Simpler Complete Equational Theories for Quantum Circuits with Ancillae or Partial Trace

Alexandre Clément, Noé Delorme,
Simon Perdrix, *Renaud Vilmart*

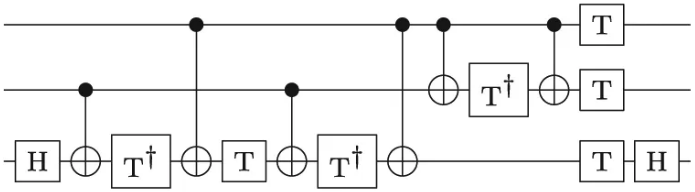
Mocqua / Loria

QPL23

arXiv:2303.03117

Loria
Laboratoire lorrain de recherche en informatique et ses applications
cnrs dépasser les frontières
Inria Nancy Grand Est
UNIVERSITÉ DE LORRAINE

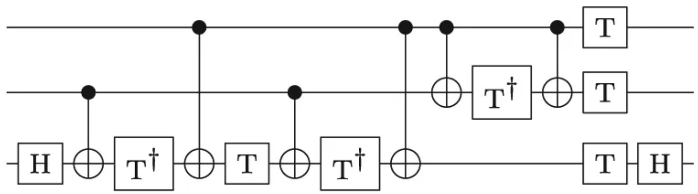
Quantum Circuits



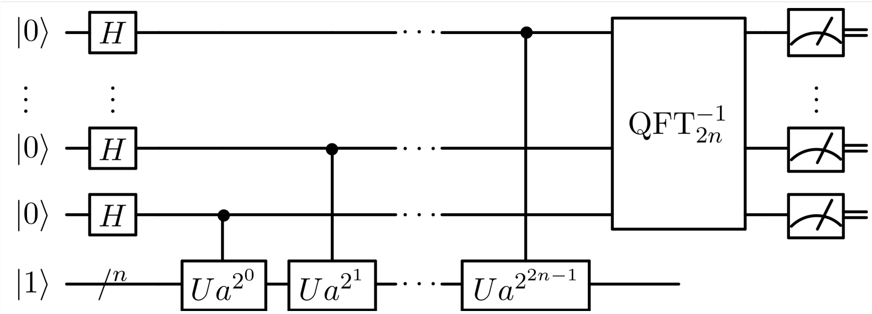
Quantum Circuits

D. Deutsch. Quantum computational networks. Proceedings of the Royal Society of London, A425:73–90, 1989.

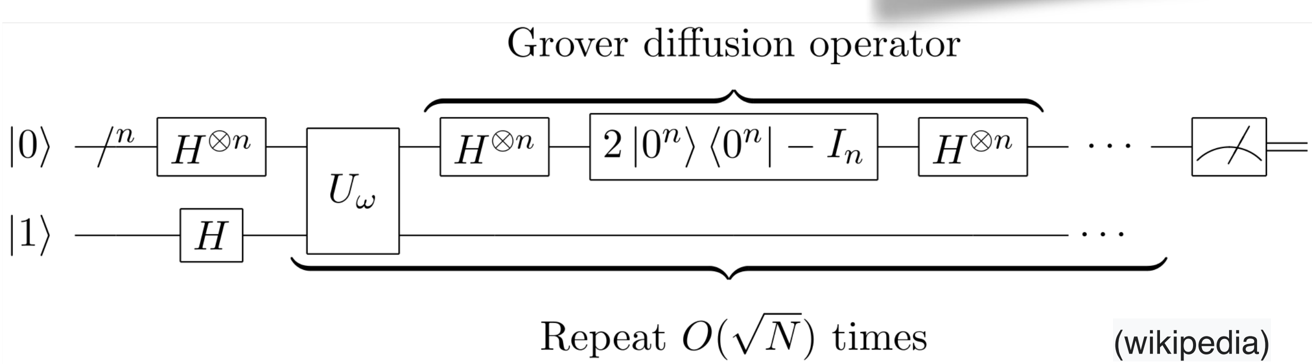
Quantum Circuits



Quantum Circuits



Quantum subroutine in Shor's algorithm (wikipedia)



(wikipedia)

D. Deutsch. Quantum computational networks. Proceedings of the Royal Society of London, A425:73-90, 1989.

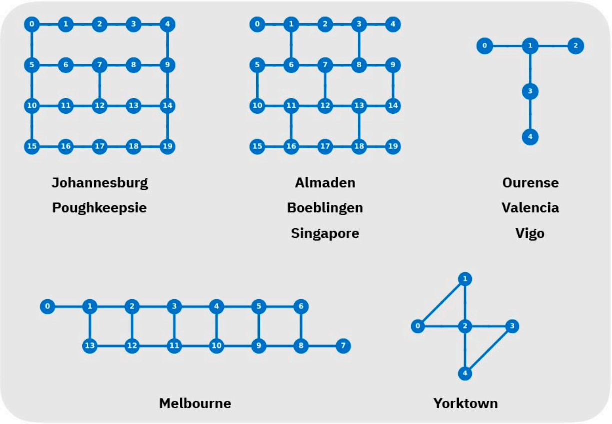
Quantum Circuits

Ubiquitous intermediate language for:

- Resource optimisation (#gates, #T, #CNot…)
- Hardware-constraint satisfaction (primitives, topological constraints, …)
- Fault-tolerant Quantum Computing
- Verification, circuit equivalence testing.

=> Circuit Transformation

IBM's 10 Quantum Device Lineup

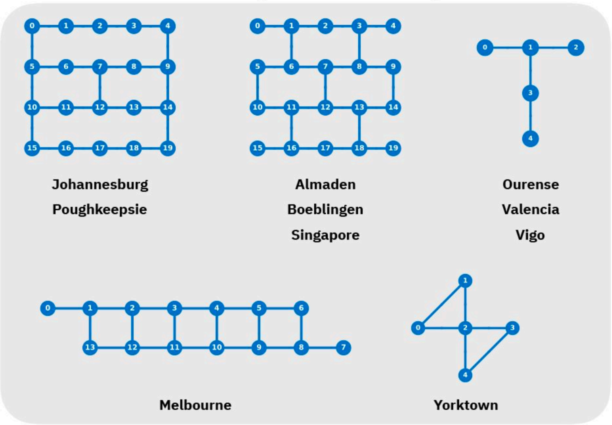


Quantum Circuits

Ubiquitous intermediate language for:

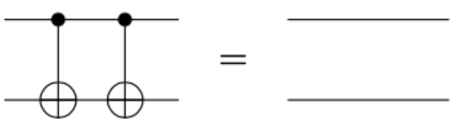
- Resource optimisation (#gates, #T, #CNot…)
- Hardware-constraint satisfaction (primitives, topological constraints, …)
- Fault-tolerant Quantum Computing
- Verification, circuit equivalence testing.

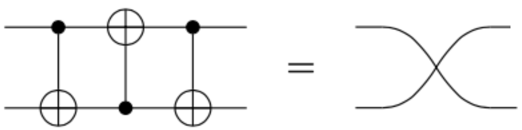
IBM's 10 Quantum Device Lineup

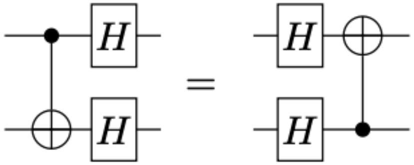


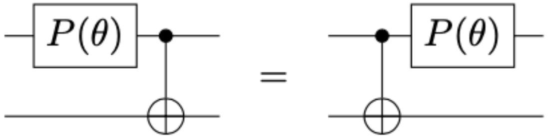
=> Circuit Transformation

Equational theory, e.g.:





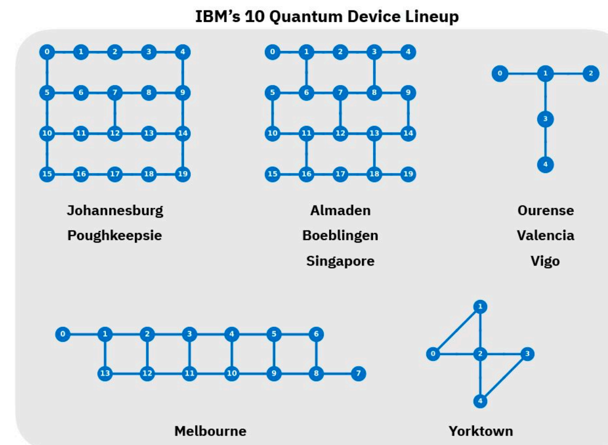




Quantum Circuits

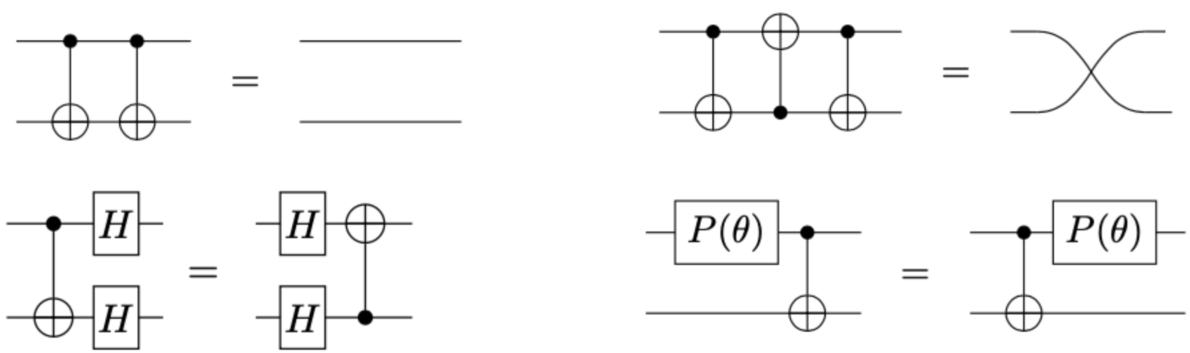
Ubiquitous intermediate language for:

- Resource optimisation (#gates, #T, #CNot…)
- Hardware-constraint satisfaction (primitives, topological constraints, …)
- Fault-tolerant Quantum Computing
- Verification, circuit equivalence testing.



=> Circuit Transformation

Equational theory, e.g.:

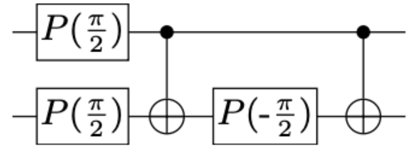


Completeness[1]?

1. if two circuits represent the same unitary, one can be transformed into the other using the equational theory, i.e, all true equations can be derived.

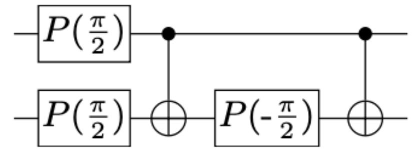
Circuits versus Matrices

Definition. The prop of quantum circuits is generated by $-\boxed{H}-$: $1 \to 1$, $-\boxed{P(\varphi)}-$: $1 \to 1$,  : $2 \to 2$, $\varphi : 0 \to 0$ for any $\varphi \in \mathbb{R}$.

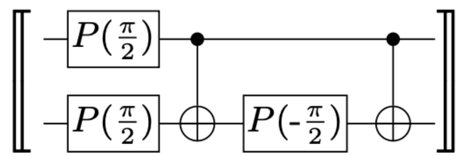


Circuits versus Matrices

Definition. The prop of quantum circuits is generated by $-\boxed{H}- : 1 \to 1$, $-\boxed{P(\varphi)}- : 1 \to 1$, $\bullet\!\!-\!\!\oplus : 2 \to 2$, $\textcircled{\varphi} : 0 \to 0$ for any $\varphi \in \mathbb{R}$.

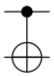


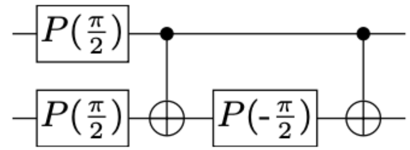
For any quantum circuit C, $[\![C]\!]$ is the corresponding matrix.



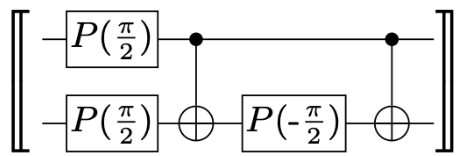
$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

Circuits versus Matrices

Definition. The prop of quantum circuits is generated by $-\boxed{H}-$: $1 \to 1$, $-\boxed{P(\varphi)}-$: $1 \to 1$,  : $2 \to 2$, φ : $0 \to 0$ for any $\varphi \in \mathbb{R}$.



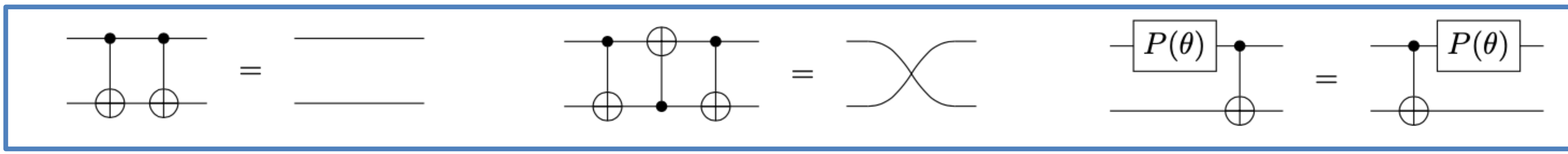
For any quantum circuit C, $[\![C]\!]$ is the corresponding matrix.



