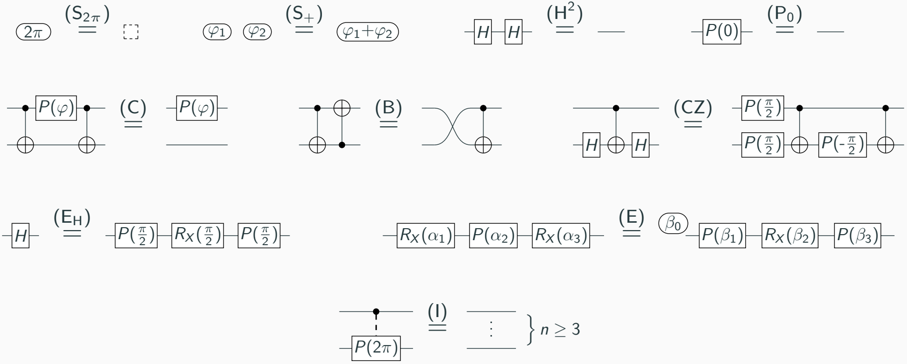
Minimal Equational Theories for Quantum Circuits

Alexandre Clément*, Noé Delorme†, Simon Perdrix†

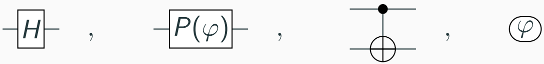
*Université Paris-Saclay, ENS Paris-Saclay, CNRS, Inria, LMF, 91190, Gif-sur-Yvette, France
†Université de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, France

This is a minimal complete equational theory for quantum circuits.



Quantum circuits as a graphical language

Quantum circuits are generated by



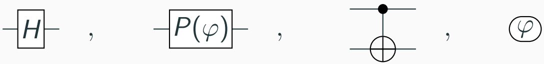
together with

which come from the prop formalism[1] together with some deformation rules that ensure that circuits are defined "up to deformation".

[1]The prop formalism is a mathematical framework for graphical language.

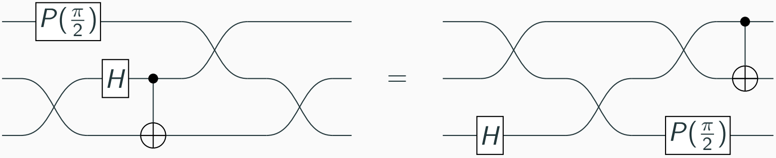
Quantum circuits as a graphical language

Quantum circuits are generated by



together with

which come from the prop formalism[1] together with some deformation rules that ensure that circuits are defined "up to deformation".



[1]The prop formalism is a mathematical framework for graphical language.

Standard interpretation of quantum circuits

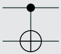
$$\text{circuits} \neq \text{unitaries}$$

Semantics

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

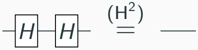
$[\![$  $]\!] = (1)$ $\qquad [\![\varphi]\!] = (e^{i\varphi})$

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

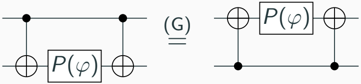
$[\![$  $]\!] = \begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \end{pmatrix}$ $\qquad [\![$  $]\!] = \begin{pmatrix} 1&0&0&0 \\ 0&0&1&0 \\ 0&1&0&0 \\ 0&0&0&1 \end{pmatrix}$

Using axioms to transform circuits

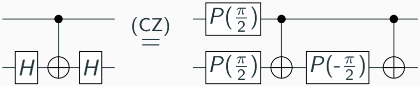
We can use simple axioms such that,



,



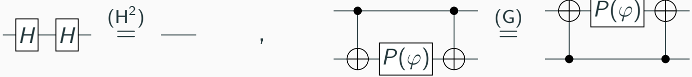
and



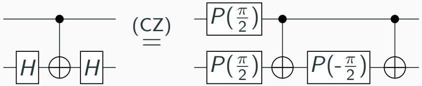
to derive new equations. For instance,

Using axioms to transform circuits

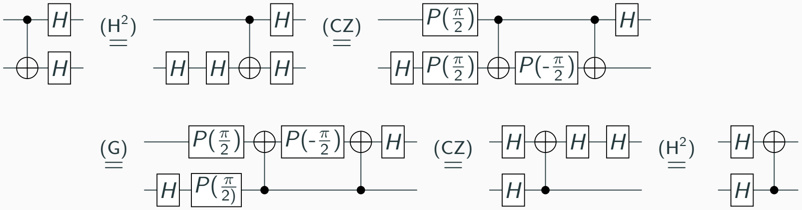
We can use simple axioms such that,



and



to derive new equations. For instance,



Desired properties for equational theories

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

Soundness

Any derivable equation is true.

