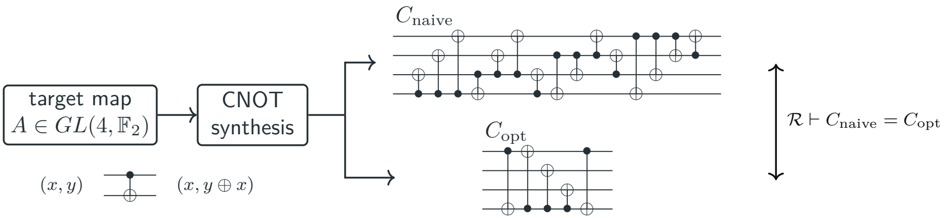
Simpler Presentations for Many Fragments of Quantum Circuits

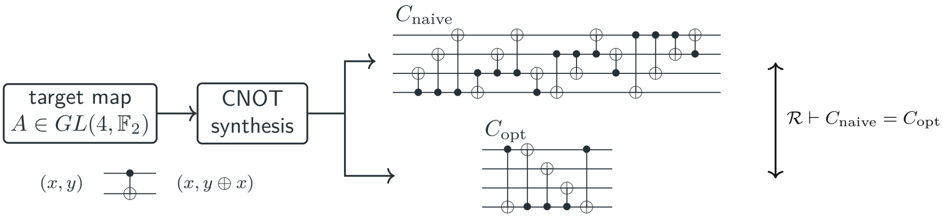
Colin Blake
Université de Lorraine, CNRS, Inria, LORIA

FSCD 2026, ISCTE, Lisbon, Portugal
20–23 July 2026

Completeness proves circuit equivalence



Completeness proves circuit equivalence



Definition (presentation, soundness, completeness)

A presentation $\langle \Sigma \mid \mathcal{R} \rangle$ fixes generators Σ and equations $\mathcal{R}$. For a semantics $[\![-]\!]$, it is *sound* when $\mathcal{R} \vdash C = D \Longrightarrow [\![C]\!] = [\![D]\!]$, and *complete* when $[\![C]\!] = [\![D]\!] \Longrightarrow \mathcal{R} \vdash C = D$.

Ways to prove completeness

Normal forms

$$C \iff \underbrace{N(U)}_{\text{unique}} \iff D$$

+ canonical representative
+ can become an algorithm
− hard to design for rich syntax
− must prove actual normalization

[Selinger 2015] [Li et al. 2025]

Group presentation

$$\langle G \mid R \rangle \;\cong\; \mathrm{Im}[\![-]\!]$$

+ proves generators and relations
+ good for discrete fragments
− relation sets can explode
− less natural with real parameters

[Bian–Selinger 2023a] [2023b]

Transfer

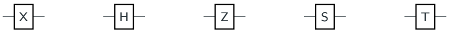
$$\begin{tikzcd} C = D \arrow[r, bend left, "E"] & C' = D' \arrow[l, bend left, "D"] \end{tikzcd}$$

+ reuses a complete calculus
+ isolates E, D, and mimicry
− expressivity must match
− auxiliary rules must decode

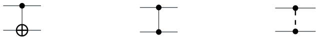
[Clément et al. 2022]