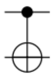
$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

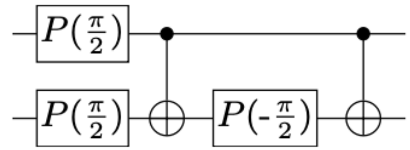
Equational theory, e.g.:

(E_0)

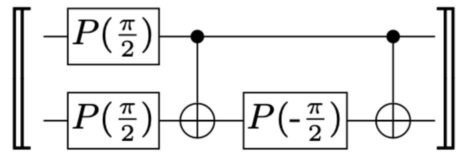


Circuits versus Matrices

Definition. The prop of quantum circuits is generated by $\boxed{H} : 1 \to 1$, $\boxed{P(\varphi)} : 1 \to 1$,  $: 2 \to 2$, $\varphi : 0 \to 0$ for any $\varphi \in \mathbb{R}$.



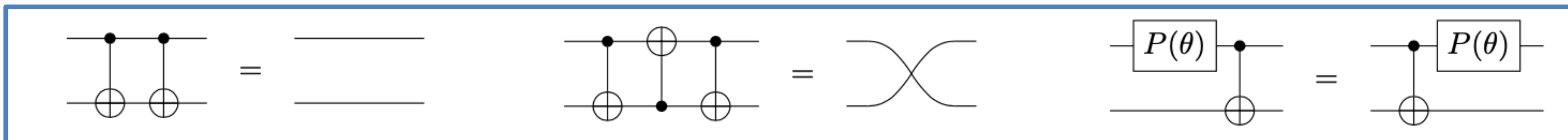
For any quantum circuit C, $[\![C]\!]$ is the corresponding matrix.



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

Equational theory, e.g.:

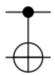
(E_0)

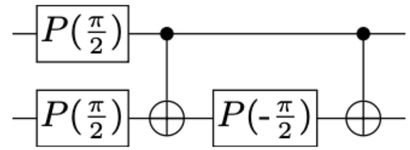


Soundness. If $E \vdash C_0 = C_1$ then $[\![C_0]\!] = [\![C_1]\!]$.

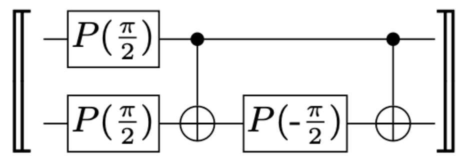
Completeness. If $[\![C_0]\!] = [\![C_1]\!]$ then $E \vdash C_0 = C_1$.

Circuits versus Matrices

Definition. The prop of quantum circuits is generated by $-\boxed{H}-$: $1 \to 1$, $-\boxed{P(\varphi)}-$: $1 \to 1$,  : $2 \to 2$, $\textcircled{\varphi}$: $0 \to 0$ for any $\varphi \in \mathbb{R}$.



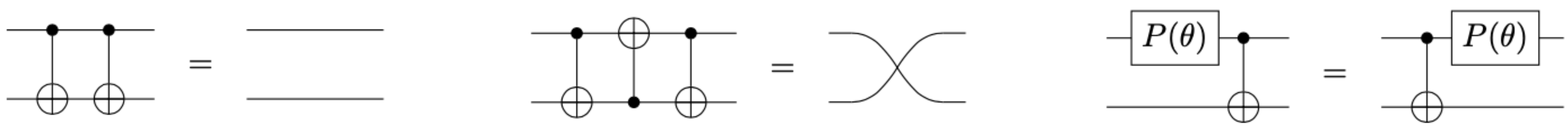
For any quantum circuit C, $[\![C]\!]$ is the corresponding matrix.



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

Equational theory, e.g.:

(E_0)



Soundness. If $E \vdash C_0 = C_1$ then $[\![C_0]\!] = [\![C_1]\!]$.

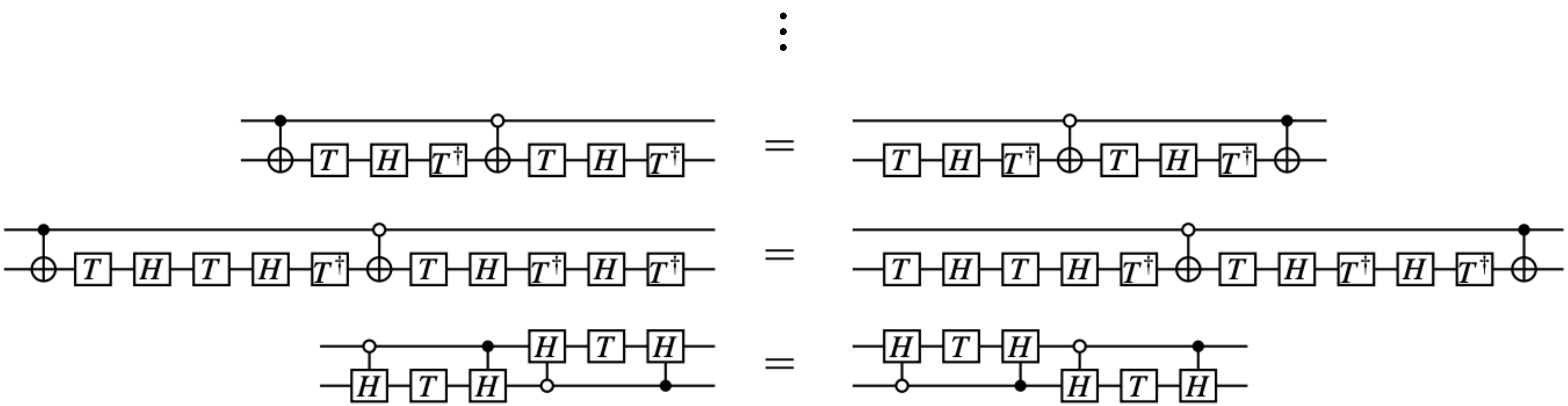
Completeness. If $[\![C_0]\!] = [\![C_1]\!]$ then $E \vdash C_0 = C_1$.

Example. (E_0) is sound but not complete:

QC Completeness

Complete equational theories for non-universal and classically simulatable **fragments**:

- 2-qubit circuits (Clifford+T) [Bian,Selinger'22]



(C18)

(C19)

(C20)

QC Completeness

Complete equational theories for non-universal and classically simulatable **fragments**:

- 2-qubit circuits (Clifford+T) [Bian,Selinger'22],
- 3-qubit circuits (Clifford+CS) [Bian,Selinger'23],

QC Completeness

Complete equational theories for non-universal and classically simulatable **fragments**:

- 2-qubit circuits (Clifford+T) [Bian,Selinger'22],
- 3-qubit circuits (Clifford+CS) [Bian,Selinger'23],
- Stabilizer [Ranchin,Coecke'18],

QC Completeness

Complete equational theories for non-universal and classically simulatable **fragments**:

- 2-qubit circuits (Clifford+T) [Bian,Selinger'22],
- 3-qubit circuits (Clifford+CS) [Bian,Selinger'23],
- Stabilizer [Ranchin,Coecke'18],
- Toffoli [Cockett,Comfort'19],

QC Completeness

Complete equational theories for non-universal and classically simulatable **fragments**:

- 2-qubit circuits (Clifford+T) [Bian,Selinger'22],
- 3-qubit circuits (Clifford+CS) [Bian,Selinger'23],
- Stabilizer [Ranchin,Coecke'18],
- Toffoli [Cockett,Comfort'19],
- CNot-dihedral (CNot+X+T) [Amy,Chen,Ross'21].

QC Completeness

Complete equational theories for non-universal and classically simulatable **fragments**:

- 2-qubit circuits (Clifford+T) [Bian,Selinger'22],
- 3-qubit circuits (Clifford+CS) [Bian,Selinger'23],
- Stabilizer [Ranchin,Coecke'18],
- Toffoli [Cockett,Comfort'19],
- CNot-dihedral (CNot+X+T) [Amy,Chen,Ross'21].

Complete equational theory for **universal quantum circuits**

- **Quantum Circuits** [Clément,Heurtel,Mansfield,Perdrix,Valiron LICS'23]

QC Completeness

Complete equational theories for non-universal and classically simulatable **fragments:**

- 2-qubit circuits (Clifford+T) [Bian,Selinger'22],
- 3-qubit circuits (Clifford+CS) [Bian,Selinger'23],
- Stabilizer [Ranchin,Coecke'18],
- Toffoli [Cockett,Comfort'19],
- CNot-dihedral (CNot+X+T) [Amy,Chen,Ross'21].

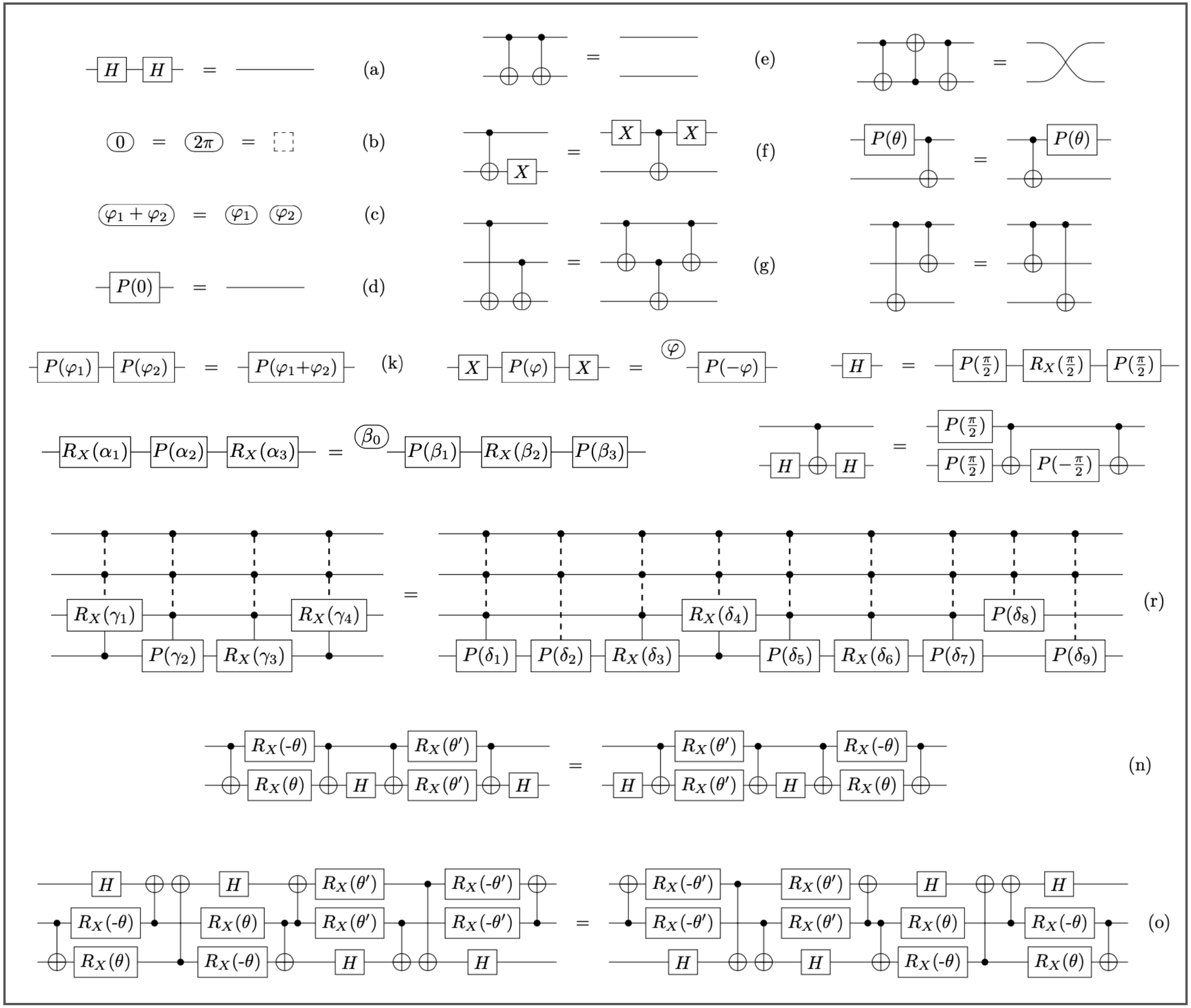
Complete equational theory for **universal quantum circuits**

- **Quantum Circuits** [Clément,Heurtel,Mansfield,Perdrix,Valiron LICS'23]

