Minimal Equational Theories for Quantum Circuits

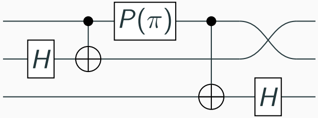
16th July 2024 - QPL'24

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?

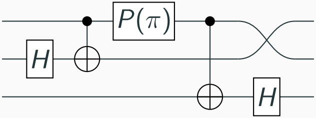
Quantum circuits are a rigourous graphical language used to represent quantum algorithms.



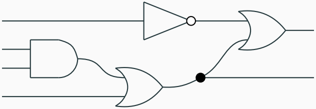
Just like boolean circuits are a rigourous graphical language used to represent classical algorithms.

What is it all about?

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

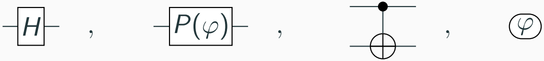


Just like boolean circuits are a rigourous graphical language used to represent classical algorithms.



Quantum circuits as a graphical language

Quantum circuits are generated by the universal gateset



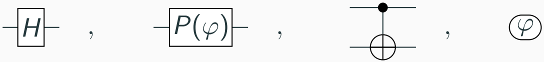
and can be composed sequentially with ∘ and in parallel with ⊗ as

and

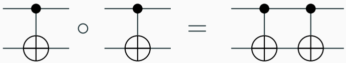
to form new circuits.

Quantum circuits as a graphical language

Quantum circuits are generated by the universal gateset



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

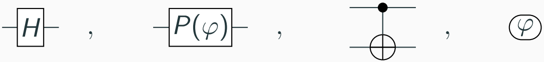


and

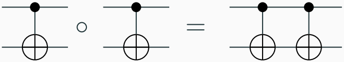
to form new circuits.

Quantum circuits as a graphical language

Quantum circuits are generated by the universal gateset

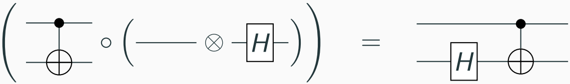


and can be composed sequentially with ∘ and in parallel with ⊗ as



and

to form new circuits.



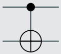
Standard interpretation of quantum circuits

Interpretation

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

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

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

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

circuits $\neq$ matrices

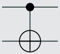
Standard interpretation of quantum circuits

Interpretation

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

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

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

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

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

$$\text{circuits} \neq \text{matrices}$$

Definition "up to deformation"

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

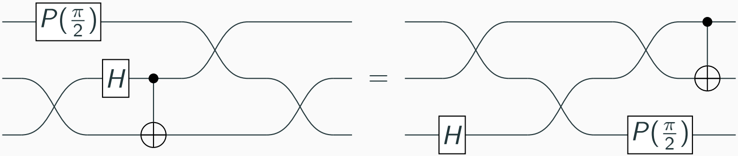
or

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

Definition “up to deformation”

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

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



Other gates as shortcut notations

Other usual gates can be defined as shortcut notation by composition of the generators.

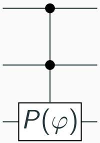
$$-\boxed{Z}- \;:=\; -\boxed{P(\pi)}-$$

$$-\boxed{X}- \;:=\; -\boxed{H}-\boxed{Z}-\boxed{H}-$$

$$-\boxed{R_X(\theta)}- \;:=\; \left(\,{}^{-\theta}\!/_{2}\,\right)\; -\boxed{H}-\boxed{P(\theta)}-\boxed{H}-$$

Controlled gates as shortcut notations

We use the standard bullet notation for controlled gates.

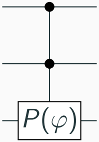


Controlled gates can be constructed inductively. The $(n+1)$-controlled gate is a shortcut containing several instances of n-controlled gates.

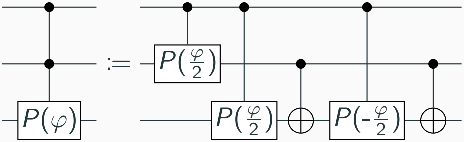
Note that unfolding the inductive definition divides the parameters by 2.

Controlled gates as shortcut notations

We use the standard bullet notation for controlled gates.



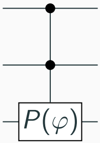
Controlled gates can be constructed inductively. The $(n+1)$-controlled gate is a shortcut containing several instances of n-controlled gates.



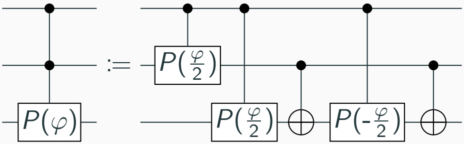
Note that unfolding the inductive definition divides the parameters by 2.

Controlled gates as shortcut notations

We use the standard bullet notation for controlled gates.



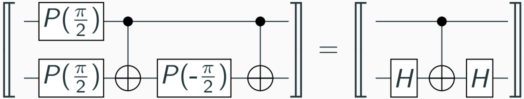
Controlled gates can be constructed inductively. The $(n+1)$-controlled gate is a shortcut containing several instances of n-controlled gates.



Note that unfolding the inductive definition divides the parameters by 2.

Motivations

Distinct circuits can have the same interpretation.



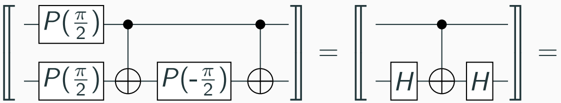
$$
= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}
$$

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.



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

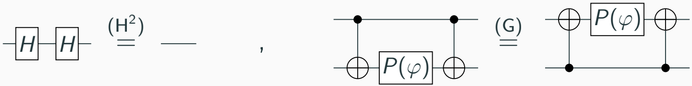
Given a quantum algorithm, which circuit is the best?

Motivations:

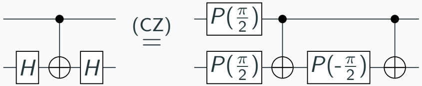
- Resource optimisation (for instance the number of gates).
- Hardware-constraint satisfaction (for instance topological constraints).
- Verification, circuit equivalence testing.