Six circuit fragments

local gates



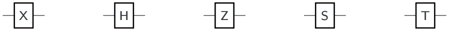
controlled gates



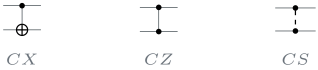
CX CZ CS

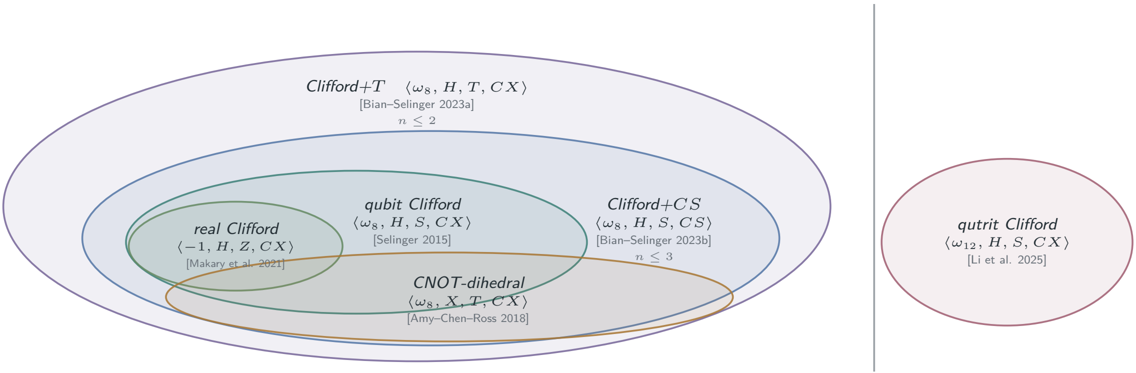
Six circuit fragments

local gates



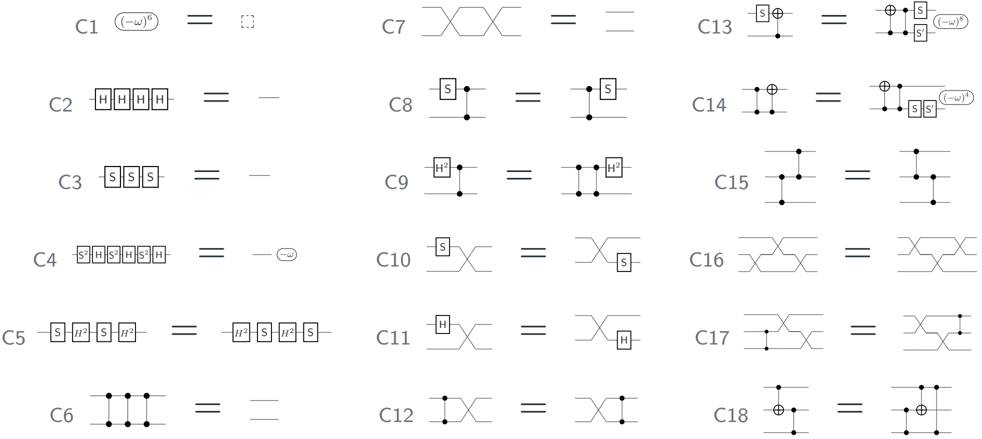
controlled gates





Start with qutrit Clifford

Source complete PRO presentation for qutrit Clifford circuits [Li et al. 2025].



PROs compose circuits

Definition

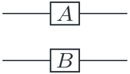
A *PRO* is a strict monoidal category $\mathcal{P}$ with objects $\mathbb{N}$, tensor $m \otimes n = m + n$, and unit 0.

Read n as n *wires*; a morphism $C : n \to m$ as a circuit with n inputs and m outputs.

sequential

$B \circ A$

parallel

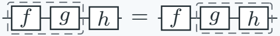


$A \otimes B$

identity

$f \circ \mathrm{id} = f = \mathrm{id} \circ f$

associativity

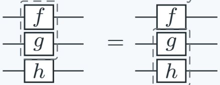


$h \circ (g \circ f) = (h \circ g) \circ f$

tensor unit

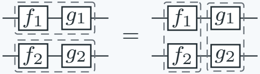
$f \otimes \mathrm{id}_0 = f = \mathrm{id}_0 \otimes f$

tensor associativity



$(f \otimes g) \otimes h = f \otimes (g \otimes h)$

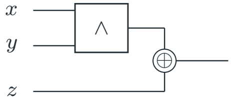
interchange



$(g_1 \circ f_1) \otimes (g_2 \circ f_2) = (g_1 \otimes g_2) \circ (f_1 \otimes f_2)$

PROs model classical networks

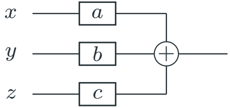
Boolean circuits



$$(x \wedge y) \oplus z$$

[Lafont 2003]

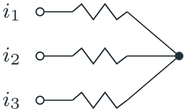
Signal-flow diagrams



$$ax + by + cz$$

[Bonchi–Sobociński–Zanasi 2017]