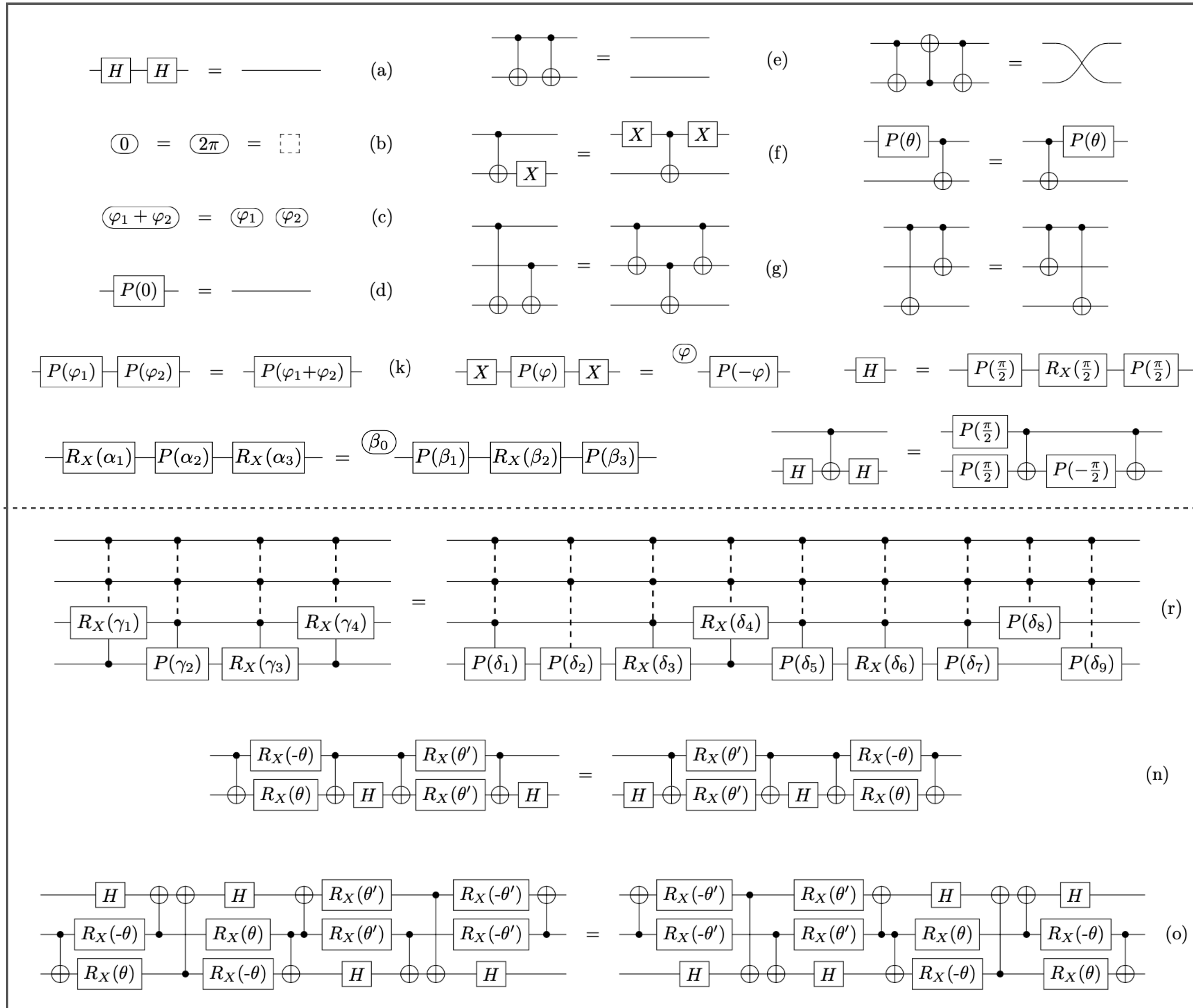
Our contributions:

- Simplifying equational theory for vanilla QC
- Extension to quantum circuits with ancilla and/or discarding

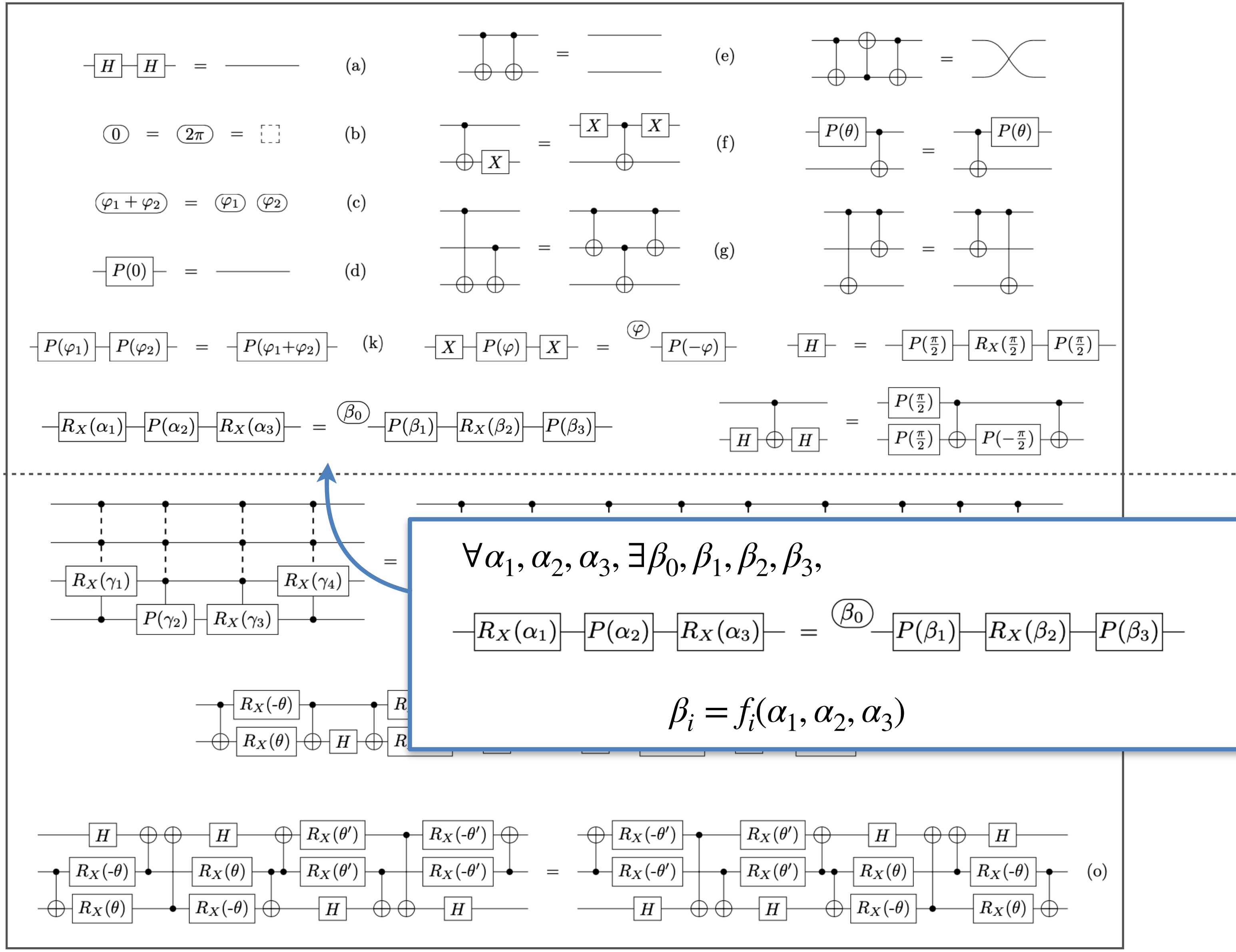
Complete Equational Theory [CHMPV LICS'23]



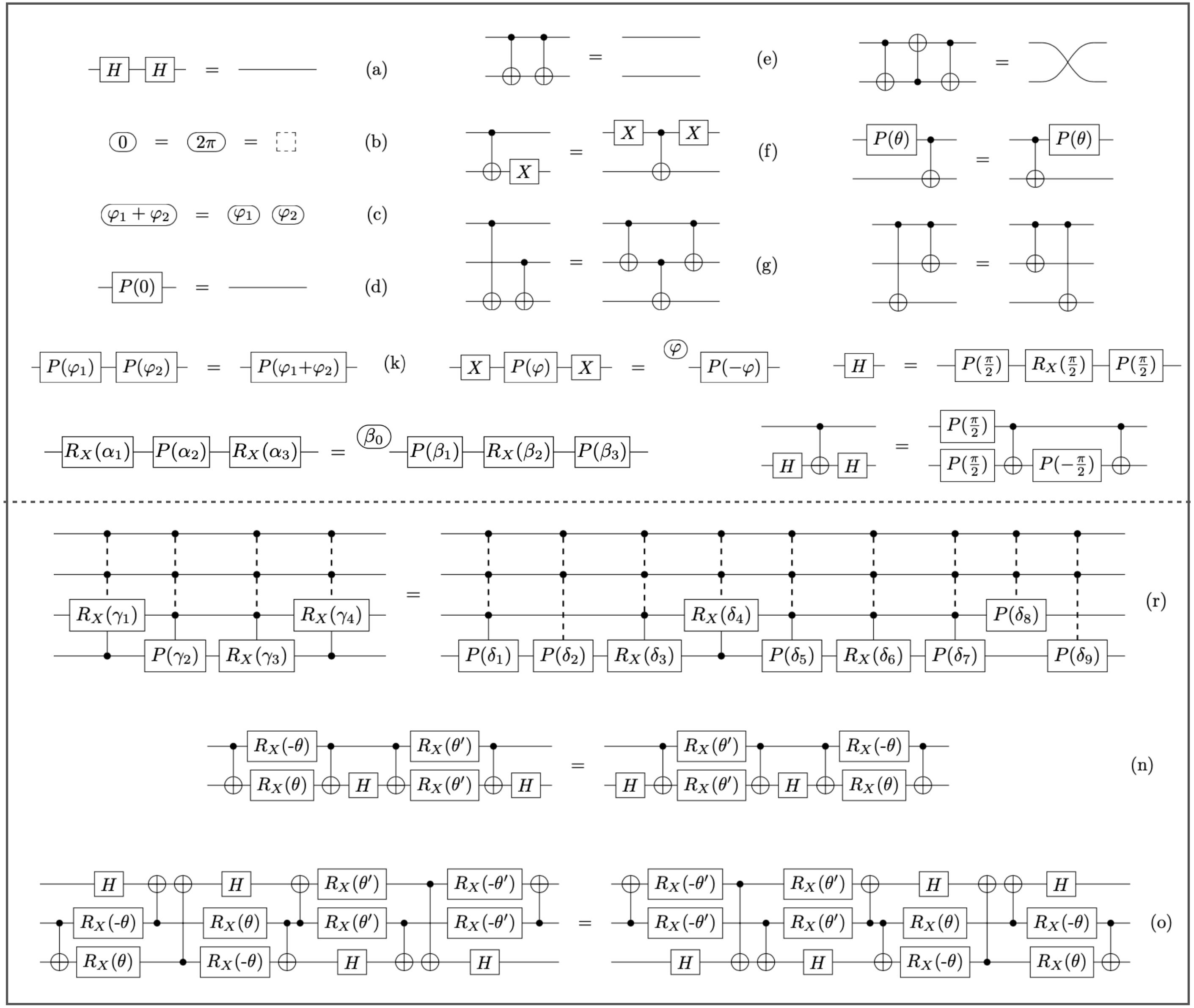
Complete Equational Theory [CHMPV LICS'23]



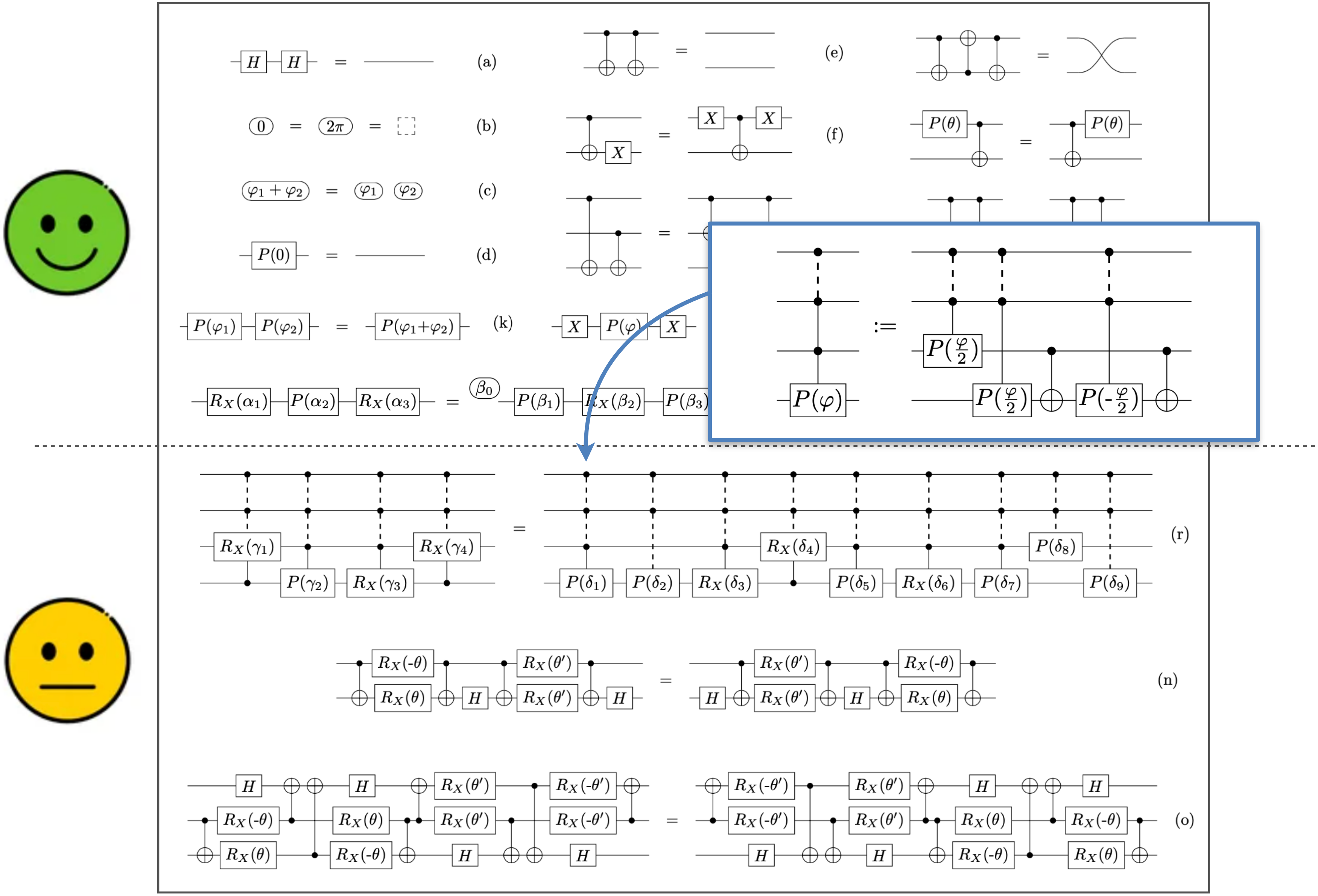
Complete Equational Theory [CHMPV LICS'23]



