Escape the Matrix: Graphical Reasoning and Minimal Axioms for Quantum Circuits

Colin Blake

PhD Day Edition 2025

May 6, 2025

Outline

Motivation: The Matrix Problem

What happens if you try to verify a *20-gate* quantum circuit by hand?

- You multiply 20 matrices, each $2^n \times 2^n$, by hand
- Errors multiply and it becomes intractable for even 5 qubits

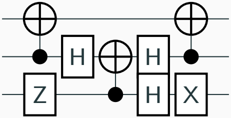
Motivation: The Matrix Problem

What happens if you try to verify a *20-gate* quantum circuit by hand?

- You multiply 20 matrices, each $2^n \times 2^n$, by hand
- Errors multiply and it becomes intractable for even 5 qubits

Motivation: Diagrams to the Rescue

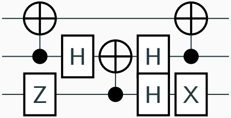
How graphical reasoning turns that mountain of matrices into friendly diagrams



- Rewrite rules on wires & nodes
- Local transformations, no full-blown matrix multiplication
- Fully automated in tools like `Quantomatic`, `PyZX`, ...

Motivation: Diagrams to the Rescue

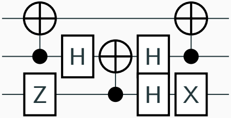
How graphical reasoning turns that mountain of matrices into friendly diagrams



- Rewrite rules on wires & nodes
- Local transformations, no full-blown matrix multiplication
- Fully automated in tools like `Quantomatic`, `PyZX`, ...

Motivation: Diagrams to the Rescue

How graphical reasoning turns that mountain of matrices into friendly diagrams

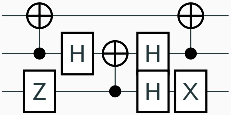


- Rewrite rules on wires & nodes
- Local transformations, no full-blown matrix multiplication
- Fully automated in tools like `Quantomatic`, `PyZX`, ...

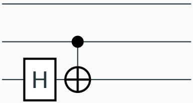
Circuit Optimization with Rewrites

Goal: Simplify a complex quantum circuit while preserving its function.

Before:



After:



Such rewrites come from a set of *equational rules* (axioms).

Equational Theory: Musical Analogy

- **Generators:** Musical note durations (whole, half, quarter, ...)
- **Equations:** Duration identities, e.g. half $+$ half $=$ whole
- Minimal identities suffice to express all timing equivalences

Equational Theory: Musical Analogy

- **Generators:** Musical note durations (whole, half, quarter, ...)
- **Equations:** Duration identities, e.g. half + half = whole
- Minimal identities suffice to express all timing equivalences

Equational Theory: Musical Analogy

- **Generators:** Musical note durations (whole, half, quarter, ...)
- **Equations:** Duration identities, e.g. half $+$ half $=$ whole
- Minimal identities suffice to express all timing equivalences

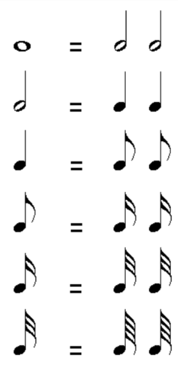
Note Duration Example

Original

half note + half note

Rewritten

whole note



A small, minimal rule delivers powerful rewriting capabilities.

What is Completeness?

A set of circuit equations is **complete** if:

- *Any* two circuits implementing the same unitary can be transformed into each other by these rules.
- Guarantees no missing identities: every true equality is derivable.

Why it matters: Ensures we can automate verification of equivalence.

What is Completeness?

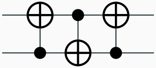
A set of circuit equations is **complete** if:

- *Any* two circuits implementing the same unitary can be transformed into each other by these rules.
- Guarantees no missing identities: every true equality is derivable.

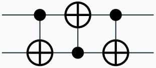
Why it matters: Ensures we can automate verification of equivalence.

Completeness Example: SWAP Circuits

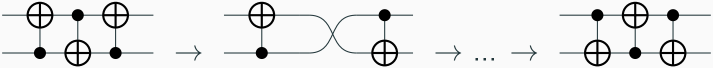
Two implementations of a SWAP gate:



(3 CNOTs)



A complete theory provides a sequence of rewrites:



proving semantic equivalence without matrices.

What is Minimality?

- **Minimality:** No axiom is redundant.
- Removing any single rule breaks completeness: some equalities become unprovable.
- Think of each axiom as a "+1 leg" supporting the theory table.

What is Minimality?

- **Minimality:** No axiom is redundant.
- Removing any single rule breaks completeness: some equalities become unprovable.
- Think of each axiom as a "+1 leg" supporting the theory table.

What is Minimality?

- **Minimality:** No axiom is redundant.
- Removing any single rule breaks completeness: some equalities become unprovable.
- Think of each axiom as a "+1 leg" supporting the theory table.

Proving Independence via Interpretations

- To show axiom X is necessary:
  - Construct an *alternate interpretation* where all other axioms hold,
  - But axiom X fails (gives different semantics).
- This counter-model demonstrates X cannot be derived from the rest.