Using equations to transform circuits

We can use simple equations such that,



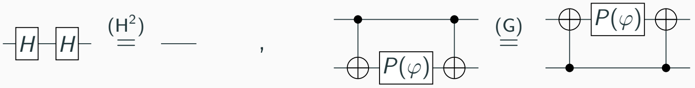
and



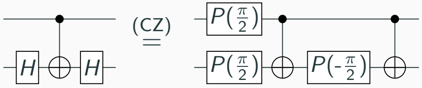
to derive new equations. For instance,

Using equations to transform circuits

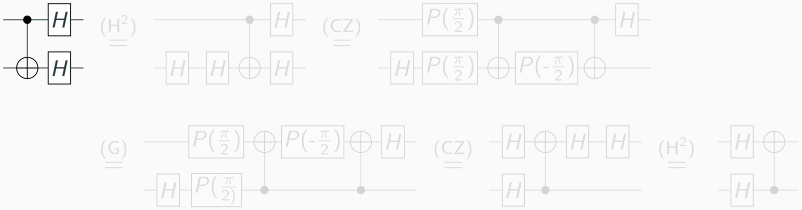
We can use simple equations such that,



and

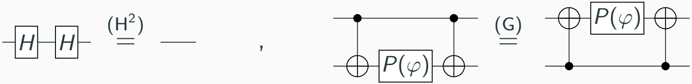


to derive new equations. For instance,

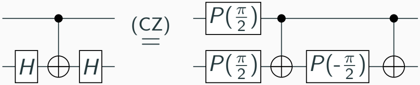


Using equations to transform circuits

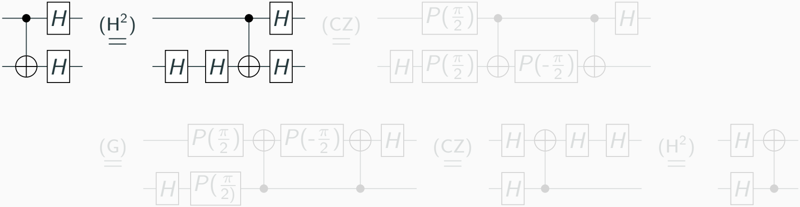
We can use simple equations such that,



and

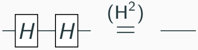


to derive new equations. For instance,

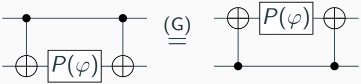


Using equations to transform circuits

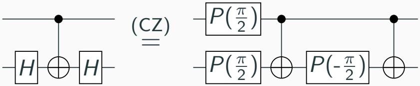
We can use simple equations such that,



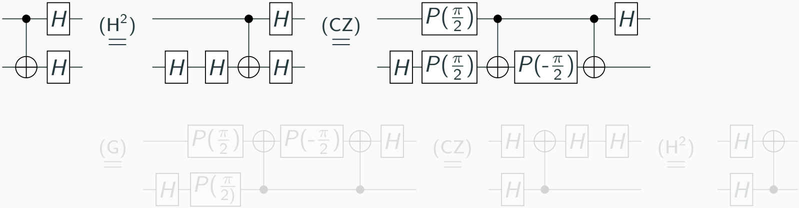
,



and

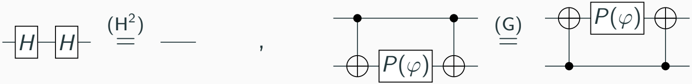


to derive new equations. For instance,

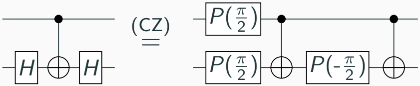


Using equations to transform circuits

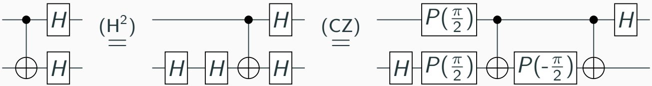
We can use simple equations such that,



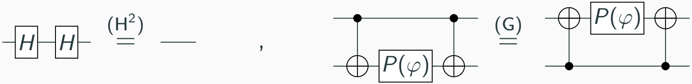
and



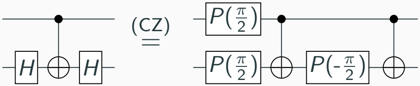
to derive new equations. For instance,



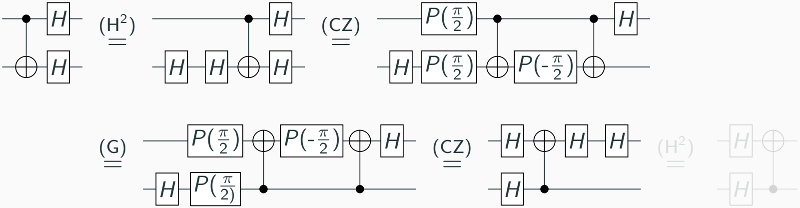
We can use simple equations such that,



and

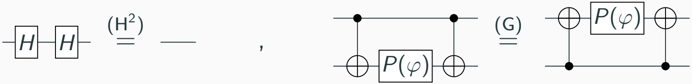


to derive new equations. For instance,

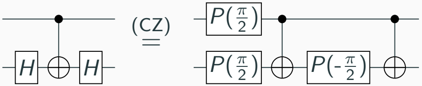


Using equations to transform circuits

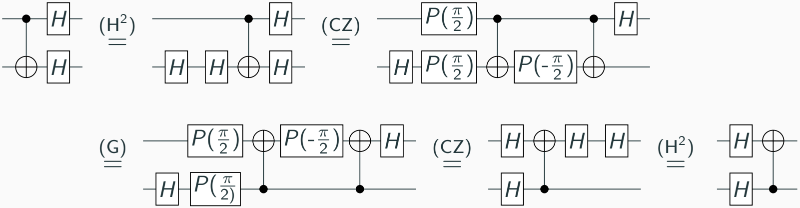
We can use simple equations such that,



and



to derive new equations. For instance,



Soundness and completeness

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.

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

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

The first complete and sound equational theory.

Soundness and completeness

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.

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

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

The first complete and sound equational theory.

Soundness and completeness

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.

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

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

The first complete and sound equational theory.