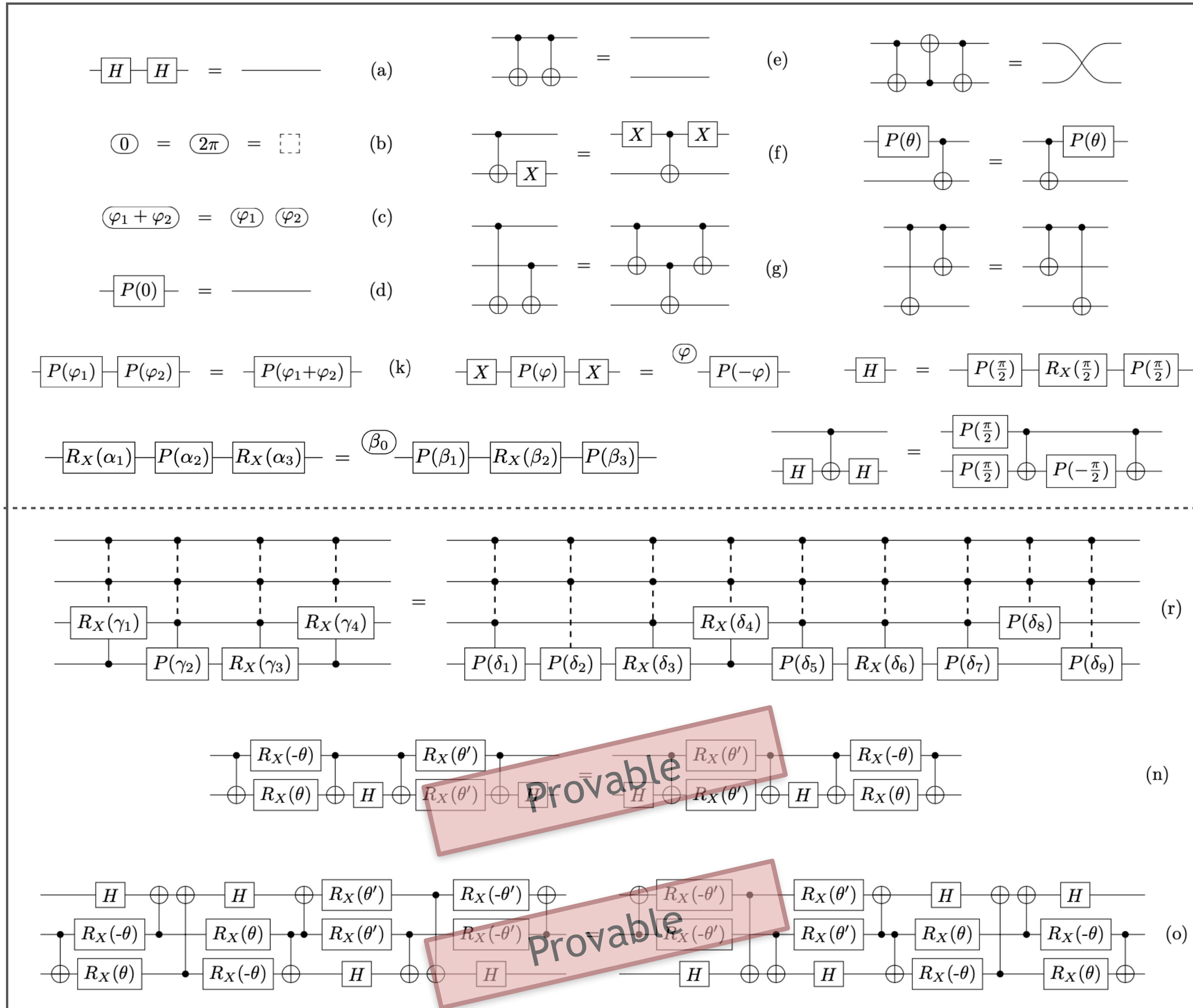
Complete Equational Theory [CHMPV LICS'23]



Complete Equational Theory [CHMPV LICS'23]



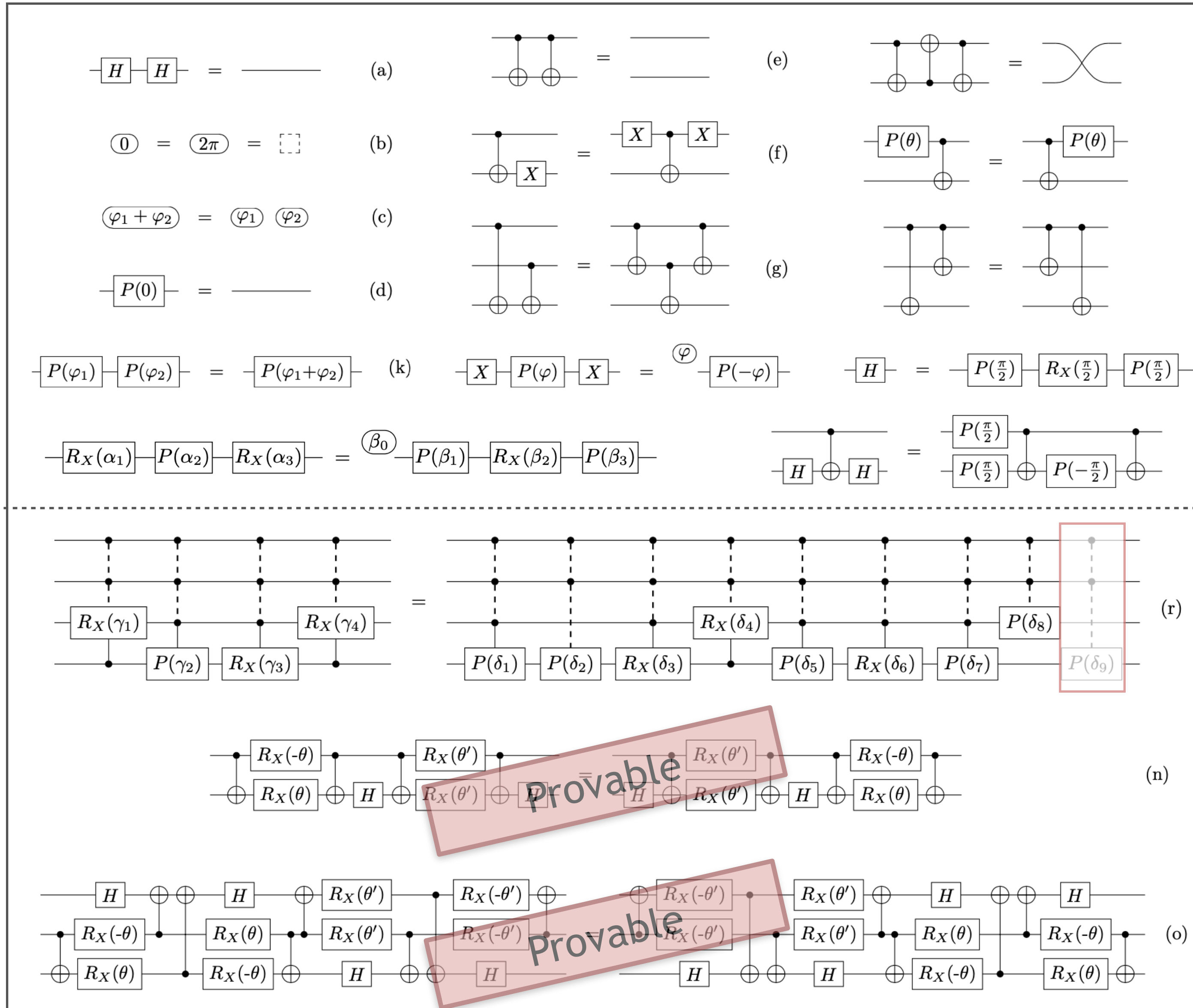
Complete Equational Theory [CHMPV LICS'23]



Property [CDPV QPL23]

(n) and (o) can be derived from the other equations, and (r) (slightly) simplified

Complete Equational Theory [CHMPV LICS'23]

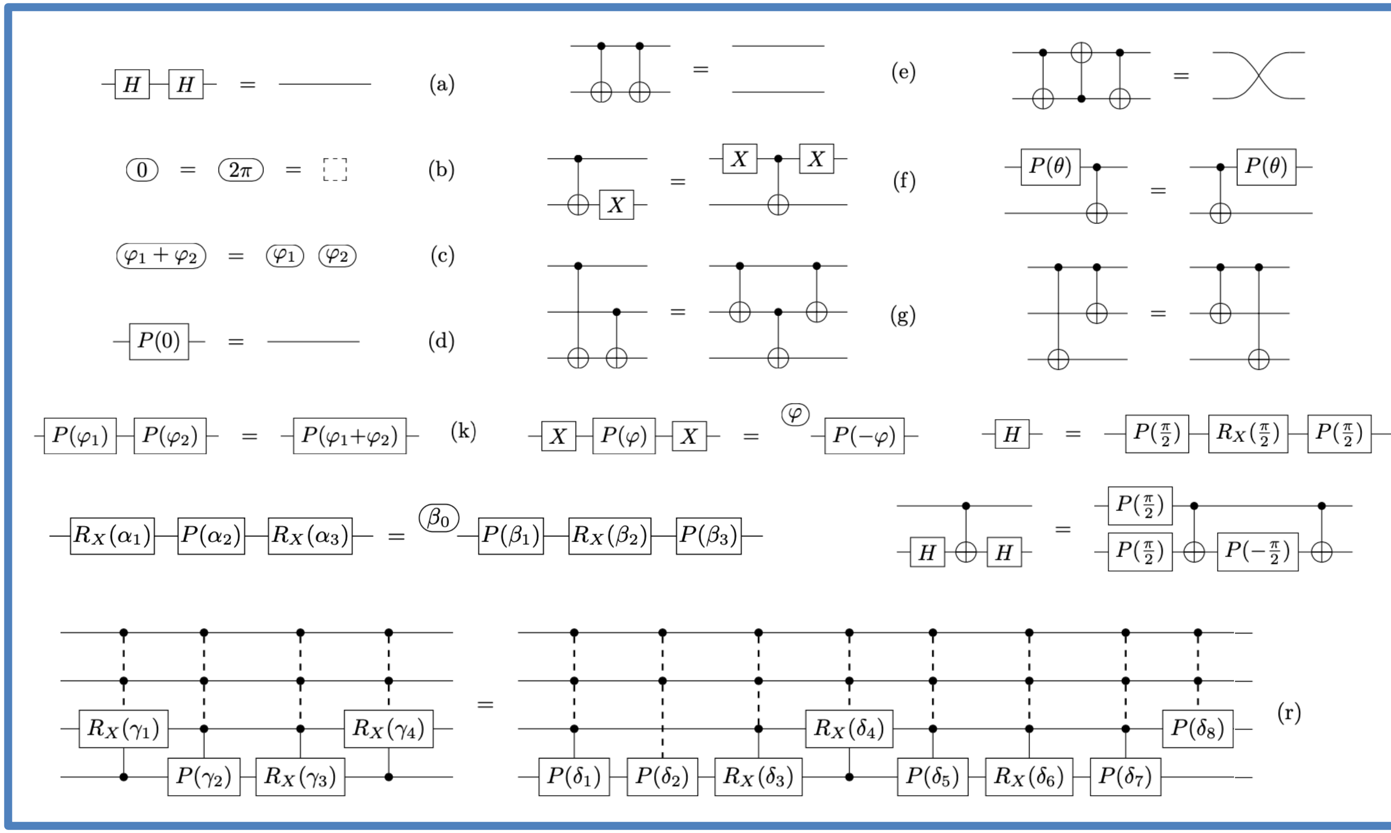


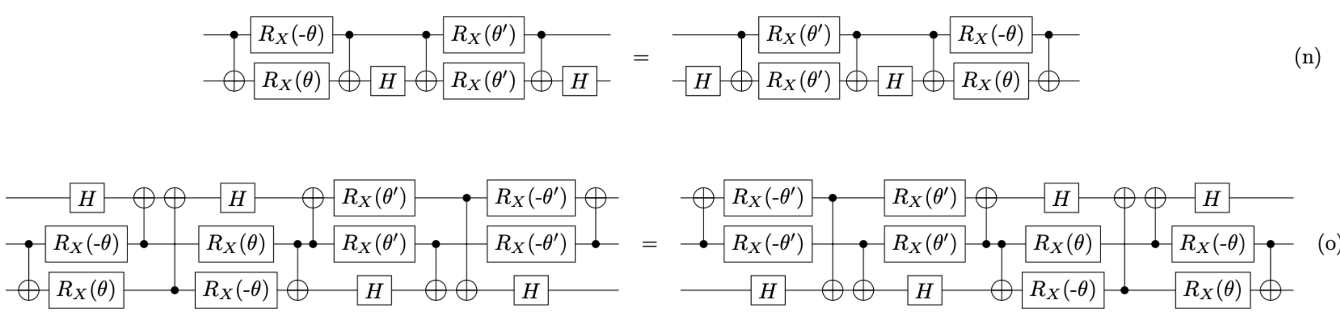
Property **[CDPV QPL23]**

(n) and (o) can be derived from the other equations, and (r) (slightly) simplified