Electrical networks

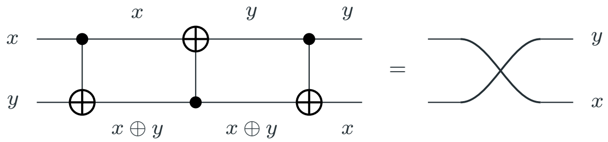


$$i_1 + i_2 + i_3 = 0$$

[Baez–Coya–Rebro 2017]

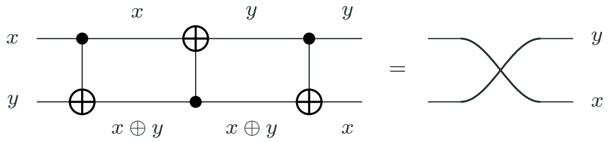
Qubits hide qutrit corrections

On two qubits, three controlled additions exchange the wires.



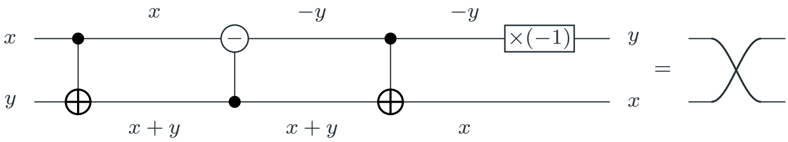
Qubits hide qutrit corrections

On two qubits, three controlled additions exchange the wires.



Is it still a swap on qutrits?

Qubits hide qutrit corrections



$\mathbb{Z}_2$: $-u = u$, so both corrections collapse. $\mathbb{Z}_3$: both remain.

PROPs make swaps structural

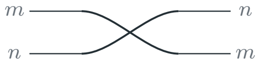
Definition

A *PROP* is a strict symmetric monoidal category $\mathcal{P}$ with

$$\mathrm{Ob}(\mathcal{P}) = \mathbb{N}, \qquad I = 0,$$
$$m \otimes n = m + n.$$