Soundness and completeness

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

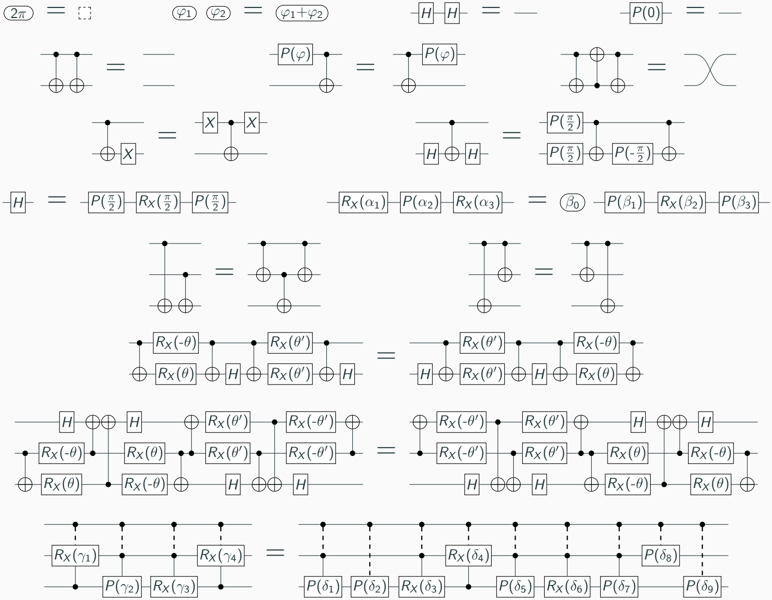
Any true equation is derivable.

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

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

The first complete and sound equational theory.

Complete and sound equational theory



Euler decomposition equation

This equation follows from the well-known Euler-decomposition which states that any unitary can be decomposed, up to a global phase, into basic X- and Z-rotations.

$$-\boxed{R_X(\alpha_1)}-\boxed{P(\alpha_2)}-\boxed{R_X(\alpha_3)}- \;=\; (\beta_0)\; -\boxed{P(\beta_1)}-\boxed{R_X(\beta_2)}-\boxed{P(\beta_3)}-$$

It represents a family of equations: there are explicit trigonometric relations to compute $\beta_0, \beta_1, \beta_2, \beta_3$ as functions of $\alpha_1, \alpha_2, \alpha_3$.

By choosing specific parameters, we can retrieve simple equations, such that

$$-\boxed{P(\varphi_1)}-\boxed{P(\varphi_2)}- \;=\; -\boxed{P(\varphi_1+\varphi_2)}- \qquad -\boxed{X}-\boxed{P(\varphi)}-\boxed{X}- \;=\; (\varphi)\; -\boxed{P(-\varphi)}-$$

Euler decomposition equation

This equation follows from the well-known Euler-decomposition which states that any unitary can be decomposed, up to a global phase, into basic X- and Z-rotations.

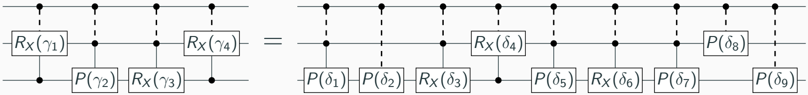
$$-\boxed{R_X(\alpha_1)}-\boxed{P(\alpha_2)}-\boxed{R_X(\alpha_3)}- \;=\; (\beta_0)\; -\boxed{P(\beta_1)}-\boxed{R_X(\beta_2)}-\boxed{P(\beta_3)}-$$

It represents a family of equations: there are explicit trigonometric relations to compute $\beta_0, \beta_1, \beta_2, \beta_3$ as functions of $\alpha_1, \alpha_2, \alpha_3$.

By choosing specific parameters, we can retrieve simple equations, such that

$$-\boxed{P(\varphi_1)}-\boxed{P(\varphi_2)}- \;=\; -\boxed{P(\varphi_1+\varphi_2)}- \qquad\qquad -\boxed{X}-\boxed{P(\varphi)}-\boxed{X}- \;=\; (\varphi)\; -\boxed{P(-\varphi)}-$$

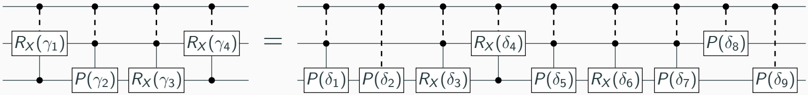
The weird equation



Similarly to the Euler decomposition equation, it represents a family of equations: there is an instance of this equation in the equational theory for any number of wires $n \geq 2$ and for any parameters $\gamma_1, \gamma_2, \gamma_3, \gamma_4 \in \mathbb{R}$.

The presence of such weird equation is the consequence of the technique used to prove completeness: the proof is based on back and forth translations between quantum circuits and optical circuits.