Equational Theory

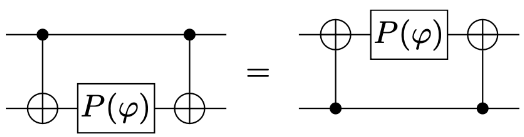
QC





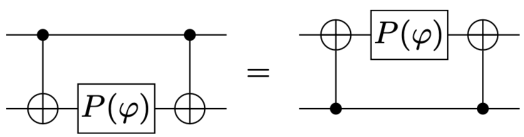
Derivations in QC

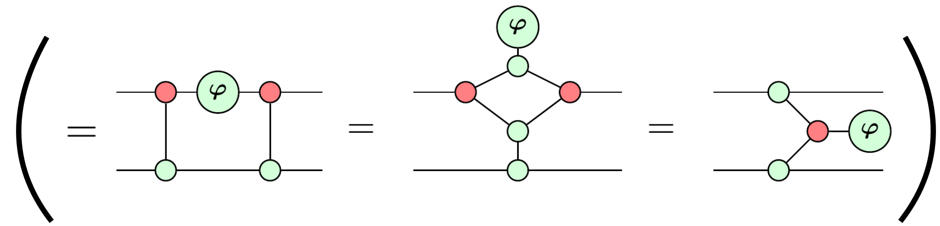
- Useful properties, e.g.:

QC $\vdash$ 

Derivations in QC

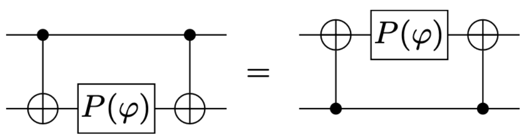
- Useful properties, e.g.:

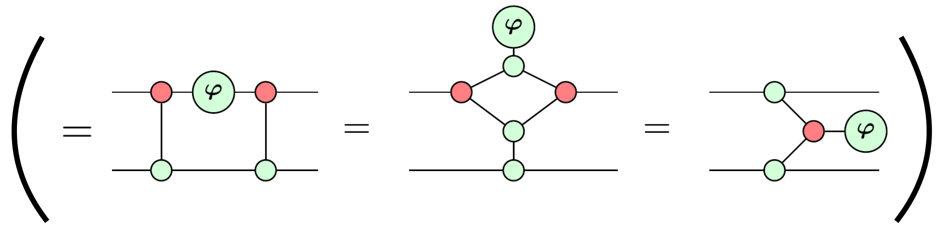
QC $\vdash$ 



Derivations in QC

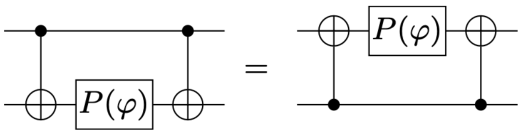
- Useful properties, e.g.: **Phase gadget**

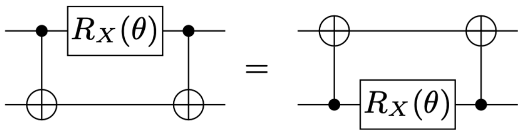
QC ⊢ 

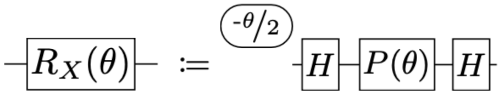


Derivations in QC

- Useful properties, e.g.: **Phase gadget**

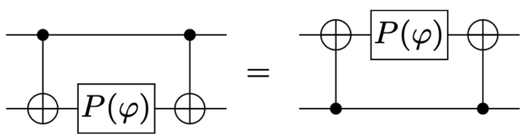
QC $\vdash$ 

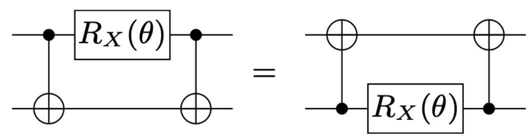
QC $\vdash$ 

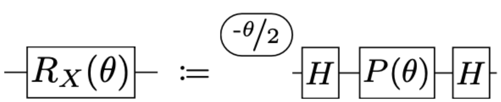
where 

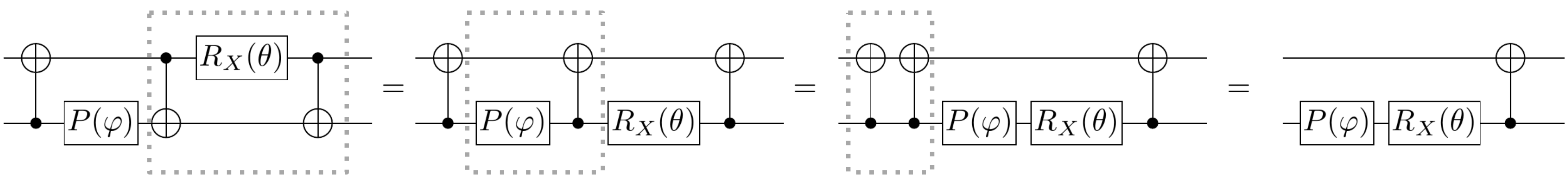
Derivations in QC

- Useful properties, e.g.: **Phase gadget**

QC $\vdash$ 

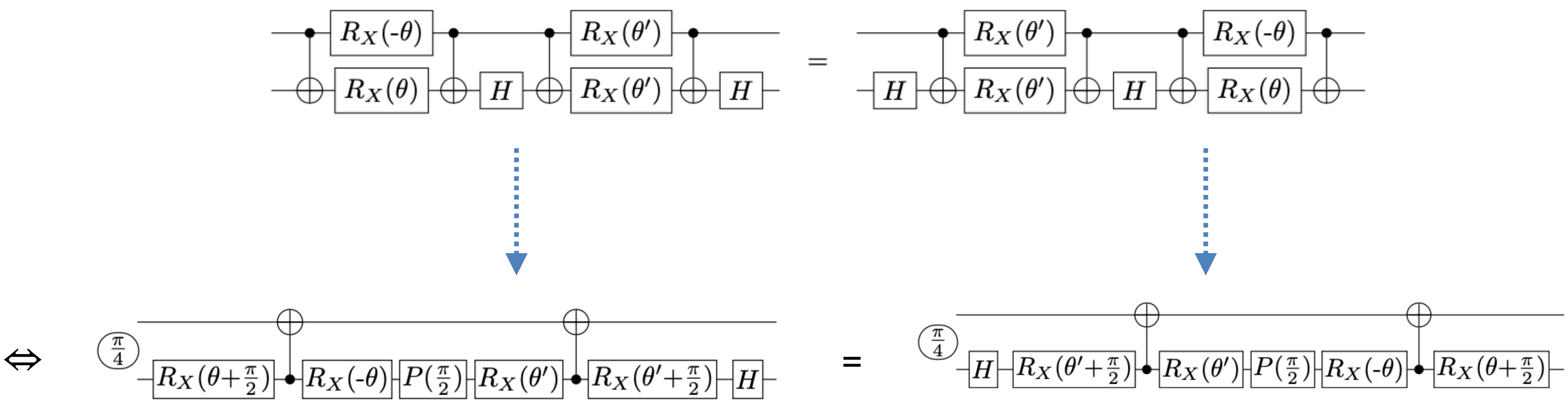
QC $\vdash$ 

where 



Derivations in QC

- Useful properties, e.g.: Phase gadget, Euler decomposition



Derivations in QC

- Useful properties
- **Simplification principal**

Definition For any quantum circuit C, let $C^\dagger$ be the *adjoint* of C inductively defined as $(C_2 \circ C_1)^\dagger := C_1^\dagger \circ C_2^\dagger$; $(C_1 \otimes C_2)^\dagger := C_1^\dagger \otimes C_2^\dagger$; and for any $\varphi \in \mathbb{R}$, $(\textcircled{\varphi})^\dagger := \textcircled{-\varphi}$, $(-\boxed{P(\varphi)}-)^\dagger := -\boxed{P(-\varphi)}-$, and $g^\dagger := g$ for any other generator g.

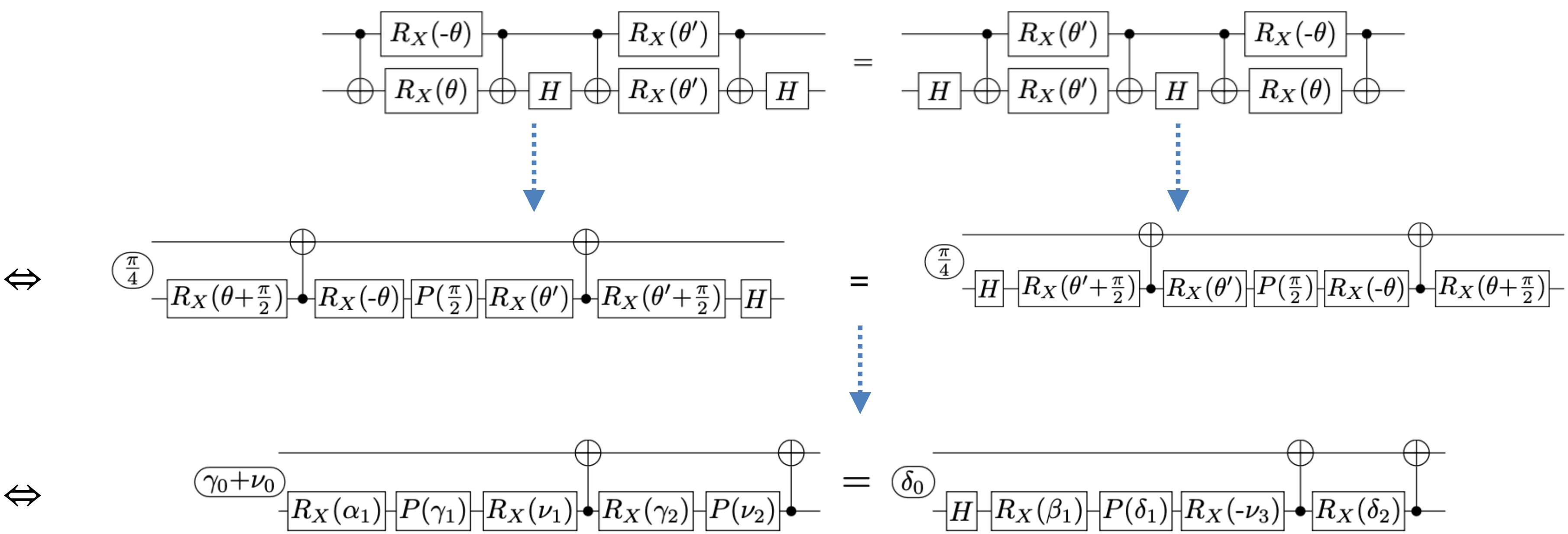
Proposition. For any circuit C, $\mathrm{QC} \vdash \boxed{C}\,\boxed{C^\dagger} = \overline{}$

Corollary. For any circuits C, C_0, C_1,

$$\mathrm{QC} \vdash \boxed{C_0}\,\boxed{C} = \boxed{C_1} \quad \Leftrightarrow \quad \mathrm{QC} \vdash \boxed{C_0} = \boxed{C_1}\,\boxed{C^\dagger}$$

