simplify the equational theory even more?

Theorem

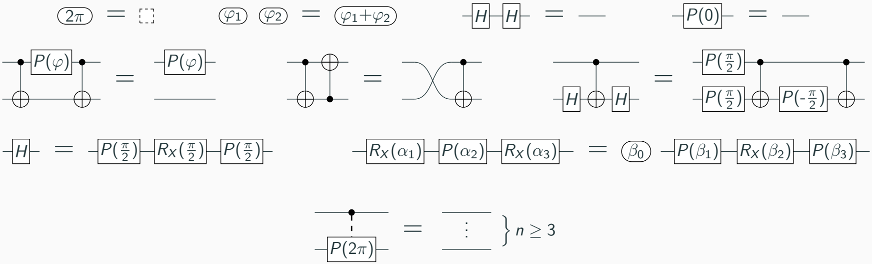
This equational theory is complete, sound and minimal.

Minimality

All equations are independents.

$\forall (C_1 = C_2) \in \Gamma \quad : \quad \Gamma \setminus \{C_1 = C_2\} \nvdash C_1 = C_2$

Towards the limit of simplifications



Question: Can we simplify the equational theory even more?

Theorem

This equational theory is complete, sound and minimal.

Minimality

All equations are independents.

$\forall (C_1 = C_2) \in \Gamma \quad : \quad \Gamma \backslash \{C_1 = C_2\} \nvdash C_1 = C_2$

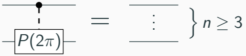
Unboundedness of the equational theory

Every instances of  $n \geq 3$ are necessary (for every $n \geq 3$).

Theorem

There is no complete equational theory for quantum circuits made of equations acting on a bounded number of wires.

More precisely, any complete equational theory for quantum circuits has at least one equation acting on n wires for any $n \in \mathbb{N}$.

Every instances of  are necessary (for every $n \geq 3$).

Theorem

There is no complete equational theory for quantum circuits made of equations acting on a bounded number of wires.

More precisely, any complete equational theory for quantum circuits has at least one equation acting on n wires for any $n \in \mathbb{N}$.

Unboundedness of the equational theory

Every instances of  $n \geq 3$ are necessary (for every $n \geq 3$).

Theorem

There is no complete equational theory for quantum circuits made of equations acting on a bounded number of wires.

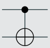
More precisely, any complete equational theory for quantum circuits has at least one equation acting on n wires for any $n \in \mathbb{N}$.

Alternative interpretation

For any $k \in \mathbb{N}$, for any quantum circuit C, let $[\![C]\!]_k^\sharp \in [0, 2\pi)$ be inductively defined as

$$[\![C_2 \circ C_1]\!]_k^\sharp = [\![C_1 \otimes C_2]\!]_k^\sharp = [\![C_2]\!]_k^\sharp + [\![C_1]\!]_k^\sharp \bmod 2\pi$$

$$[\![\,\fbox{}\,]\!]_k^\sharp = [\![\,-\!\!-\!\!-\,]\!]_k^\sharp = 0 \qquad [\![\,\textcircled{\varphi}\,]\!]_k^\sharp = 2^k\varphi \bmod 2\pi \qquad [\![\,-\boxed{H}-\,]\!]_k^\sharp = 2^{k-1}\pi \bmod 2\pi$$

$[\![$  $]\!]_k^\sharp = [\![$  $]\!]_k^\sharp = 2^{k-2}\pi \bmod 2\pi \qquad [\![\,-\boxed{P(\varphi)}-\,]\!]_k^\sharp = 2^{k-1}\varphi \bmod 2\pi$

Any sound equation involving circuits acting on at most $n-1$ wires is also sound according to $[\![\cdot]\!]_{n-1}^\sharp$.