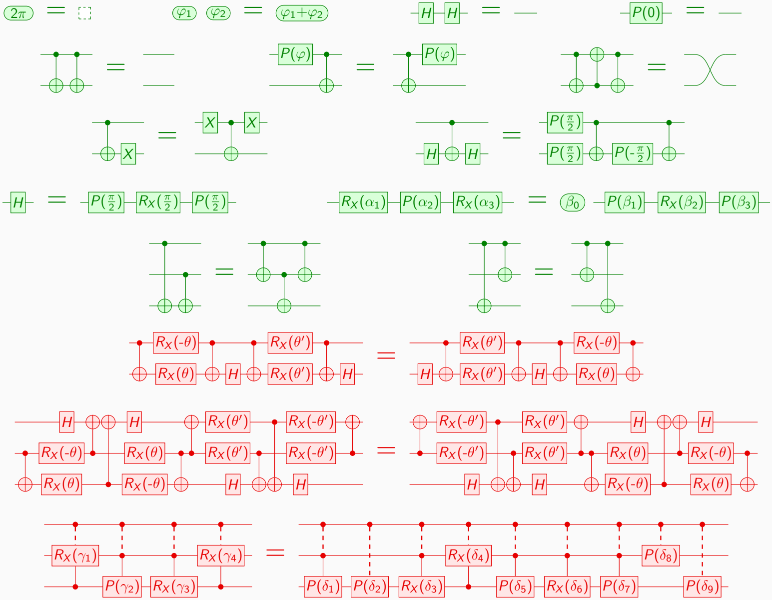
The weird equation



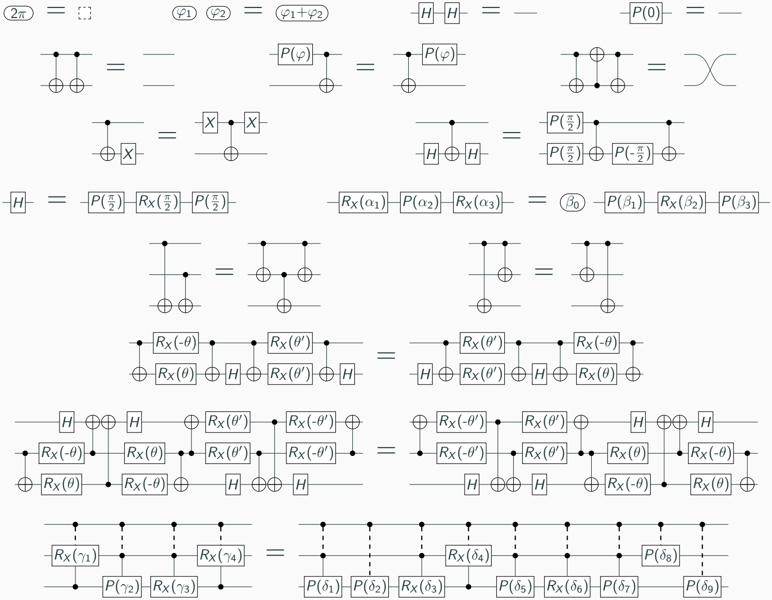
Similarly to the Euler decomposition equation, it represents a family of equations: there is an instance of this equation in the equational theory for any number of wires $n \geq 2$ and for any parameters $\gamma_1, \gamma_2, \gamma_3, \gamma_4 \in \mathbb{R}$.

The presence of such weird equation is the consequence of the technique used to prove completeness: the proof is based on back and forth translations between quantum circuits and optical circuits.