$$\forall C_1, C_2 \in \mathcal{QC} \quad : \quad \Gamma \vdash C_1 = C_2 \implies [\![C_1]\!] = [\![C_2]\!]$$

Completeness

Any true equation is derivable.

$$\forall C_1, C_2 \in \mathcal{QC} \quad : \quad [\![C_1]\!] = [\![C_2]\!] \implies \Gamma \vdash C_1 = C_2$$

Goal: find a complete and sound equational theory.

Desired properties for equational theories

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

Soundness

Any derivable equation is true.

$\forall C_1, C_2 \in \mathcal{QC} \quad : \quad \Gamma \vdash C_1 = C_2 \implies [\![C_1]\!] = [\![C_2]\!]$

Completeness

Any true equation is derivable.

$\forall C_1, C_2 \in \mathcal{QC} \quad : \quad [\![C_1]\!] = [\![C_2]\!] \implies \Gamma \vdash C_1 = C_2$

Goal: find a complete and sound equational theory.

Desired properties for equational theories

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

Soundness

Any derivable equation is true.

$\forall C_1, C_2 \in \mathcal{QC} \quad : \quad \Gamma \vdash C_1 = C_2 \implies [\![C_1]\!] = [\![C_2]\!]$

Completeness

Any true equation is derivable.

$\forall C_1, C_2 \in \mathcal{QC} \quad : \quad [\![C_1]\!] = [\![C_2]\!] \implies \Gamma \vdash C_1 = C_2$

Goal: find a complete and sound equational theory.

Desired properties for equational theories

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

Soundness

Any derivable equation is true.

$$\forall C_1, C_2 \in \mathcal{QC} \quad : \quad \Gamma \vdash C_1 = C_2 \implies [\![C_1]\!] = [\![C_2]\!]$$

Completeness

Any true equation is derivable.

$$\forall C_1, C_2 \in \mathcal{QC} \quad : \quad [\![C_1]\!] = [\![C_2]\!] \implies \Gamma \vdash C_1 = C_2$$

Goal: find a complete and sound equational theory.

Trivial, just take all sound equations.

🙃

Real goal: find a small complete and sound equational theory.

$\longrightarrow$ `arXiv:2206.10577(LICS2023)`[2]

[2]A Complete Equational Theory for Quantum Circuits. Alexandre Clément, Nicolas Heurtel, Shane Mansfield, Simon Perdrix, Benoît Valiron. LICS2023.

Trivial, just take all sound equations.

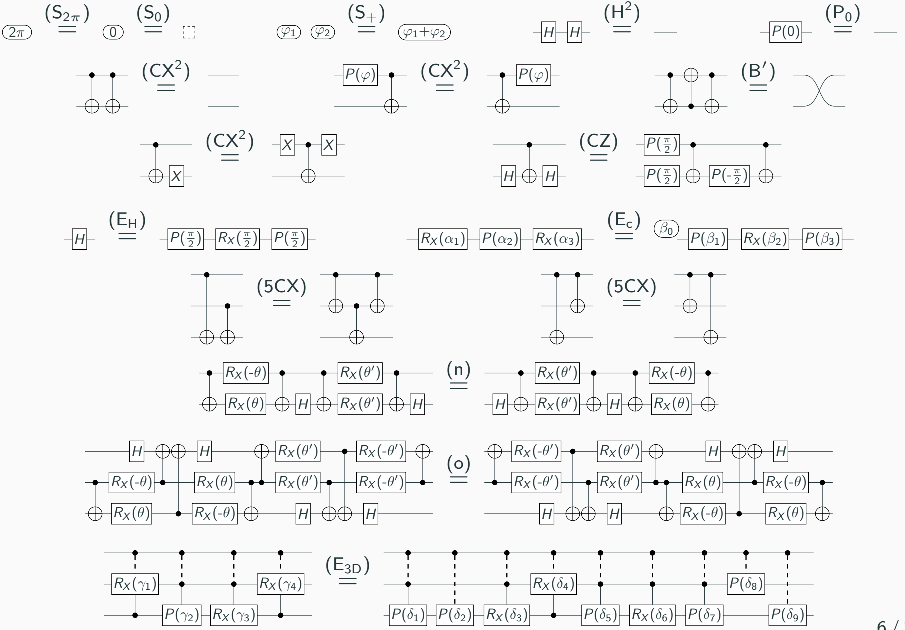
🙃

Real goal: find a small complete and sound equational theory.