However,

$[\![$

$]\!]_{n-1}^\sharp = \pi \neq 0 = [\![$

$]\!]_{n-1}^\sharp$

Proof sketch

Alternative interpretation

For any $k \in \mathbb{N}$, for any quantum circuit C, let $\llbracket C \rrbracket^\sharp_k \in [0, 2\pi)$ be inductively defined as

$$\llbracket C_2 \circ C_1 \rrbracket^\sharp_k = \llbracket C_1 \otimes C_2 \rrbracket^\sharp_k = \llbracket C_2 \rrbracket^\sharp_k + \llbracket C_1 \rrbracket^\sharp_k \mod 2\pi$$

$$\llbracket \boxed{} \rrbracket^\sharp_k = \llbracket \text{---} \rrbracket^\sharp_k = 0 \qquad \llbracket \varphi \rrbracket^\sharp_k = 2^k \varphi \mod 2\pi \qquad \llbracket \text{-}\boxed{H}\text{-} \rrbracket^\sharp_k = 2^{k-1}\pi \mod 2\pi$$

$$\left\llbracket \begin{smallmatrix} \bullet \\ | \\ \oplus \end{smallmatrix} \right\rrbracket^\sharp_k = \left\llbracket \times \right\rrbracket^\sharp_k = 2^{k-2}\pi \mod 2\pi \qquad \llbracket \text{-}\boxed{P(\varphi)}\text{-} \rrbracket^\sharp_k = 2^{k-1}\varphi \mod 2\pi$$

Any sound equation involving circuits acting on at most $n-1$ wires is also sound according to $\llbracket \cdot \rrbracket^\sharp_{n-1}$.

However,

$$\left\llbracket \left.\begin{smallmatrix} \bullet \\ \vdots \\ \boxed{P(2\pi)} \end{smallmatrix}\right\}n \right\rrbracket^\sharp_{n-1} = \pi \neq 0 = \left\llbracket \left.\begin{smallmatrix} \text{---} \\ \vdots \\ \text{---} \end{smallmatrix}\right\}n \right\rrbracket^\sharp_{n-1}$$

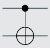
Proof sketch

Alternative interpretation

For any $k \in \mathbb{N}$, for any quantum circuit C, let $[\![C]\!]^\sharp_k \in [0, 2\pi)$ be inductively defined as

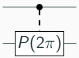
$$[\![C_2 \circ C_1]\!]^\sharp_k = [\![C_1 \otimes C_2]\!]^\sharp_k = [\![C_2]\!]^\sharp_k + [\![C_1]\!]^\sharp_k \bmod 2\pi$$

$[\![\,\fbox{}\,]\!]^\sharp_k = [\![\,-\!\!-\!\!-\,]\!]^\sharp_k = 0 \qquad [\![\,(\varphi)\,]\!]^\sharp_k = 2^k\varphi \bmod 2\pi \qquad [\![\,-\boxed{H}-\,]\!]^\sharp_k = 2^{k-1}\pi \bmod 2\pi$

$[\![$  $]\!]^\sharp_k = [\![$  $]\!]^\sharp_k = 2^{k-2}\pi \bmod 2\pi \qquad [\![\,-\boxed{P(\varphi)}-\,]\!]^\sharp_k = 2^{k-1}\varphi \bmod 2\pi$

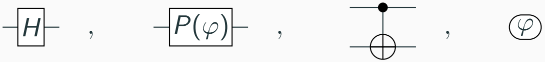
Any sound equation involving circuits acting on at most $n-1$ wires is also sound according to $[\![\cdot]\!]^\sharp_{n-1}$.

However,

$[\![$  $\Big\}\, n \,]\!]^\sharp_{n-1} \;=\; \pi \;\neq\; 0 \;=\; [\![$  $\Big\}\, n \,]\!]^\sharp_{n-1}$

Extension to quantum circuits with ancillae

Quantum circuits with ancillae are generated by



together with

$$\vdash \quad \text{and} \quad \dashv$$

respectively denoting wire initialisation and wire termination.

(The generator $\dashv$ can only be applied to wires in the $|0\rangle$-state.)

Semantics

We extend $[\![\cdot]\!]$ with $[\![\vdash]\!] = |0\rangle$ and $[\![\dashv]\!] = \langle 0|$.