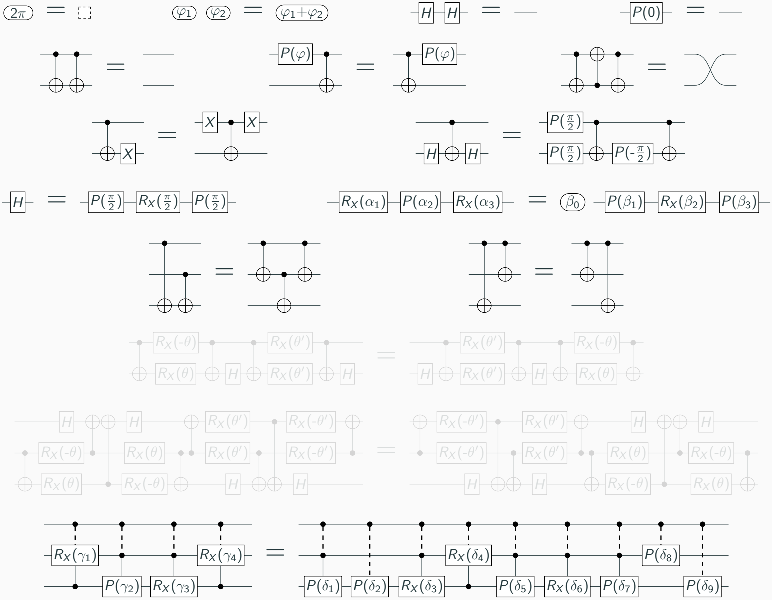
Some easy and some intricate equations



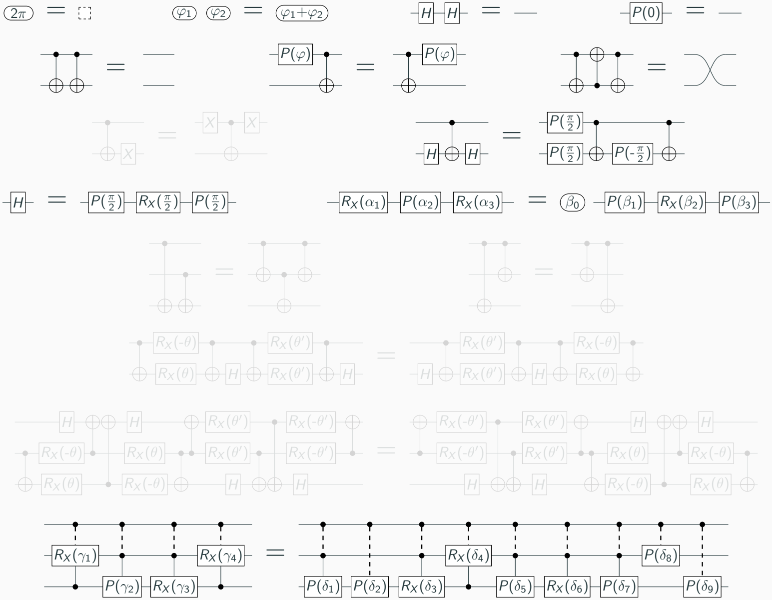
Simplifications



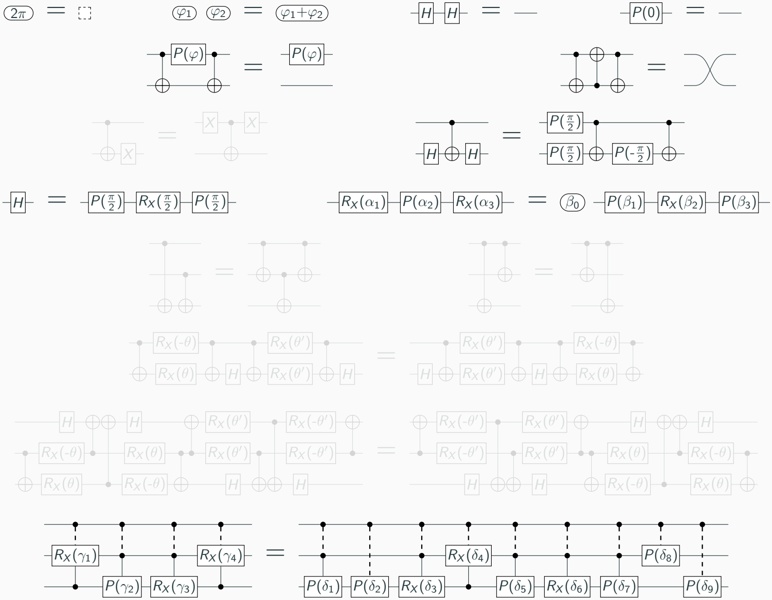
Simplifications



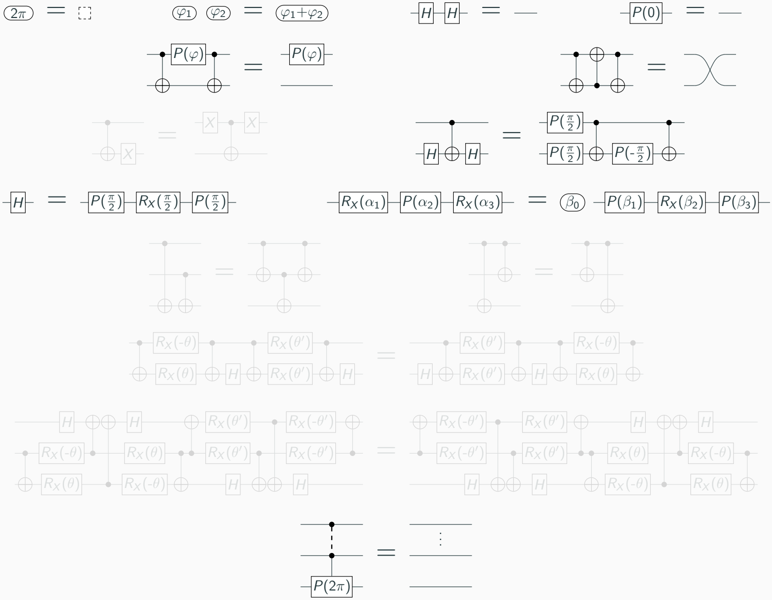
Simplifications



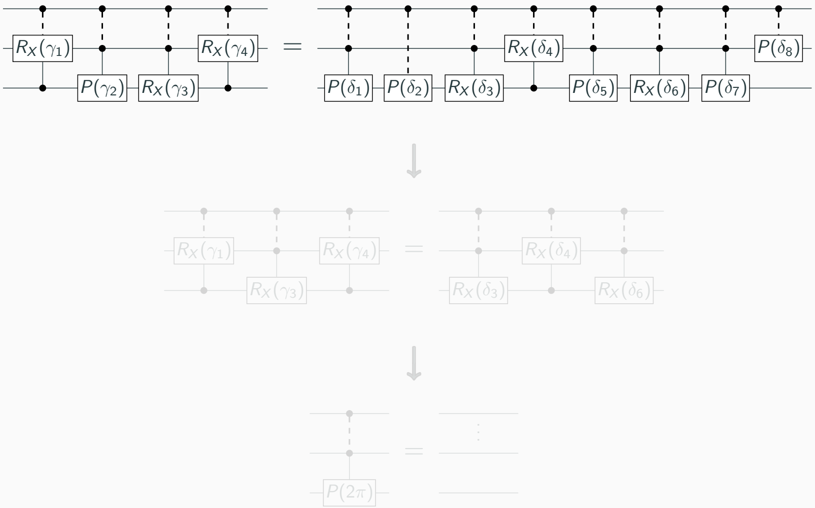
Simplifications



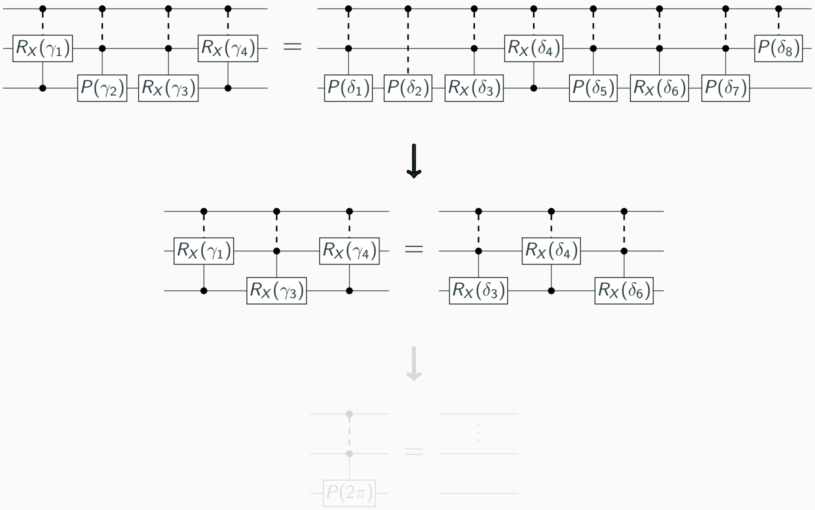
Simplifications



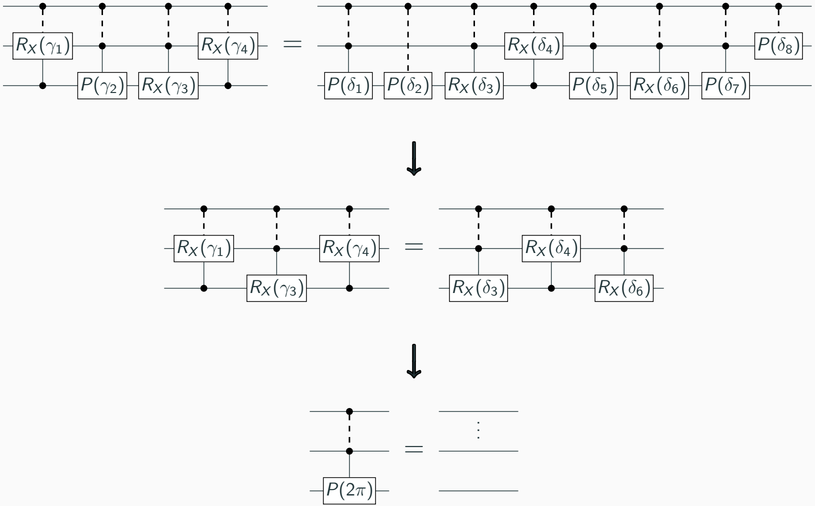
Killing the remaining weird rule



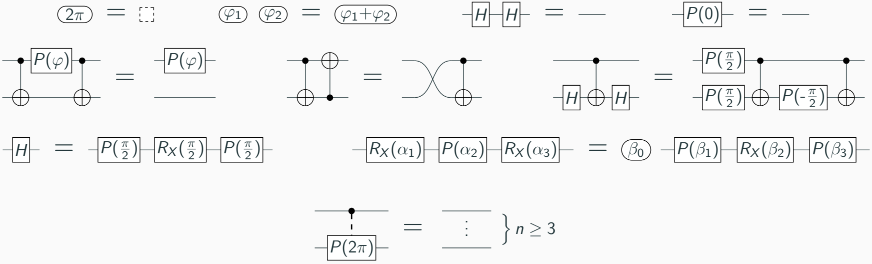
Killing the remaining weird rule



Killing the remaining weird rule



Towards the limit of simplification



Question: Can we simplify the equational theory even more?

Theorem

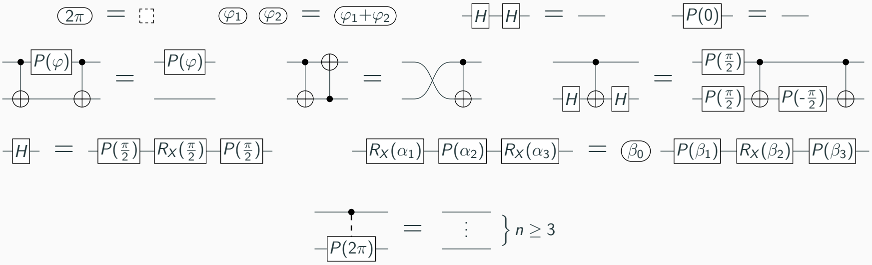
This equational theory is complete, sound and minimal.

Minimality

All equations are independents.

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

Towards the limit of simplification



Question: Can we simplify the equational theory even more?

Theorem

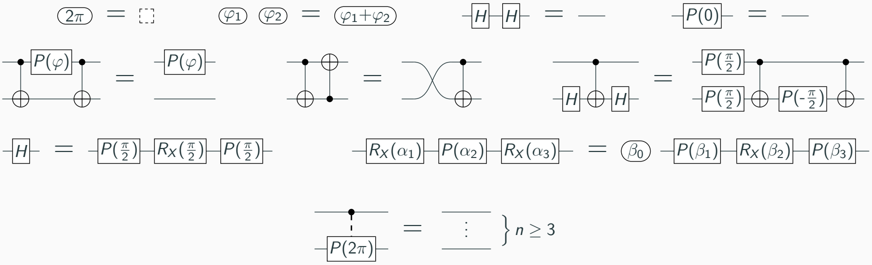
This equational theory is complete, sound and minimal.

Minimality

All equations are independents.

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

Towards the limit of simplification



Question: Can we simplify the equational theory even more?

Theorem

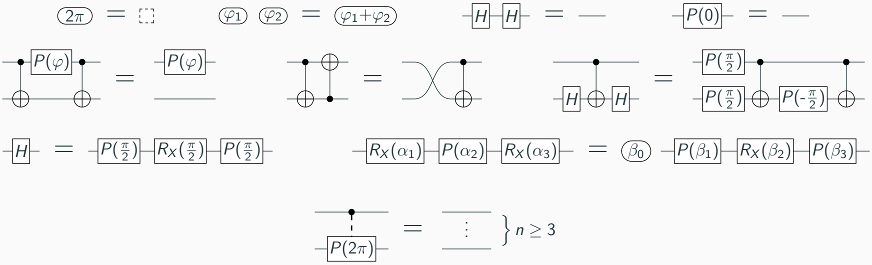
This equational theory is complete, sound and minimal.

Minimality

All equations are independents.