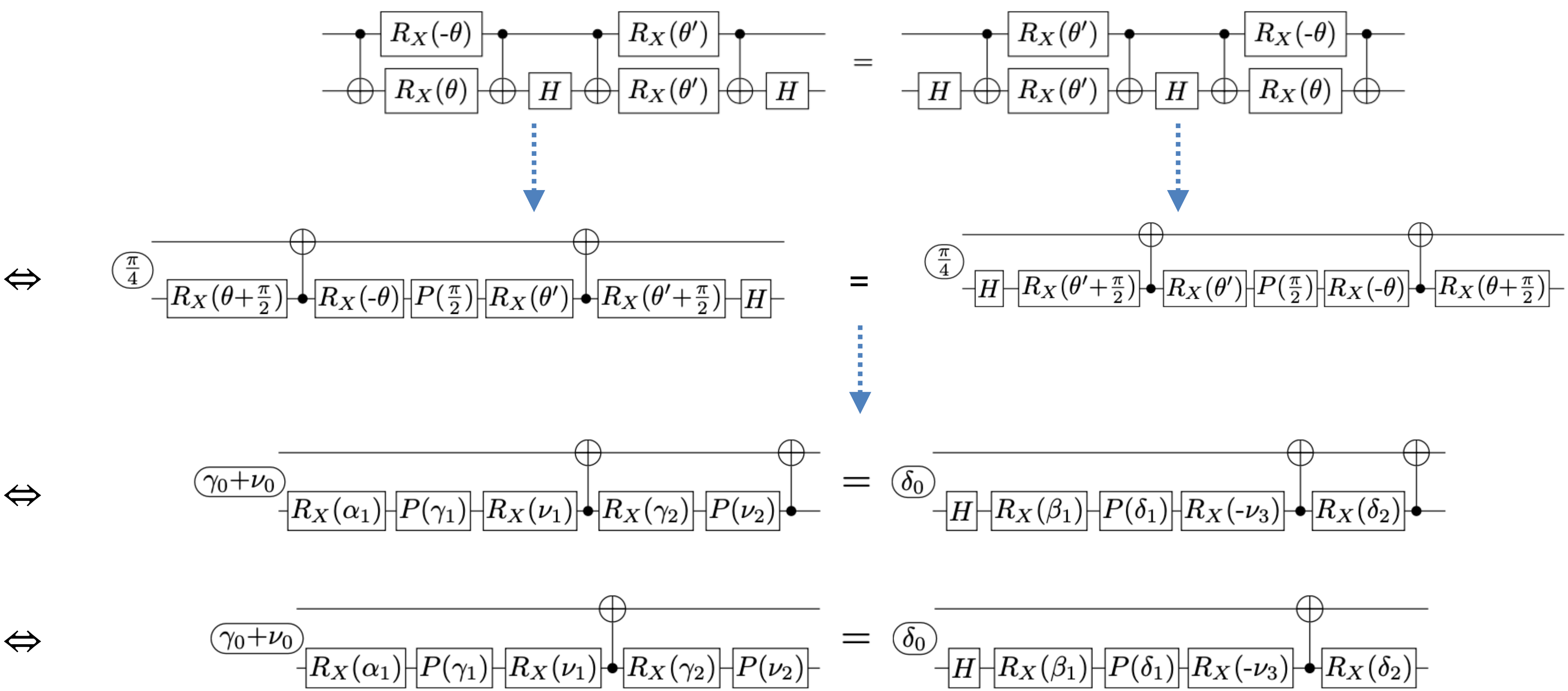
Derivations in QC

- Useful properties
- **Simplification principal**



Derivations in QC

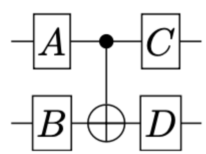
- Useful properties
- **Simplification principal**



Derivations in QC

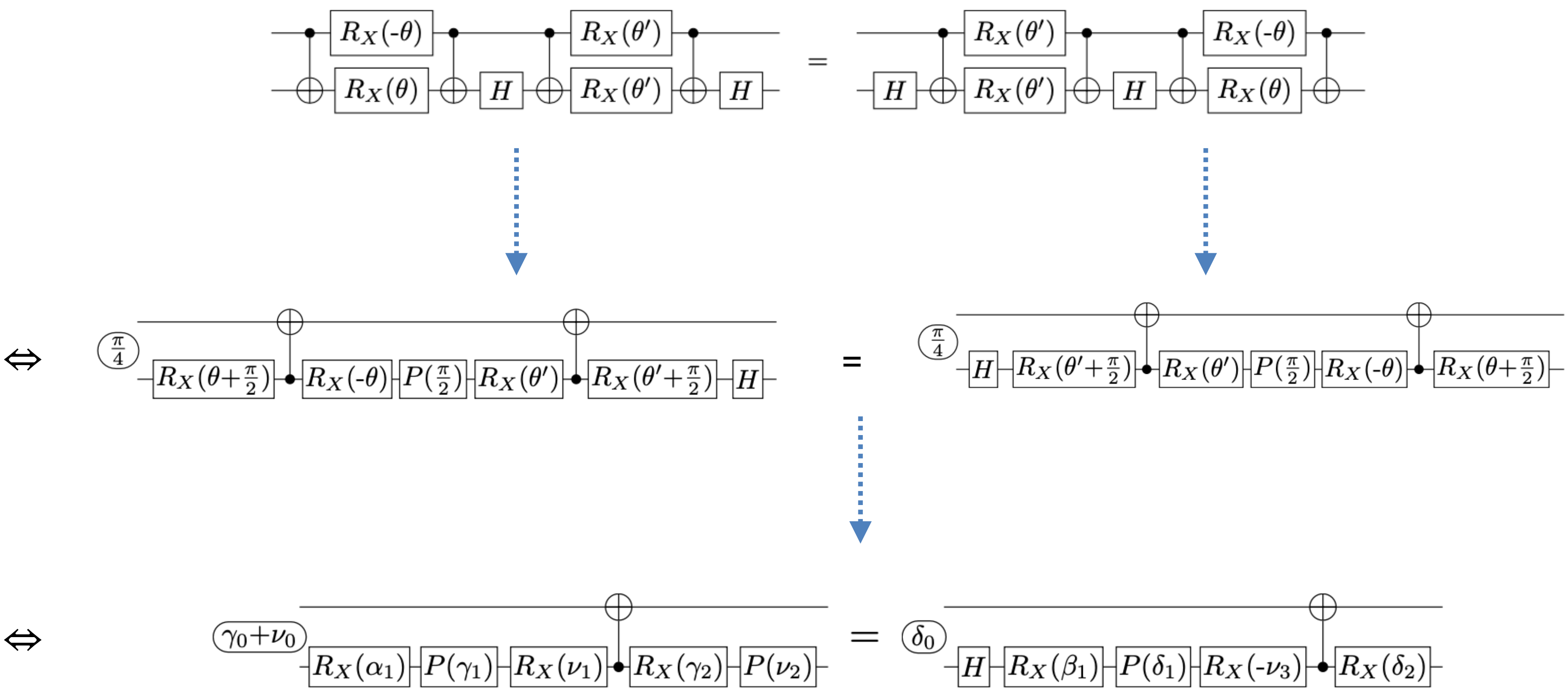
- Useful properties
- Simplification principal
- **1-CNot completeness**

Lemma. QC is complete for circuits containing at most one , i.e. for any quantum circuits $C_1, C_2 \in \mathbf{QC}$ with at most one , if $[\![C_1]\!] = [\![C_2]\!]$ then $\mathrm{QC} \vdash C_1 = C_2$.



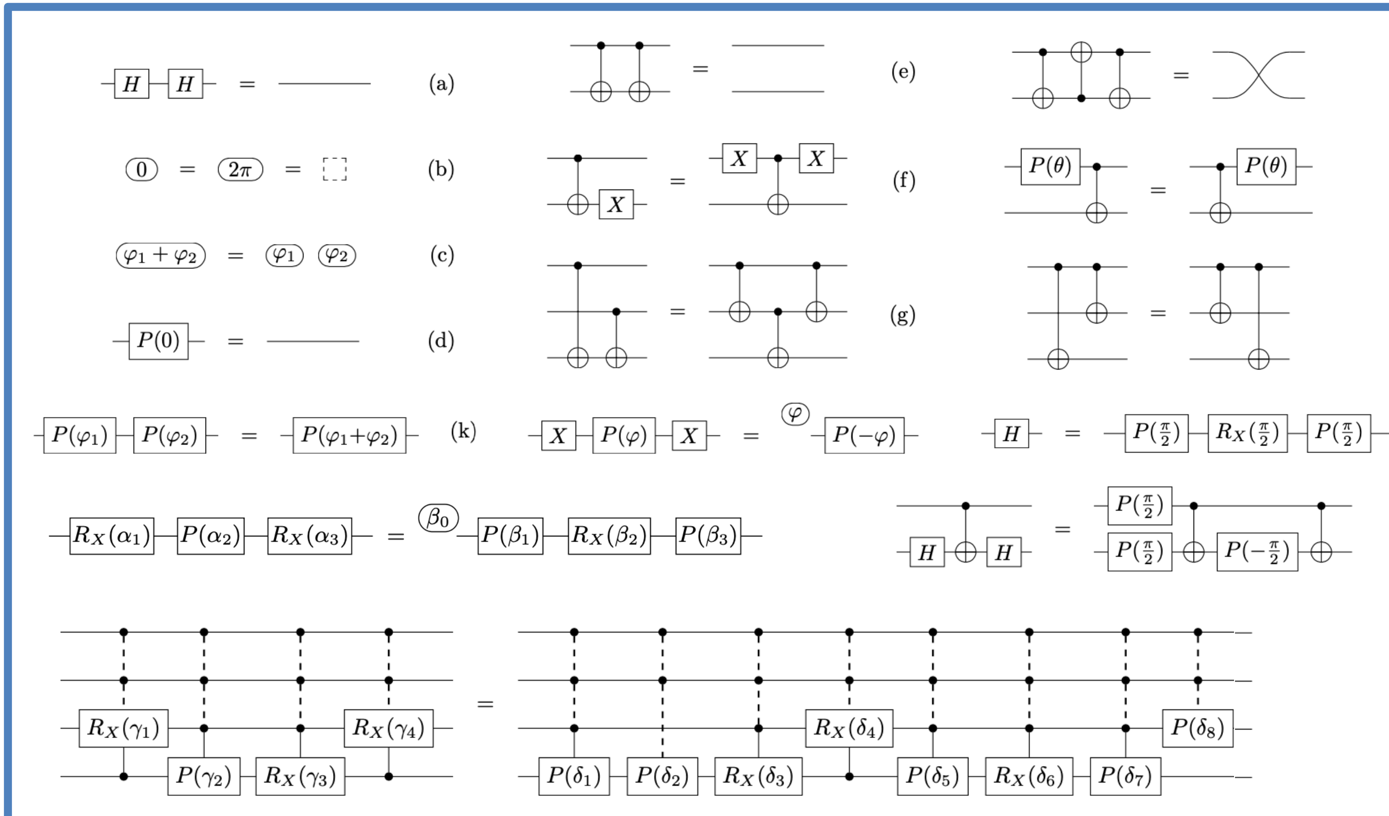
Derivations in QC

- Useful properties
- Simplification principal
- **1-CNot completeness**



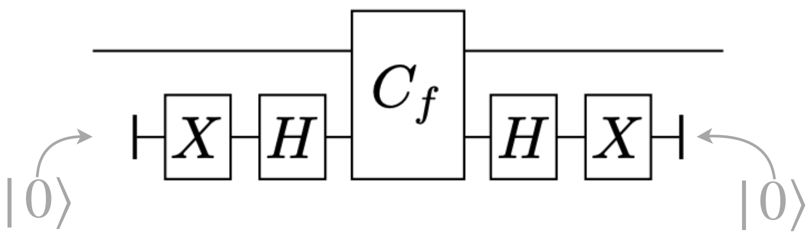
QC completeness

QC



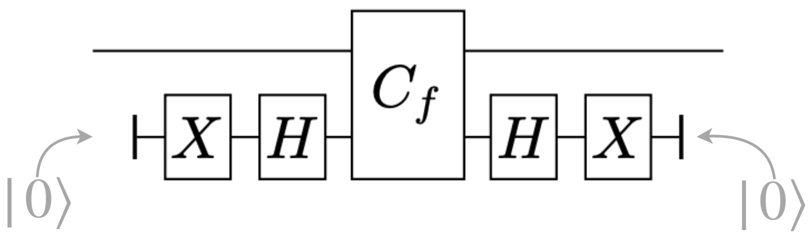
Theorem. QC is complete.

Quantum Circuits with
ancilla and/or trace out

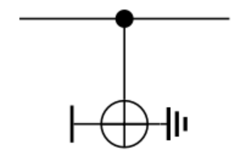


Universal for Isometries

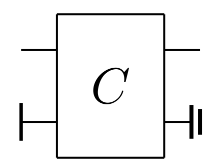
Quantum Circuits with
ancilla and/or trace out