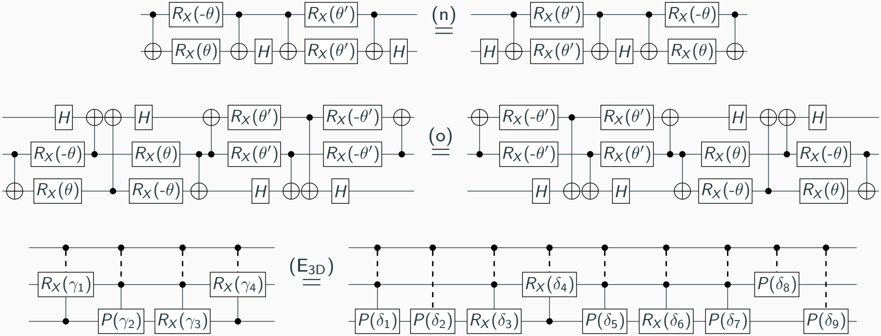
$\longrightarrow$ `arXiv:2206.10577(LICS2023)`[2]

[2] A Complete Equational Theory for Quantum Circuits. Alexandre Clément, Nicolas Heurtel, Shane Mansfield, Simon Perdrix, Benoît Valiron. LICS2023.

The first complete and sound equational theory



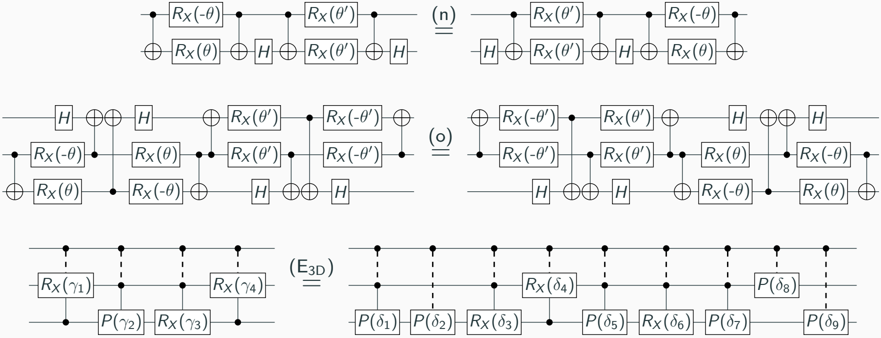
Problem: Many equations including non-intuitive and weird ones.



Real real goal: find a small complete and sound equational theory made of simple and intuitive axioms.

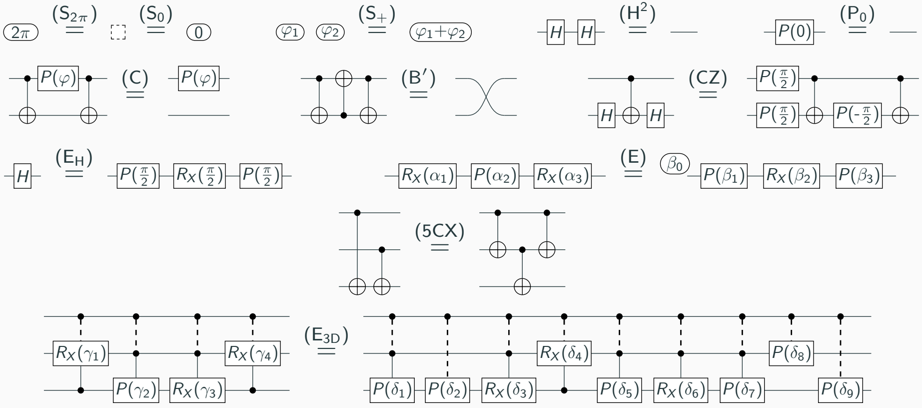
The problem of the equational theory

Problem: Many equations including non-intuitive and weird ones.