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

Towards the limit of simplification



Question: Can we simplify the equational theory even more?

Theorem

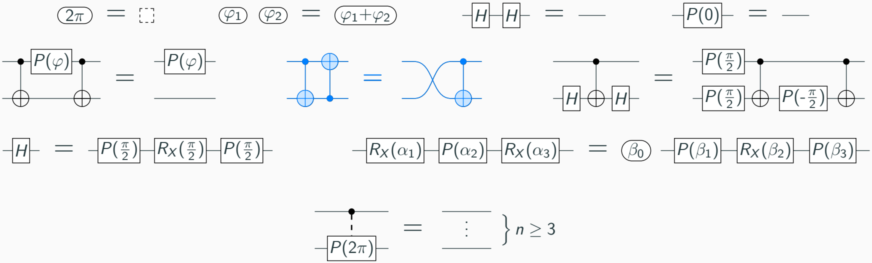
This equational theory is complete, sound and minimal.

Minimality

All equations are independents.

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

Necessity of the simple equations



For instance, the blue equation is the only one that does not preserve the parity of the number of swap gates.

Necessity of the Euler decomposition equation

Equation (E) represent a family of equations and is the only equation involving non-linear computations.

$$-\boxed{R_X(\alpha_1)}-\boxed{P(\alpha_2)}-\boxed{R_X(\alpha_3)}- \overset{(E)}{=} \ (\beta_0) \ -\boxed{P(\beta_1)}-\boxed{R_X(\beta_2)}-\boxed{P(\beta_3)}-$$

Maybe (E) is in the equational theory only to retrieve simple equations such that

$$-\boxed{P(\varphi_1)}-\boxed{P(\varphi_2)}- \overset{(P_+)}{=} -\boxed{P(\varphi_1+\varphi_2)}- \qquad -\boxed{X}-\boxed{P(\varphi)}-\boxed{X}- \overset{(P_-)}{=} \ (\varphi) \ -\boxed{P(-\varphi)}-$$

Proposition

Let Γ be a set of equations containing

- all the equations of the equational theory except (E),
- any set of instance of (E) of cardinality strictly less than $2^{\aleph_0}$,
- all instances of (P_+) and (P_-).

Then there exists an instance of (E) which is not a consequence of Γ. Hence, uncountably many instances of (E) are requiered.