Its symmetry contains a natural family

$$\sigma_{m,n} : m+n \longrightarrow n+m \qquad (m, n \in \mathbb{N})$$



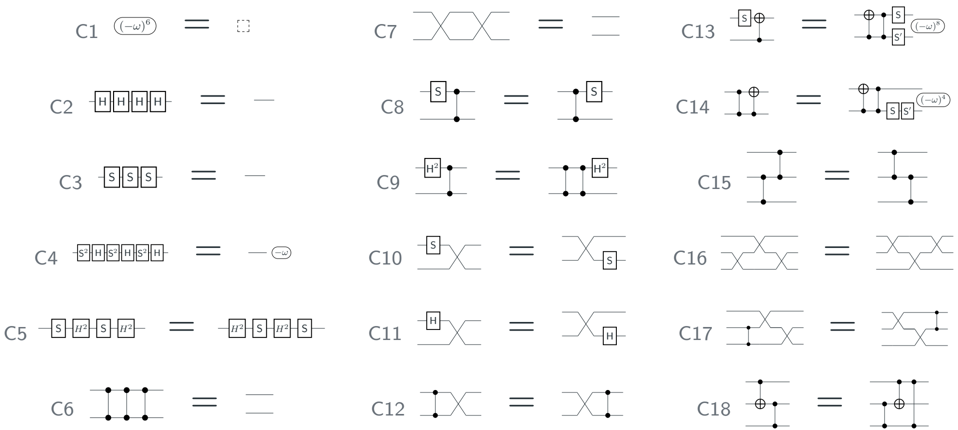
involution

$$\sigma_{n,m} \circ \sigma_{m,n} = \mathrm{id}_{m+n}$$

naturality

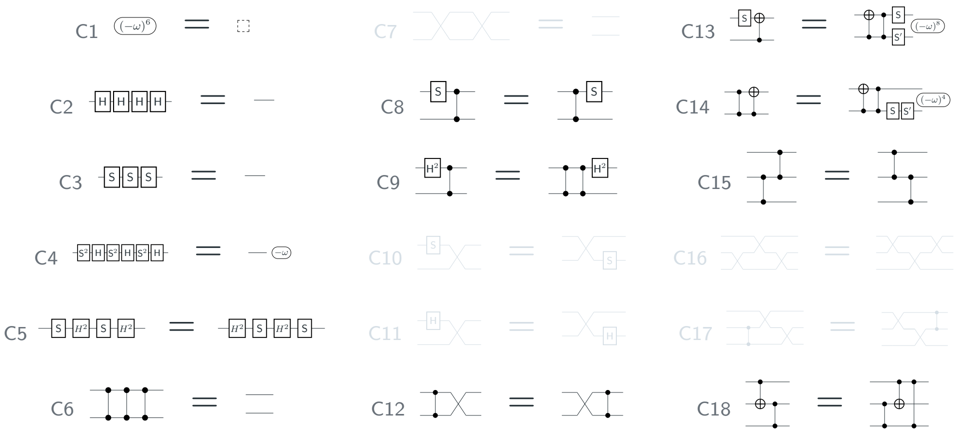
$$\sigma \circ (f \otimes \mathrm{id}) = (\mathrm{id} \otimes f) \circ \sigma$$

Swap equations become structural



The *faded rows* are supplied by *PROP symmetry*: $\sigma^2 = \mathrm{id}$, naturality, and symmetric monoidal coherence.

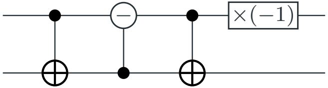
Swap equations become structural



The *faded rows* are supplied by *PROP symmetry*: $\sigma^2 = \mathrm{id}$, naturality, and symmetric monoidal coherence.

One equation transfers completeness

circuit term $\tau : 2 \to 2$ | *structural symmetry* $\sigma_{1,1}$



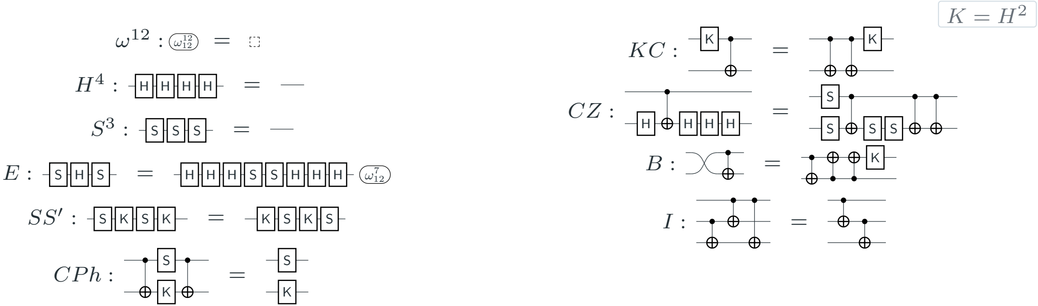
$=$

Completeness transfer

For a PROP term D, let D^τ be the PRO term obtained by replacing each structural crossing by the circuit τ. If $\langle \Sigma \mid \mathcal{R} \rangle_{\mathrm{PRO}}$ is complete and $[\![\tau]\!]$ is the wire swap, then $\langle \Sigma \mid \mathcal{R}, \sigma_{1,1} = \tau \rangle_{\mathrm{PROP}}$ is complete.

$[\![D]\!] = [\![E]\!]$ → $[\![D^\tau]\!] = [\![E^\tau]\!]$ ($\sigma \mapsto \tau$) → $\mathcal{R} \vdash D^\tau = E^\tau$ (source completeness) → $\mathcal{R}, \sigma = \tau \vdash D = E$ (replace τ by σ)

Ten qutrit equations remain



Is each equation necessary?

Independent equation

Let $\rho : L_\rho = R_\rho$ belong to $\mathcal{R}$. Then

$$\rho \text{ is independent} \iff \mathcal{R} \setminus \{\rho\} \nvdash L_\rho = R_\rho.$$

Minimal presentation

$$\mathcal{R} \text{ is minimal} \iff \forall \rho \in \mathcal{R},\ \rho \text{ is independent}.$$

Why check?