Universal for isometries

Extension to quantum circuits with ancillae

Quantum circuits with ancillae are generated by

together with

$$\vdash \quad \text{and} \quad \dashv$$

respectively denoting wire initialisation and wire termination.

(The generator $\dashv$ can only be applied to wires in the $|0\rangle$-state.)

Semantics

We extend $[\![\cdot]\!]$ with $[\![\vdash]\!] = |0\rangle$ and $[\![\dashv]\!] = \langle 0|$.

Universal for isometries

Extension to quantum circuits with ancillae

Quantum circuits with ancillae are generated by

together with

$$\vdash \quad \text{and} \quad \dashv$$

respectively denoting wire initialisation and wire termination.

(The generator $\dashv$ can only be applied to wires in the $|0\rangle$-state.)

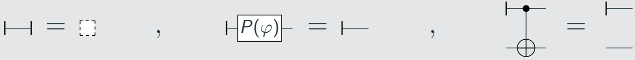
Semantics

We extend $[\![\cdot]\!]$ with $[\![\vdash]\!] = |0\rangle$ and $[\![\dashv]\!] = \langle 0|$.

Universal for isometries

Theorem [CDPV CSL'24]

Adding those three equations makes the equational theory complete for quantum circuits with ancillae.



Using ancillae, we can build controlled gates without dividing the angles.

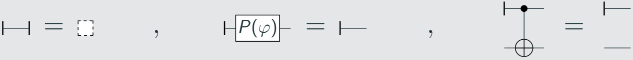
In these more general settings, is derivable for $n \geq 4$.

Hence, using ancillae, there is a complete equational theory made of equations acting on at most 3 wires.

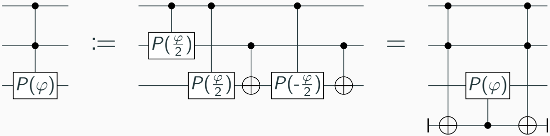
Boundedness of the equational theory with ancillae

Theorem [CDPV CSL'24]

Adding those three equations makes the equational theory complete for quantum circuits with ancillae.



Using ancillae, we can build controlled gates without dividing the angles.



In these more general settings,

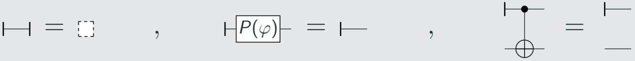
is derivable for $n \geq 4$.

Hence, using ancillae, there is a complete equational theory made of equations acting on at most 3 wires.

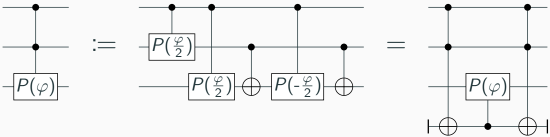
Boundedness of the equational theory with ancillae

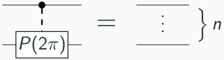
Theorem [CDPV CSL'24]

Adding those three equations makes the equational theory complete for quantum circuits with ancillae.



Using ancillae, we can build controlled gates without dividing the angles.



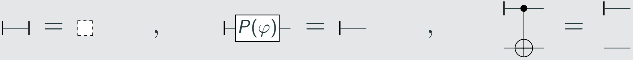
In these more general settings, 

is derivable for $n \geq 4$.

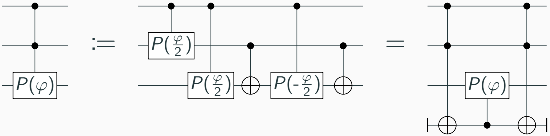
Hence, using ancillae, there is a complete equational theory made of equations acting on at most 3 wires.

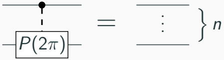
Theorem [CDPV CSL'24]

Adding those three equations makes the equational theory complete for quantum circuits with ancillae.



Using ancillae, we can build controlled gates without dividing the angles.



In these more general settings, 

is derivable for $n \geq 4$.

Hence, using ancillae, there is a complete equational theory made of equations acting on at most 3 wires.

Thanks

arXiv:2311.07476

Minimal Equational Theories for Quantum Circuits

Alexandre Clément, Noé Delorme and Simon Perdrix