Necessity of the Euler decomposition equation

Equation (E) represent a family of equations and is the only equation involving non-linear computations.

$$-\boxed{R_X(\alpha_1)}-\boxed{P(\alpha_2)}-\boxed{R_X(\alpha_3)}- \overset{(E)}{=} \ (\beta_0)\ -\boxed{P(\beta_1)}-\boxed{R_X(\beta_2)}-\boxed{P(\beta_3)}-$$

Maybe (E) is in the equational theory only to retrieve simple equations such that

$$-\boxed{P(\varphi_1)}-\boxed{P(\varphi_2)}- \overset{(P_+)}{=} -\boxed{P(\varphi_1+\varphi_2)}- \qquad -\boxed{X}-\boxed{P(\varphi)}-\boxed{X}- \overset{(P_-)}{=} \ (\varphi)\ -\boxed{P(-\varphi)}-$$

Proposition

Let Γ be a set of equations containing

- all the equations of the equational theory except (E),
- any set of instance of (E) of cardinality strictly less than $2^{\aleph_0}$,
- all instances of (P_+) and (P_-).

Then there exists an instance of (E) which is not a consequence of Γ.
Hence, uncountably many instances of (E) are requiered.

Necessity of the Euler decomposition equation

Equation (E) represent a family of equations and is the only equation involving non-linear computations.

$$-\boxed{R_X(\alpha_1)}-\boxed{P(\alpha_2)}-\boxed{R_X(\alpha_3)}- \overset{(E)}{=} \circled{\beta_0} -\boxed{P(\beta_1)}-\boxed{R_X(\beta_2)}-\boxed{P(\beta_3)}-$$

Maybe (E) is in the equational theory only to retrieve simple equations such that

$$-\boxed{P(\varphi_1)}-\boxed{P(\varphi_2)}- \overset{(P_+)}{=} -\boxed{P(\varphi_1+\varphi_2)}- \qquad -\boxed{X}-\boxed{P(\varphi)}-\boxed{X}- \overset{(P_-)}{=} \circled{\varphi} -\boxed{P(-\varphi)}-$$

Proposition

Let Γ be a set of equations containing

- all the equations of the equational theory except (E),
- any set of instance of (E) of cardinality strictly less than $2^{\aleph_0}$,
- all instances of (P_+) and (P_-).

Then there exists an instance of (E) which is not a consequence of Γ. Hence, uncountably many instances of (E) are requiered.

Unboundedness of the equational theory

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

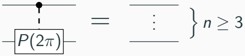
are necessary (for every $n \geq 3$).

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 

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 $n \in \mathbb{N}$.

Proof sketch [1/2]

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

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

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

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

Intuition: $[\![C]\!]_n^\sharp = \arg(\det([\![C]\!]))$ for any n-qubit quantum circuit C.

More precisely, for any n-qubit quantum circuit C and $k \geq n$,

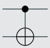
$$[\![C]\!]_k^\sharp = 2^{k-n} \arg(\det([\![C]\!]))$$

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

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

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

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

Intuition: $[\![C]\!]^\sharp_n = \arg(\det([\![C]\!]))$ for any n-qubit quantum circuit C.

More precisely, for any n-qubit quantum circuit C and $k \geq n$,

$$[\![C]\!]^\sharp_k = 2^{k-n} \arg(\det([\![C]\!]))$$

Proof sketch [1/2]

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

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

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

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

Intuition: $[\![C]\!]_n^\sharp = \arg(\det([\![C]\!]))$ for any n-qubit quantum circuit C.

More precisely, for any n-qubit quantum circuit C and $k \geq n$,

$$[\![C]\!]_k^\sharp = 2^{k-n} \arg(\det([\![C]\!]))$$

Lemme

For any n-qubit quantum circuits C_1, C_2 and $k \geq n$,

$$[\![C_1]\!] = [\![C_2]\!] \quad\Longrightarrow\quad [\![C_1]\!]^\sharp_k = [\![C_2]\!]^\sharp_k$$

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

However,

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

Hence $=$ $\}n$ cannot be derived from an equational theory containing only equations acting on strictly less than n wires.

Proof sketch [2/2]

Lemme

For any *n*-qubit quantum circuits C_1, C_2 and $k \geq n$,

$$[\![C_1]\!] = [\![C_2]\!] \quad \Longrightarrow \quad [\![C_1]\!]_k^\sharp = [\![C_2]\!]_k^\sharp$$

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

However,

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

Hence = $\}_n$ cannot be derived from an equational theory containing only equations acting on strictly less than n wires.

Proof sketch [2/2]

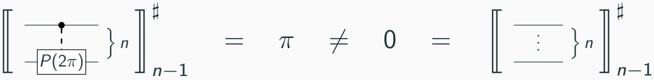
Lemme

For any n-qubit quantum circuits C_1, C_2 and $k \geq n$,

$$[\![C_1]\!] = [\![C_2]\!] \implies [\![C_1]\!]^\sharp_k = [\![C_2]\!]^\sharp_k$$

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

However,



Hence

cannot be derived from an equational theory containing only equations acting on strictly less than n wires.

Proof sketch [2/2]

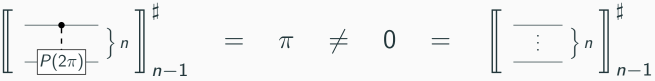
Lemme

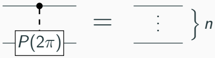
For any n-qubit quantum circuits C_1, C_2 and $k \geq n$,

$$[\![C_1]\!] = [\![C_2]\!] \quad \Longrightarrow \quad [\![C_1]\!]^\sharp_k = [\![C_2]\!]^\sharp_k$$

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

However,



Hence 

cannot be derived from an equational theory containing only equations acting on strictly less than n wires.

Discussion of the theorem

Possible weakness: $[\![C]\!]_k^\sharp$ is closely related to the determinant of $[\![C]\!]$. What if we consider quantum circuits up to global phases?

$\longrightarrow$ The theorem still holds!

Possible weakness: The choice of the generators
may seem arbitrary. What if we take another univeral gate set?

$\longrightarrow$ The theorem still holds! (for unitary quantum circuits.)

Discussion of the theorem

Possible weakness: $[\![C]\!]_k^\sharp$ is closely related to the determinant of $[\![C]\!]$. What if we consider quantum circuits up to global phases?