- A mechanized proof records each primitive equation as an assumption.
  [Bian–Selinger 2023b]
- Fewer primitive rules reduce branching in derivation search.
- Finite-model search can certify non-derivability.
  [McCune 2003]

Countermodels certify independence

Separation lemma

$$\exists\, [\![\cdot]\!]_{\mathrm{alt}} : \mathcal{P}_\Sigma \longrightarrow \mathcal{M}, \quad [\![\cdot]\!]_{\mathrm{alt}} \models \mathcal{R} \setminus \{\rho\}, \quad [\![L_\rho]\!]_{\mathrm{alt}} \neq [\![R_\rho]\!]_{\mathrm{alt}} \quad \Longrightarrow \quad \mathcal{R} \setminus \{\rho\} \nvdash L_\rho = R_\rho.$$

$[\![\cdot]\!]_{\mathrm{alt}}$ is a PROP morphism, so $\ker([\![\cdot]\!]_{\mathrm{alt}})$ is closed under identities, composition, tensor, and structural symmetries.

Equational soundness: [Birkhoff 1935]

A $\mathbb{Z}_4$ countermodel

$$\mathcal{P} = \langle a \mid \rho_2 : a^2 = e,\ \ \rho_4 : a^4 = e\rangle$$

ρ_4 is derivable

The relation ρ_2 gives

$$a^4 = (a^2)^2 = e.$$

Hence ρ_4 is redundant in this presentation.

ρ_2 is independent

Define a monoid homomorphism into $(\mathbb{Z}_4, +)$ by

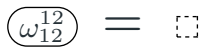
$$F(a^k) = k \bmod 4, \qquad F(e) = 0.$$

$$\begin{aligned} F(a^4) &= 0 = F(e), \\ F(a^2) &= 2 \neq 0 = F(e). \end{aligned}$$

$\{\rho_4\} \nvdash \rho_2$, witnessed by the four-element model $(\mathbb{Z}_4, +)$.

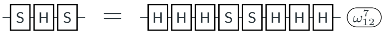
Occurrence separates CPh

In $\mathbb{B}_{\max}$, set $F(\text{CNOT}) = 1$, every other generator and symmetry to 0, and use $\max$ for $\circ$ and $\otimes$.

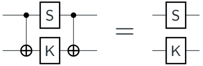
ω^{12}  $0 = 0$

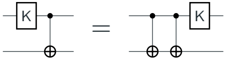
H^4  $0 = 0$

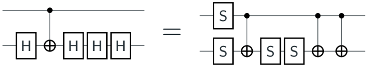
S^3  $0 = 0$

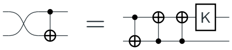
E  $0 = 0$

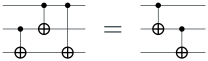
SS'  $0 = 0$

CPh  $1 \neq 0$

KC  $1 = 1$

CZ  $1 = 1$

B  $1 = 1$

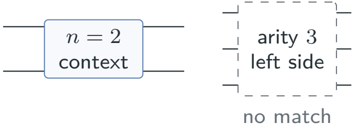
I  $1 = 1$

Arity blocks ternary rules

Arity truncation

If every generator is an endomorphism, then for $C, D : n \to n$,

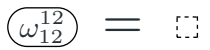
$$\mathcal{R} \vdash C = D \quad \iff \quad \mathcal{R}_{\leq n} \vdash C = D.$$

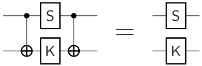
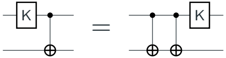
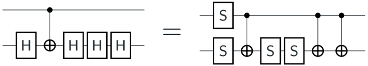
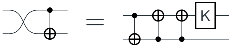
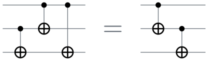


- Every generator has type $k \to k$.
- Composition, tensor, and every rewrite preserve the ambient wire count.
- A rule of arity $k > n$ cannot match inside an n-wire derivation.
- Testing $\rho : n \to n$ therefore requires only $\mathcal{R}_{\leq n}$.
- State preparation, discard, or fresh ancillas invalidate the argument.

Parity distinguishes KC

$[\![\cdot]\!]_{\text{alt}} = \#\{\text{CNOT}\}_{[2]}$, with composition and tensor interpreted as addition in $\mathbb{Z}_2$.