Example: Interpretation which counts the parity of some generators.

Proving Independence via Interpretations

- To show axiom X is necessary:
  - Construct an *alternate interpretation* where all other axioms hold,
  - But axiom X fails (gives different semantics).
- This counter-model demonstrates X cannot be derived from the rest.

Example: Interpretation which counts the parity of some generators.

Proving Independence via Interpretations

- To show axiom X is necessary:
  - Construct an *alternate interpretation* where all other axioms hold,
  - But axiom X fails (gives different semantics).
- This counter-model demonstrates X cannot be derived from the rest.

Example: Interpretation which counts the parity of some generators.

Proving Independence via Interpretations

- To show axiom X is necessary:
  - Construct an *alternate interpretation* where all other axioms hold,
  - But axiom X fails (gives different semantics).
- This counter-model demonstrates X cannot be derived from the rest.

Example: Interpretation which counts the parity of some generators.

Qubit Clifford & Real Clifford

- **Qubit Clifford** : Core operations. Widely used for error correction and efficient classical simulation. It uses phases $\pm 1, \pm i$ (complex roots).
- **Real Clifford** : Same as Qubit Clifford but with only real-valued phases ± 1, akin to working over $\mathbb{Z}_2$ instead of $\mathbb{Z}_4$.

Qubit Clifford & Real Clifford

- **Qubit Clifford** : Core operations. Widely used for error correction and efficient classical simulation. It uses phases $\pm 1, \pm i$ (complex roots).
- **Real Clifford** : Same as Qubit Clifford but with only real-valued phases ± 1, akin to working over $\mathbb{Z}_2$ instead of $\mathbb{Z}_4$.

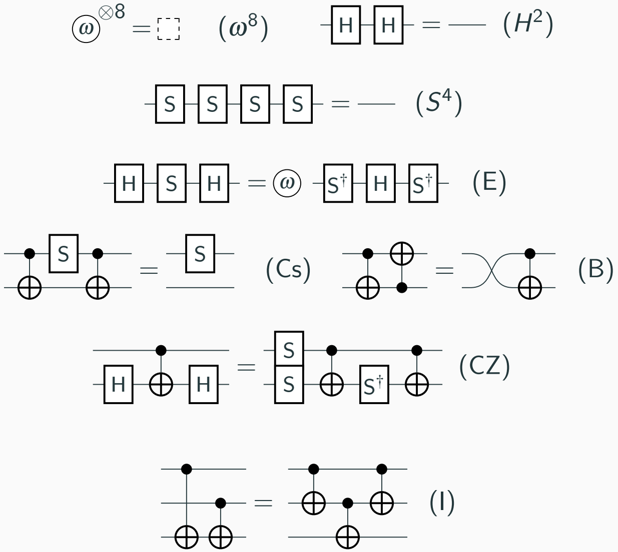
Qutrit Clifford & Clifford+T

- **Qutrit Clifford** : Generalizes Clifford operations to three-level systems for exploring higher-dimensional designs.
- **Qubit Clifford+T** : Adds the T gate to the Clifford set, achieving universal quantum computation. Central to circuit compiling and optimization.

Qutrit Clifford & Clifford+T

- **Qutrit Clifford** : Generalizes Clifford operations to three-level systems for exploring higher-dimensional designs.
- **Qubit Clifford+T** : Adds the T gate to the Clifford set, achieving universal quantum computation. Central to circuit compiling and optimization.

Equational Theory for Qubit Clifford Circuits



Example: Necessity of H^2 Axiom

Interpretation: Checks the presence of H gates in a circuit

$\mathsf{C}_2 \to \mathbb{B}$: a H will be True and any other generator will be False

Composition uses `OR`

Example: Necessity of H^2 Axiom

Interpretation: Checks the presence of H gates in a circuit

$C_2 \to \mathbb{B}$: a H will be True and any other generator will be False

Composition uses `OR`

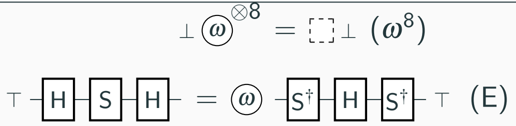
$$\bot \, \textcircled{\omega}^{\otimes 8} = \boxed{} \bot \; (\omega^8)$$

Example: Necessity of H^2 Axiom

Interpretation: Checks the presence of H gates in a circuit

$C_2 \to \mathbb{B}$: a H will be True and any other generator will be False

Composition uses `OR`

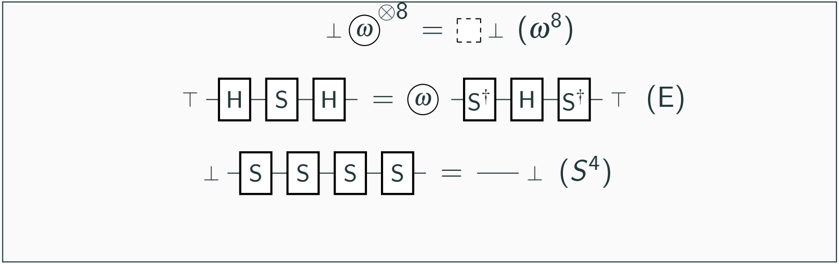


Example: Necessity of H^2 Axiom

Interpretation: Checks the presence of H gates in a circuit

$\mathrm{C}_2 \to \mathbb{B}$: a H will be True and any other generator will be False