Universal for Isometries



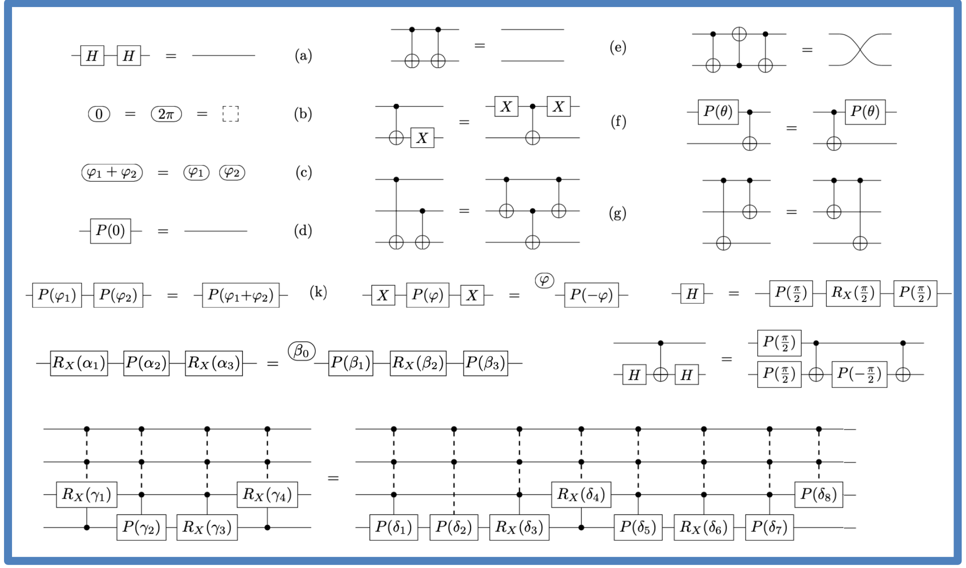
Universal for CPTP maps



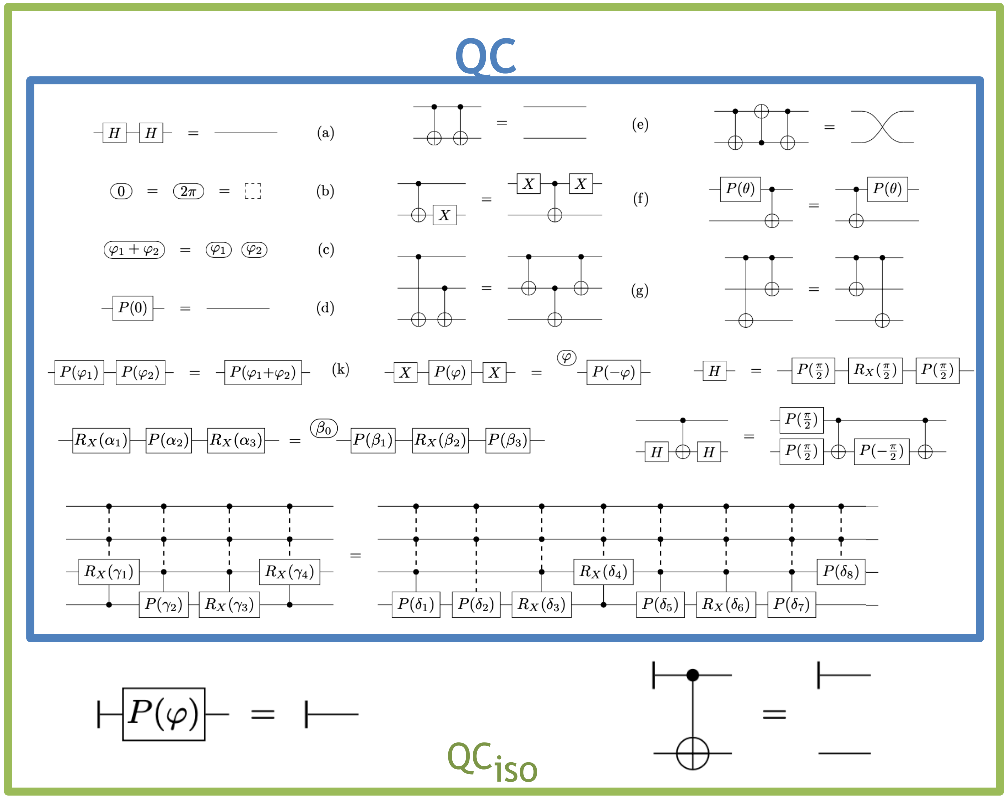
Quantum Circuits with

ancilla and/or trace out

QC



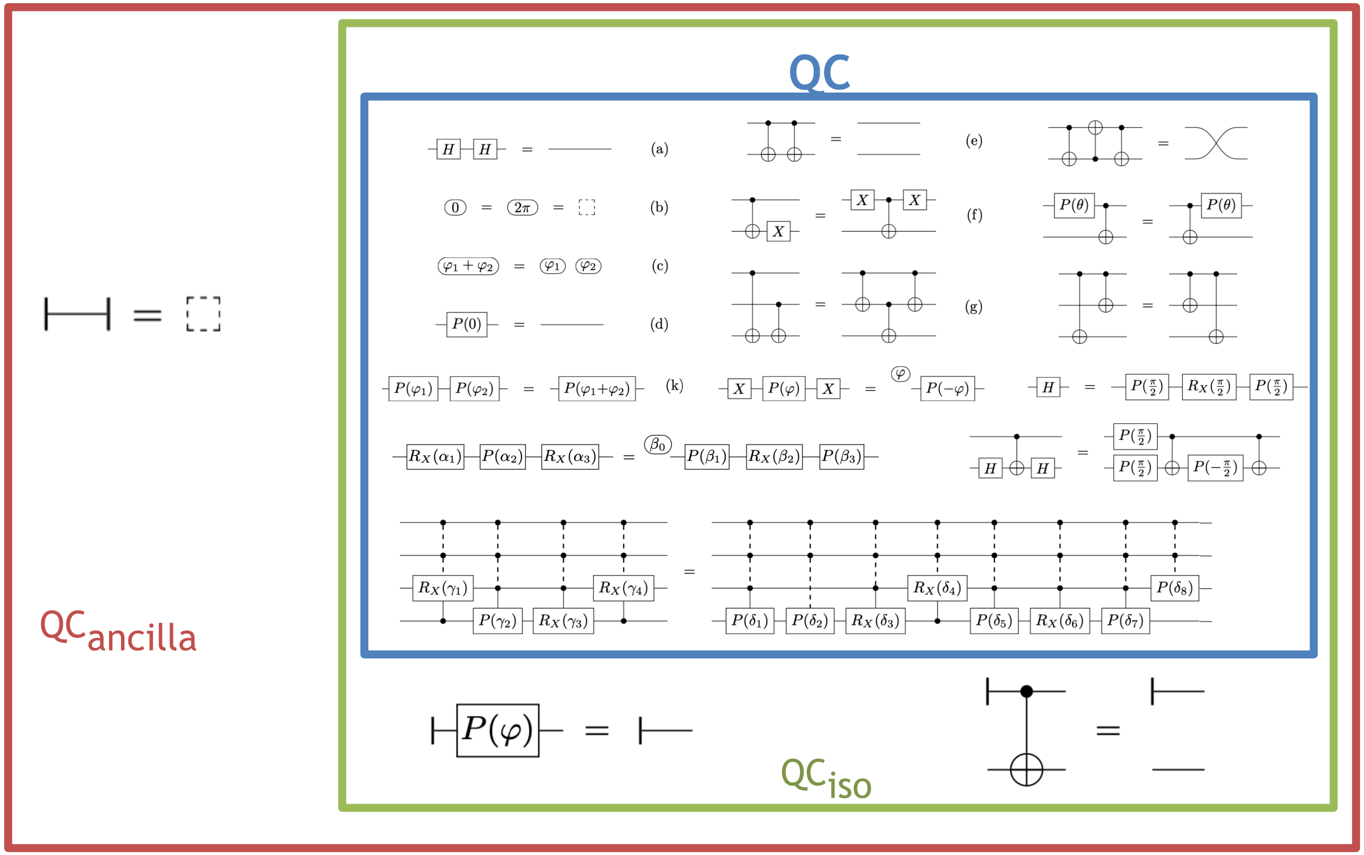
Quantum Circuits with
ancilla and/or trace out



Lemma. QC$_{iso}$ is complete for quantum circuits with qubit initialisation[1]

1 Using CSD or following S. Staton. Algebraic Effects, Linearity, and Quantum Programming Languages. POPL15

Quantum Circuits with
ancilla and/or trace out

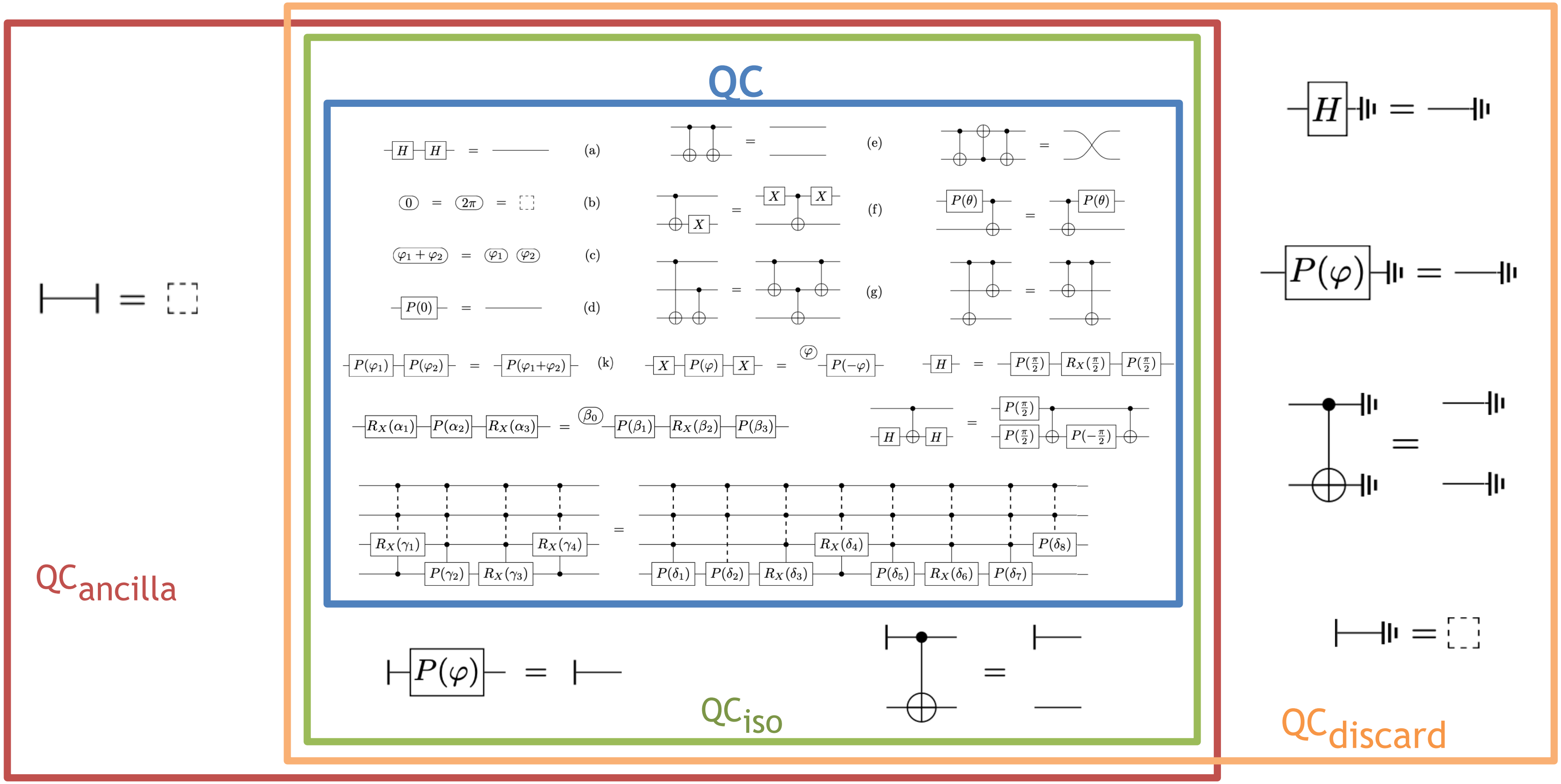


Lemma. QC$_{\text{iso}}$ is complete for quantum circuits with qubit initialisation[1]

Lemma. QC$_{\text{ancilla}}$ is complete for quantum circuits with ancilla

1 Using CSD or following S. Staton. Algebraic Effects, Linearity, and Quantum Programming Languages. POPL15

Quantum Circuits with
ancilla and/or trace out



Lemma. QC$_{\text{iso}}$ is complete for quantum circuits with qubit initialisation[1]

Lemma. QC$_{\text{ancilla}}$ is complete for quantum circuits with ancilla

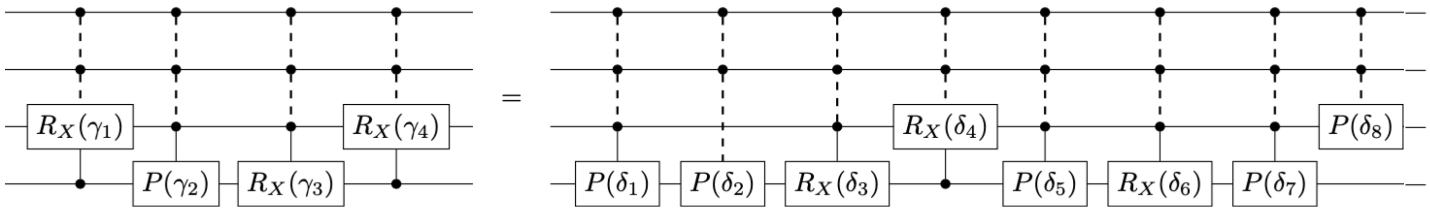
Lemma. QC$_{\text{discard}}$ is complete for quantum circuits with discard[2]

1 Using CSD or following S. Staton. Algebraic Effects, Linearity, and Quantum Programming Languages. POPL15

2 Using construction from M. Huot and S. Staton. Quantum channels as a categorical completion. LICS19 or Carette, Jeandel, Perdrix Vilmart, discard construction ICALP19

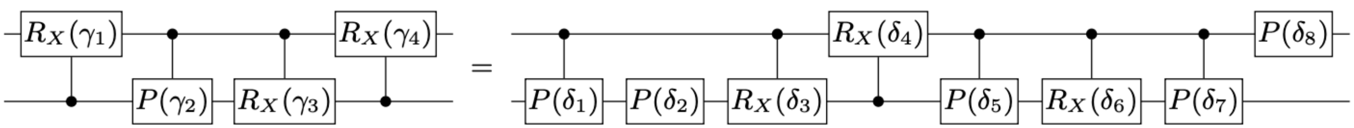
Simplifying (r)

Theorem. In $\mathrm{QC}_{\mathrm{ancilla}}$ and $\mathrm{QC}_{\mathrm{discard}}$, the family of equations