ω^{12}		$0 = 0$
H^4		$0 = 0$
S^3		$0 = 0$
E		$0 = 0$
SS'		$0 = 0$

CPh		$0 = 0$
KC		$1 \neq 0$
CZ		$1 = 1$
B		$1 = 1$
I		$1 \neq 0$

Substitution separates SS'

$$\boxed{\mathsf{S}} \quad \longmapsto \quad \boxed{\mathsf{S}}\boxed{\mathsf{X}}$$

Replace every occurrence of S by SX.

The retained scalar and one-qutrit equations still hold

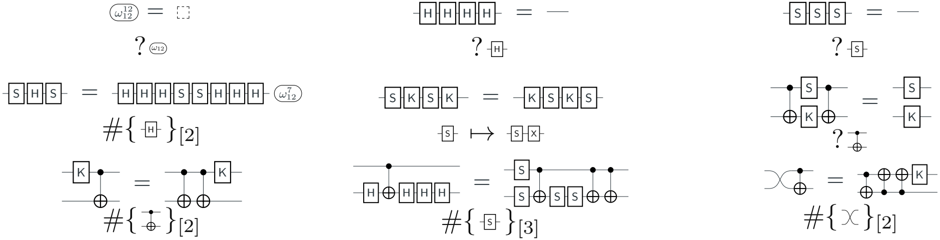
$$\omega^{12} \qquad H^4 \qquad S^3 \qquad E \qquad \checkmark$$

The removed SS' equation fails after substitution

$$\boxed{\mathsf{S}}\boxed{\mathsf{X}}\boxed{\mathsf{K}}\boxed{\mathsf{S}}\boxed{\mathsf{X}}\boxed{\mathsf{K}} \quad \neq \quad \boxed{\mathsf{K}}\boxed{\mathsf{S}}\boxed{\mathsf{X}}\boxed{\mathsf{K}}\boxed{\mathsf{S}}\boxed{\mathsf{X}}$$

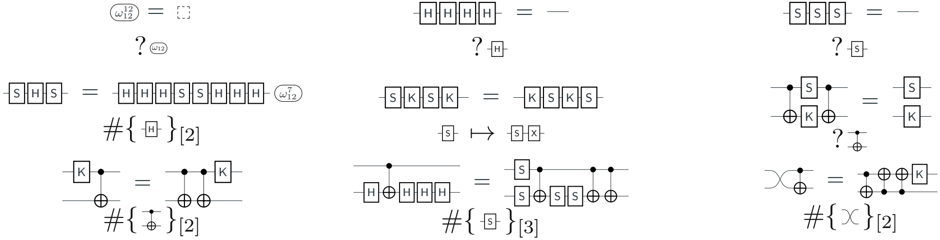
Qutrit Clifford: arity two

Each displayed rule has a separating PROP morphism.

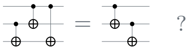


Qutrit Clifford: arity two

Each displayed rule has a separating PROP morphism.



The reduced qutrit presentation is *minimal* for circuits on at most two qutrit wires.



Six reduced presentations

fragment	previous	reduced
qubit Clifford	15	8
real Clifford	16	10
CNOT-dihedral	13	11
Clifford+T ($\leq$ 2q)	18	11
Clifford+CS ($\leq$ 3q)	17	14
qutrit Clifford	18	10

Six reduced presentations

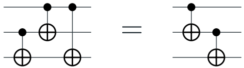
fragment	previous	reduced	minimality status
qubit Clifford	15	8	✓ minimal in all arities
real Clifford	16	10	✓ minimal in all arities
CNOT-dihedral	13	11	✓ minimal in all arities
Clifford+T (≤ 2q)	18	11	○ minimal through 1-qubit circuits; remaining 2-qubit equations undecided
Clifford+CS (≤ 3q)	17	14	○ minimal through 2-qubit circuits; remaining 3-qubit rule family undecided
qutrit Clifford	18	10	○ minimal through 2-qutrits; ternary braid open