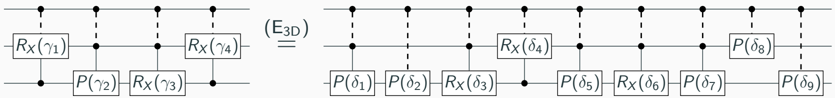
Real real goal: find a small complete and sound equational theory made of simple and intuitive axioms.

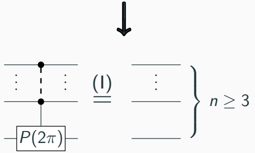
arXiv:2303.03117 (CSL2024)[3]



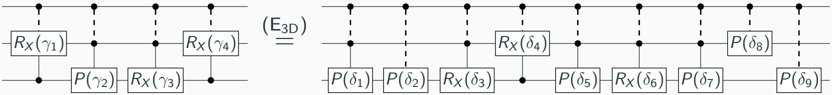
[3]Quantum Circuit Completeness: Extensions and Simplifications. Alexandre Clément, Noé Delorme, Simon Perdrix, Renaud Vilmart. CSL2024.

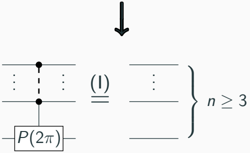
Killing the remaining weird rule



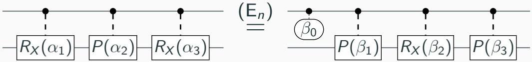


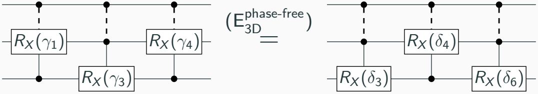
The two following intermediate results are the key to derive (E_{3D}) .





The two following intermediate results are the key to derive (E_{3D}) .





Towards the limit of simplifications

Question: Can we simplify the equational theory even more?

Minimality

All axioms are independents.

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

Real real real goal: find a minimal complete and sound equational theory made of simple and intuitive axioms.

Towards the limit of simplifications

Question: Can we simplify the equational theory even more?

Minimality

All axioms are independents.

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

Real real real goal: find a minimal complete and sound equational theory made of simple and intuitive axioms.

Towards the limit of simplifications

Question: Can we simplify the equational theory even more?

Minimality

All axioms are independents.

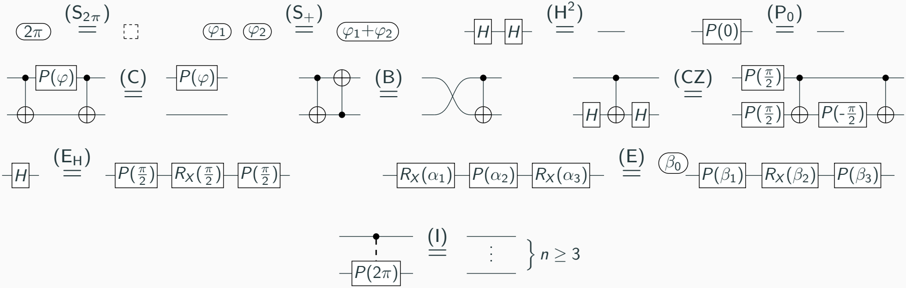
$\forall (C_1 = C_2) \in \Gamma \quad : \quad \Gamma \backslash \{C_1 = C_2\} \nvdash C_1 = C_2$

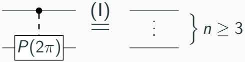
Real real real goal: find a minimal complete and sound equational theory made of simple and intuitive axioms.

The minimal complete and sound equational theory

Theorem

This equational theory is complete, sound and minimal.

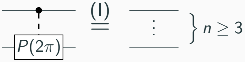


Every instances of  are necessary (for every $n \geq 3$).

Theorem

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

More precisely, any complete equational theory for n-qubit quantum circuits has at least one rule acting on n qubits.

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 qubits.

More precisely, any complete equational theory for n-qubit quantum circuits has at least one rule acting on n qubits.