Composition uses `OR`

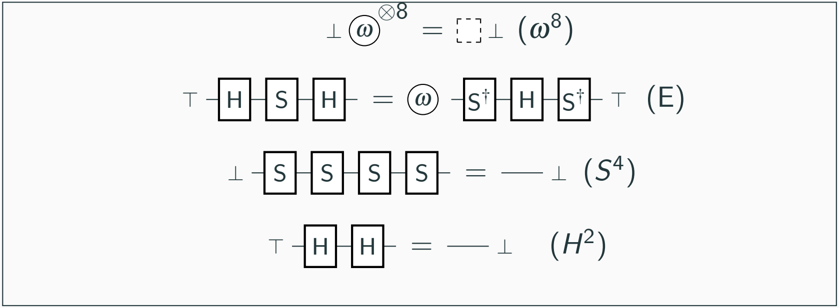


Example: Necessity of H^2 Axiom

Interpretation: Checks the presence of H gates in a circuit

$C_2 \to \mathbb{B}$: a H will be True and any other generator will be False

Composition uses `OR`



Example: Necessity of CZ Axiom

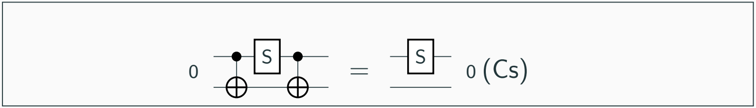
Interpretation: Count the number of CNOT and SWAP gates in a circuit, mod 2.

$C_2 \to \mathbb{Z}_2$: even CNOTs and SWAPs $\to 0$, odd $\to 1$. Composition uses addition mod 2 (XOR).

Example: Necessity of CZ Axiom

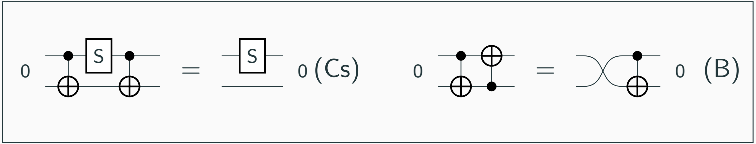
Interpretation: Count the number of CNOT and SWAP gates in a circuit, mod 2.

$C_2 \to \mathbb{Z}_2$: even CNOTs and SWAPs $\to 0$, odd $\to 1$. Composition uses addition mod 2 (XOR).



Example: Necessity of CZ Axiom

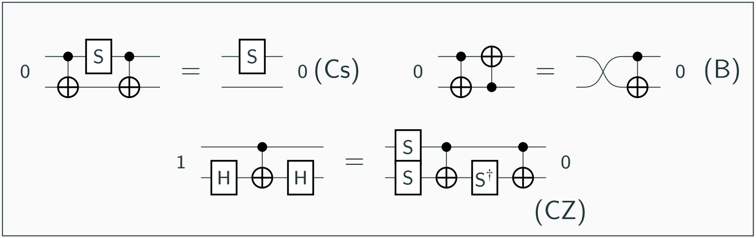
Interpretation: Count the number of CNOT and SWAP gates in a circuit, mod 2.
$C_2 \to \mathbb{Z}_2$: even CNOTs and SWAPs $\to 0$, odd $\to 1$. Composition uses addition mod 2 (XOR).



Example: Necessity of CZ Axiom

Interpretation: Count the number of CNOT and SWAP gates in a circuit, mod 2.

$C_2 \to \mathbb{Z}_2$: even CNOTs and SWAPs $\to$ 0, odd $\to$ 1. Composition uses addition mod 2 (XOR).



Comparison of Axiom Set Sizes

Fragment	Previous Theory	Our Theory
Qubit Clifford	15	8 (minimal for *n*-qubits)
Real Clifford	16	10 (minimal for *n*-qubits)
Qutrit Clifford	17	11 (minimal for 2-qutrits, conjectured for *n*)
Clifford+T	18	11 (minimal for 1-qubit, simplified for 2, no result for *n*)

Summary

- Graphical equational theories let us *reason* and *optimize* circuits visually.
- Our rule sets are *complete* (all true equivalences provable) and are *minimal* in the sense that we can't derive some equations from the others.
- Enables scalable *automation* in quantum compilation and verification.

Thank you! Questions?

Summary

- Graphical equational theories let us *reason* and *optimize* circuits visually.
- Our rule sets are *complete* (all true equivalences provable) and are *minimal* in the sense that we can't derive some equations from the others.
- Enables scalable *automation* in quantum compilation and verification.

Thank you! Questions?

Summary

- Graphical equational theories let us *reason* and *optimize* circuits visually.
- Our rule sets are *complete* (all true equivalences provable) and are *minimal* in the sense that we can't derive some equations from the others.
- Enables scalable *automation* in quantum compilation and verification.

Thank you! Questions?