$\longrightarrow$ The theorem still holds!

Possible weakness: The choice of the generators

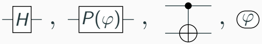
may seem arbitrary. What if we take another univeral gate set?

$\longrightarrow$ The theorem still holds! (for unitary quantum circuits.)

Discussion of the theorem

Possible weakness: $[\![C]\!]_k^\sharp$ is closely related to the determinant of $[\![C]\!]$. What if we consider quantum circuits up to global phases?

$\longrightarrow$ The theorem still holds!

Possible weakness: The choice of the generators 

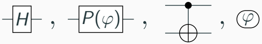
may seem arbitrary. What if we take another univeral gate set?

$\longrightarrow$ The theorem still holds! (for unitary quantum circuits.)

Discussion of the theorem

Possible weakness: $[\![C]\!]_k^\sharp$ is closely related to the determinant of $[\![C]\!]$. What if we consider quantum circuits up to global phases?

$\longrightarrow$ The theorem still holds!

Possible weakness: The choice of the generators


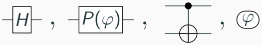
may seem arbitrary. What if we take another univeral gate set?

$\longrightarrow$ The theorem still holds! (for unitary quantum circuits.)

Discussion of the theorem

Possible weakness: $[\![C]\!]_k^\sharp$ is closely related to the determinant of $[\![C]\!]$. What if we consider quantum circuits up to global phases?

$\longrightarrow$ The theorem still holds!

Possible weakness: The choice of the generators 

may seem arbitrary. What if we take another univeral gate set?

$\longrightarrow$ The theorem still holds! (for unitary quantum circuits.)

Corollary

Any complete equational theory for the fragment where parameters are multiple of $\frac{\pi}{2^n}$ must contain at least one equation acting on $n+2$ wires.

For Clifford quantum circuits (case $n=1$),
$\longrightarrow$ The bound has been reached [Selinger'2015].

For Clifford+T quantum circuits (case $n=2$),
$\longrightarrow$ There exists equations that are not provable in the equational theory for 2-qubit Clifford+T of [Bian,Selinger'2022].

Interesting corollaries

Corollary

Any complete equational theory for the fragment where parameters are multiple of $\frac{\pi}{2^n}$ must contain at least one equation acting on $n+2$ wires.

For Clifford quantum circuits (case $n = 1$),
$\longrightarrow$ The bound has been reached [Selinger'2015].

For Clifford+T quantum circuits (case $n = 2$),
$\longrightarrow$ There exists equations that are not provable in the equational theory for 2-qubit Clifford+T of [Bian,Selinger'2022].

Interesting corollaries

Corollary

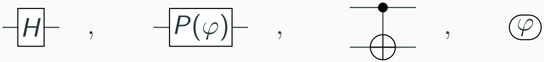
Any complete equational theory for the fragment where parameters are multiple of $\frac{\pi}{2^n}$ must contain at least one equation acting on $n+2$ wires.

For Clifford quantum circuits (case $n=1$),
$\longrightarrow$ The bound has been reached [Selinger'2015].

For Clifford+T quantum circuits (case $n=2$),
$\longrightarrow$ There exists equations that are not provable in the equational theory for 2-qubit Clifford+T of [Bian,Selinger'2022].

Extension to quantum circuits with ancillae

Quantum circuits with ancillae are generated by



together with

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

respectively denoting qubit initialisation and qubit termination.

(The generator $\dashv$ can only be applied to qubits 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 qubit initialisation and qubit termination.

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

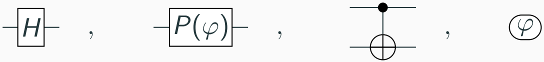
Semantics

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 qubit initialisation and qubit termination.

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

Semantics

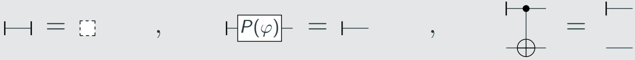
We extend $[\![\cdot]\!]$ with $[\![\vdash]\!] = |0\rangle$ and $[\![\dashv]\!] = \langle 0|$.

Universal for isometries

Boundedness of the equational theory with ancillae

Theorem [Clément,Delorme,Perdrix,Vilmart'2024]

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,

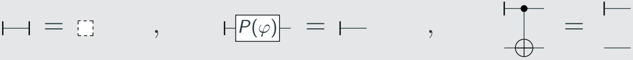
is derivable for $n \geq 4$.

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

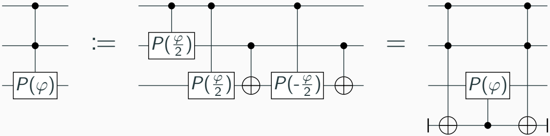
Boundedness of the equational theory with ancillae

Theorem [Clément,Delorme,Perdrix,Vilmart'2024]

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,

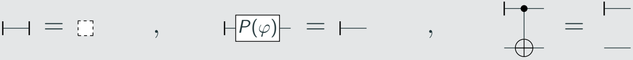
is derivable for $n \geq 4$.

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

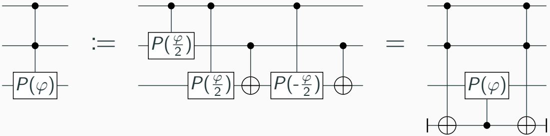
Boundedness of the equational theory with ancillae

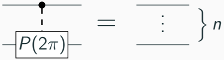
Theorem [Clément,Delorme,Perdrix,Vilmart'2024]

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.



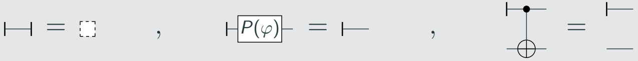
In these more general settings,  is derivable for $n \geq 4$.

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

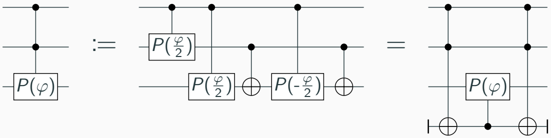
Boundedness of the equational theory with ancillae

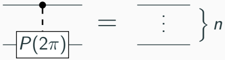
Theorem [Clément,Delorme,Perdrix,Vilmart'2024]

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