Proof sketch of the main theorem

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

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

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

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

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

However,

$$\left[\!\!\left[\; \text{multi-controlled } -\boxed{P(2\pi)}- \;\right\}n \right]\!\!\right]^\sharp_{n-1} = \pi \neq 0 = \left[\!\!\left[\; \vdots \;\right\}n \right]\!\!\right]^\sharp_{n-1}$$

Proof sketch of the main theorem

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

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

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

$$\left[\!\!\left[\begin{smallmatrix}\bullet\\ |\\ \oplus\end{smallmatrix}\right]\!\!\right]^\sharp_k = \left[\!\!\left[\times\right]\!\!\right]^\sharp_k = 2^{k-2}\pi \bmod 2\pi \qquad [\![\,\text{-}\boxed{P(\varphi)}\text{-}\,]\!]^\sharp_k = 2^{k-1}\varphi \bmod 2\pi$$

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

However,

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

Proof sketch of the main theorem

Alternative interpretation

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

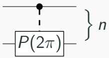
$$\llbracket C_2 \circ C_1 \rrbracket_k^\sharp = \llbracket C_1 \otimes C_2 \rrbracket_k^\sharp = \llbracket C_2 \rrbracket_k^\sharp + \llbracket C_1 \rrbracket_k^\sharp \bmod 2\pi$$

$$\llbracket \square \rrbracket_k^\sharp = \llbracket - \rrbracket_k^\sharp = 0 \qquad \llbracket \varphi \rrbracket_k^\sharp = 2^k \varphi \bmod 2\pi \qquad \llbracket -\boxed{H}- \rrbracket_k^\sharp = 2^{k-1}\pi \bmod 2\pi$$

$\llbracket$  $\rrbracket_k^\sharp = \llbracket$  $\rrbracket_k^\sharp = 2^{k-2}\pi \bmod 2\pi \qquad \llbracket -\boxed{P(\varphi)}- \rrbracket_k^\sharp = 2^{k-1}\varphi \bmod 2\pi$

Any sound equation involving quantum circuits acting on at most $n-1$ qubits is also sound according to $\llbracket \cdot \rrbracket_{n-1}^\sharp$.

However,

$\llbracket$  $\rrbracket_{n-1}^\sharp = \pi \neq 0 = \llbracket$  $\rrbracket_{n-1}^\sharp$

Discussion of the theorem

Possible weakness: $[\![C]\!]^\sharp_k$ 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 $-\boxed{H}-$, $-\boxed{P(\varphi)}-$, , φ is not unique. 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!

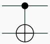
Possible weakness: The choice of the generators $-\boxed{H}-$, $-\boxed{P(\varphi)}-$, , φ is not unique. What if we take another univeral gate set?

$\longrightarrow$ 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!

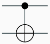
Possible weakness: The choice of the generators $\boxed{H}$, $\boxed{P(\varphi)}$,  , φ is not unique. What if we take another univeral gate set?

$\longrightarrow$ 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!

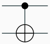
Possible weakness: The choice of the generators $\boxed{H}$, $\boxed{P(\varphi)}$,  , φ is not unique. What if we take another univeral gate set?

$\longrightarrow$ 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?

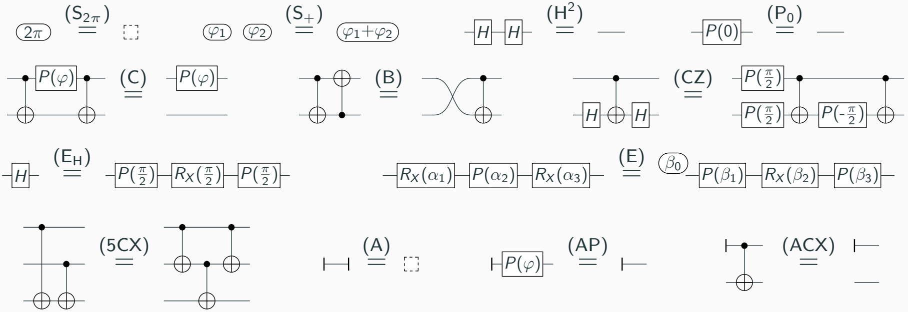
$\longrightarrow$ The theorem still holds!

Possible weakness: The choice of the generators $-\boxed{H}-$, $-\boxed{P(\varphi)}-$,  , φ is not unique. What if we take another univeral gate set?

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

Quantum circuits with ancillae

Interestingly, there is a complete equational theory for quantum circuits with auxiliary qubits (universal for isometries) made of equations acting on a bounded number of qubits.



Thanks

arxiv:2311.07476