Real Clifford + CH

```
PS C:\Users\cblake\Documents\minimality-auto> python -m minimality_auto theories\realclifford-ch-simplified.json --auto --timeout 120
Real-Clifford+CH (Figure 4): 17 separator(s) found
  [found] 19_n5: ambient-5-wire Spin-cover invariant: the commuting target factors lift with sign -1
  [found] 19_n6: ambient-6-wire Spin-cover invariant: the commuting target factors lift with sign -1; 1 retained cyclic reversal(s) scale to sign +1
  [found] 19_n7: ambient-7-wire Spin-cover invariant: the commuting target factors lift with sign -1; 1 retained cyclic reversal(s) scale to sign +1
  [found] 19_n8: ambient-8-wire Spin-cover invariant: the commuting target factors lift with sign -1; 1 retained cyclic reversal(s) scale to sign +1
  [found] 19_n9: ambient-9-wire Spin-cover invariant: the commuting target factors lift with sign -1; 1 retained cyclic reversal(s) scale to sign +1
  [found] 19_n10: ambient-10-wire Spin-cover invariant: the commuting target factors lift with sign -1; 1 retained cyclic reversal(s) scale to sign +1
  [found] 3: discovered F_7 amalgam with bridge {H}: |C|=2, |A|=1, |D|=2
  [found] 11: discovered F_7 amalgam with bridge {CH}: |C|=2304, |A|=256, |D|=512
  [found] 6: count mod 2: {'Z': 1}
  [found] 7: count mod 2: {'H': 1}
  [found] 8: count mod 2: {}, swap=1
  [found] 15: count mod 2: {'CH': 1, 'CZ': 1}, swap=1
  [found] 18: count mod 2: {'CH': 1}
  [found] 1: degree-3 permutation interpretation: generators {H=(1, 2, 0), Z=(0, 2, 1)}
  [found] 2: degree-3 permutation interpretation: generators {H=(0, 2, 1), Z=(1, 2, 0)}
  [found] 10: degree-3 permutation interpretation: generators {H=(0, 1, 2), Z=(0, 1, 2), CZ=(0, 2, 1), CH=(1, 0, 2)}; structural swaps {swap[0,1]=(0, 2, 1)}
  [found] 5: count mod 4: {'CH': 1, 'H': 2}
  [open]  12
  [open]  13
  [open]  14
  [open]  16
  [open]  17
elapsed: 120.000s (timeout)
```

https://github.com/Sukyn/minimality-auto/

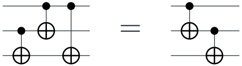
One qutrit braid remains



Conjecture

$$\mathcal{R} \setminus \{I\} \nvdash L_I = R_I.$$

One qutrit braid remains



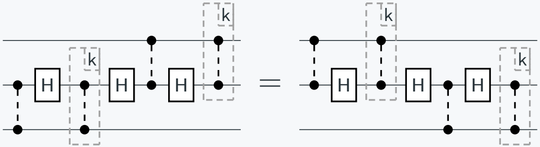
Conjecture

$$\mathcal{R} \setminus \{I\} \nvdash L_I = R_I.$$

- I is the only qutrit rule of arity 3.
- Every qutrit rule of arity at most 2 has an independence certificate.
- The corresponding ternary laws are independent in real Clifford, qubit Clifford, Clifford$+CS$, and CNOT-dihedral.

Four Clifford+CS rules remain

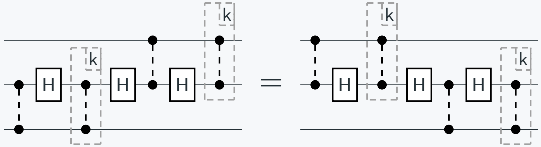
ρ_k :



$k \in \{0, 1, 2, 3\}$

Four Clifford+CS rules remain

ρ_k :



$k \in \{0, 1, 2, 3\}$

Occurrence and counts agree

$$?g(L_k) = ?g(R_k),$$
$$\#\{g\}(L_k) = \#\{g\}(R_k).$$

for the occurrence and counting tests used above.

Substitution target

$$g \mapsto g'$$
$$[\![\cdot]\!]_{\mathrm{alt}} \models \mathcal{R} \setminus \{\rho_k\}$$
$$[\![L_k]\!]_{\mathrm{alt}} \neq [\![R_k]\!]_{\mathrm{alt}}.$$

A separator for ρ_k would satisfy both conditions.