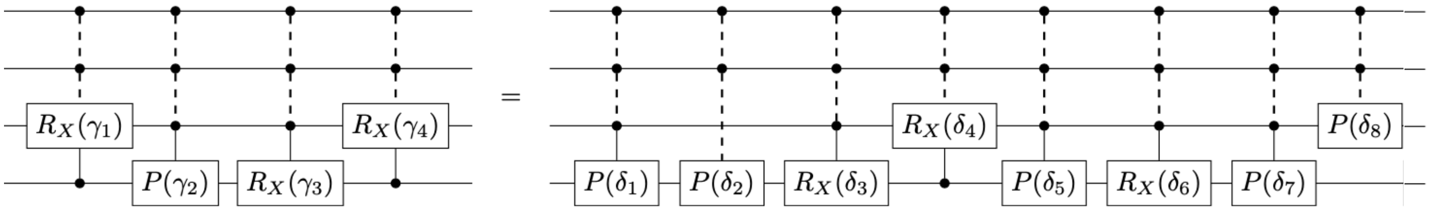


(r)

can be replaced by its 2-qubit case:

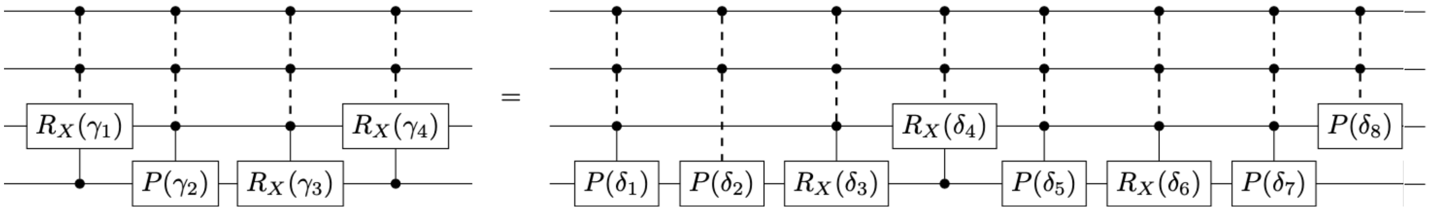


Simplifying (r)

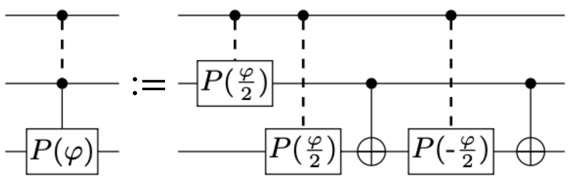


(r)

Simplifying (r)

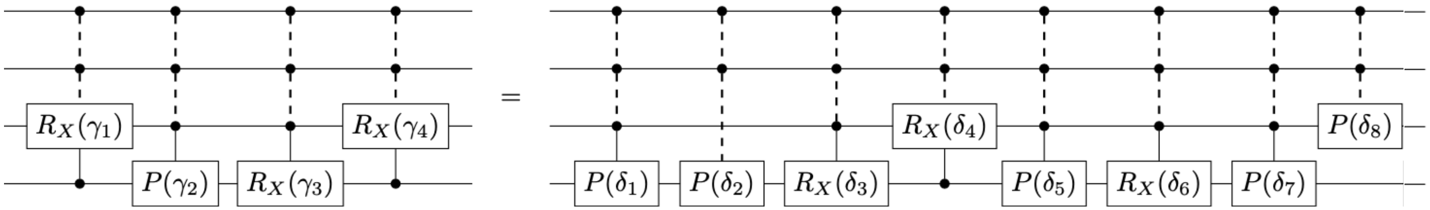


(r)

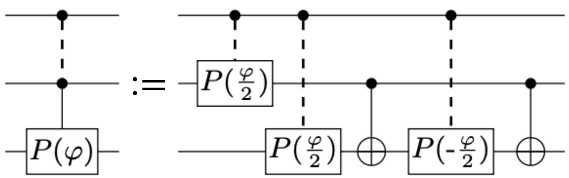


Simplifying (r)

$\forall \gamma_i, \exists \delta_j$ such that



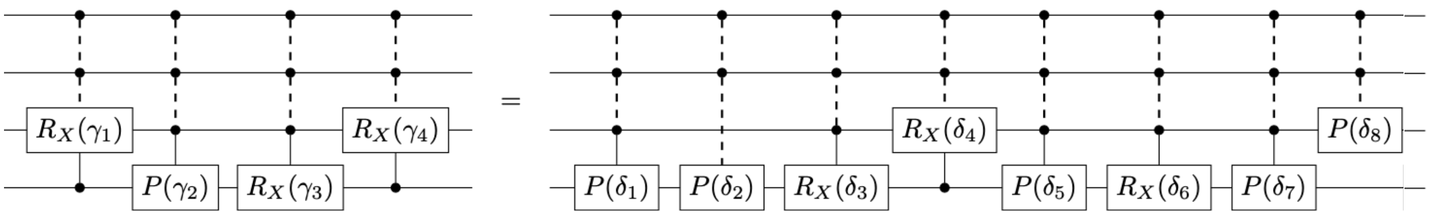
(r)



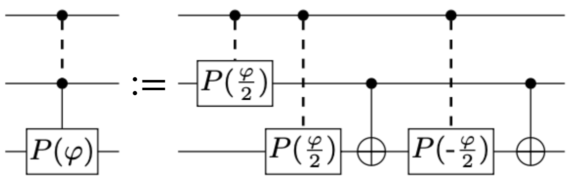
$$
\begin{aligned}
\delta_1 &= f_1(\gamma_1, \ldots, \gamma_4) \\
\delta_2 &= f_2(\gamma_1, \ldots, \gamma_4) \\
&\vdots \\
\delta_9 &= f_9(\gamma_1, \ldots, \gamma_4)
\end{aligned}
$$

Simplifying (r)

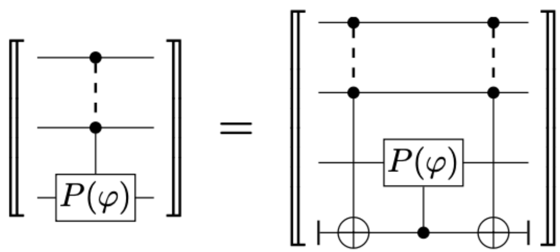
$\forall \gamma_i, \exists \delta_j$ such that



(r)

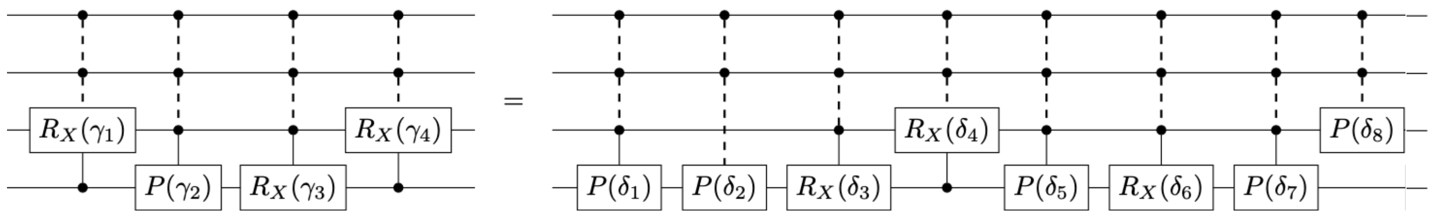


$$
\begin{aligned}
\delta_1 &= f_1(\gamma_1, \ldots, \gamma_4) \\
\delta_2 &= f_2(\gamma_1, \ldots, \gamma_4) \\
&\vdots \\
\delta_9 &= f_9(\gamma_1, \ldots, \gamma_4)
\end{aligned}
$$

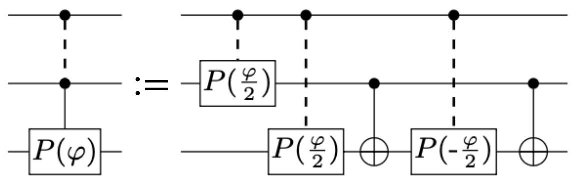


Simplifying (r)

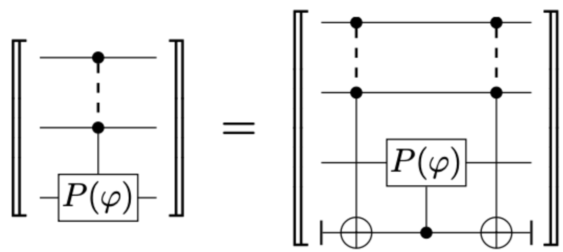
$\forall \gamma_i, \exists \delta_j$ such that



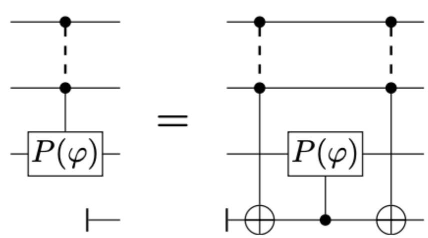
(r)



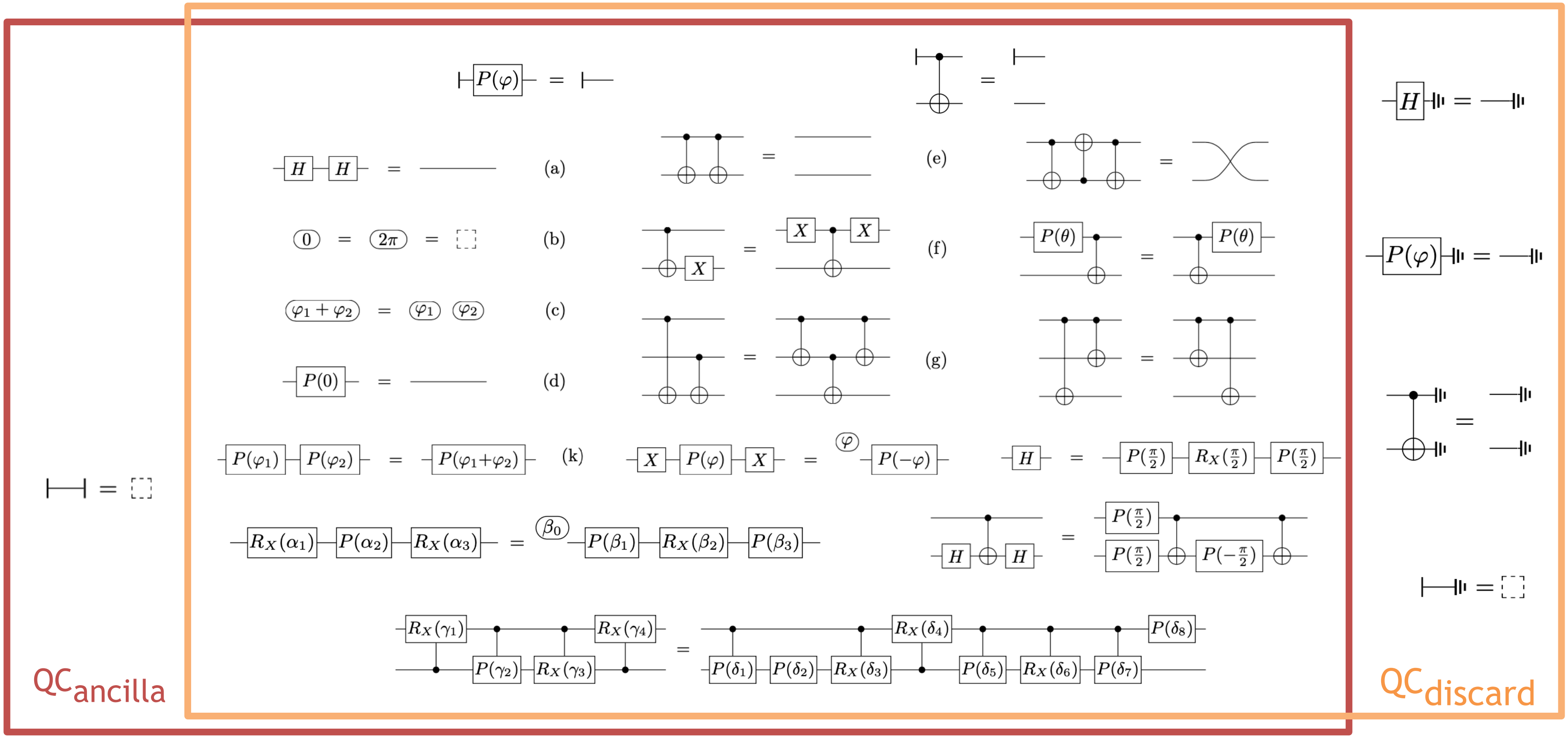
$$\begin{aligned} \delta_1 &= f_1(\gamma_1, \ldots, \gamma_4) \\ \delta_2 &= f_2(\gamma_1, \ldots, \gamma_4) \\ &\vdots \\ \delta_9 &= f_9(\gamma_1, \ldots, \gamma_4) \end{aligned}$$



Lemma. $\mathrm{QC}_{\text{ancilla}} \setminus (r) \vdash$



Quantum Circuits with
ancilla and/or trace out



Concluding remarks

Simplifying two out of the three most complicated rules

Complete equational theories for:

- Quantum circuits with qubit-initialisation
- Quantum circuits with ancilla
- Quantum circuits with initialisation and discard

Complete equational theories acting on at most 3 qubits for QC_{ancilla} and QC_{discard}.

Quantum circuit reasoning in action.