What must separators preserve?

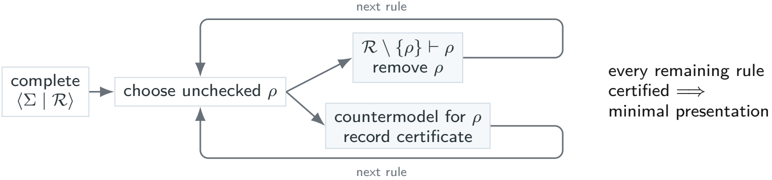
circuit language	structural operations in derivations	requirement on F
PRO	identity, $\circ$, $\otimes$	strict monoidal functor
PROP	PRO operations and σ	preserve canonical symmetry
controlled PROP	PROP operations and control	preserve the control operation
dagger / projective calculus	dagger or scalar quotient	preserve $\dagger$ or projective equality

Independence test

$$F \models \mathcal{R} \setminus \{\rho\} \qquad F(L_\rho) \neq F(R_\rho).$$

The kernel of F must be closed under every context available to a derivation.

Conclusion



Results

- Six complete presentations share one PROP formulation.
- Real Clifford, qubit Clifford, and CNOT-dihedral are minimal.
- Qutrit Clifford is minimal through arity 2.

Future work

- Complete unbounded Clifford+T and Clifford+CS.
- Automate derivation and countermodel search.
- Export certificates to Lean, Agda, or Rocq.

Backup 1: separation argument

Lemma
Let $\mathcal{P}_\Sigma$ be the free PROP on the fragment signature, let $\mathcal{R}$ be a finite set of equations in $\mathcal{P}_\Sigma$, and let $\rho : L = R \in \mathcal{R}$. Put $\mathcal{S} = \mathcal{R} \setminus \{\rho\}$. Suppose there is a PROP M and a strict symmetric monoidal functor $F : \mathcal{P}_\Sigma \to M$, identity on objects, such that

$$\forall (A = B) \in \mathcal{S}, \quad F(A) = F(B), \qquad F(L) \neq F(R).$$

Then $\mathcal{S} \nvdash L = R$, so ρ is independent.

Proof
Define

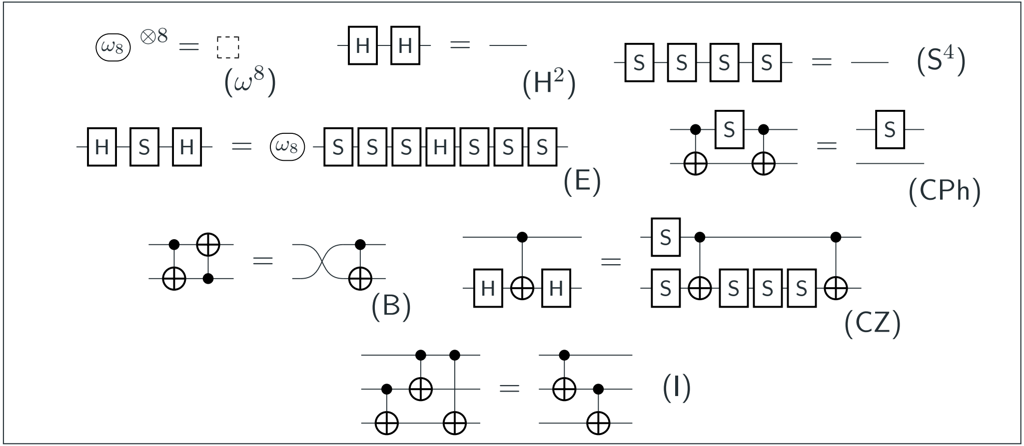
$$E_F = \{(A, B) \mid F(A) = F(B)\}.$$

Since F preserves identities, symmetries, tensor, and sequential composition, E_F is a PROP congruence on $\mathcal{P}_\Sigma$. Since $F \models \mathcal{S}$, every equation of $\mathcal{S}$ lies in E_F. The derivability relation generated by $\mathcal{S}$ is the least PROP congruence containing $\mathcal{S}$, hence

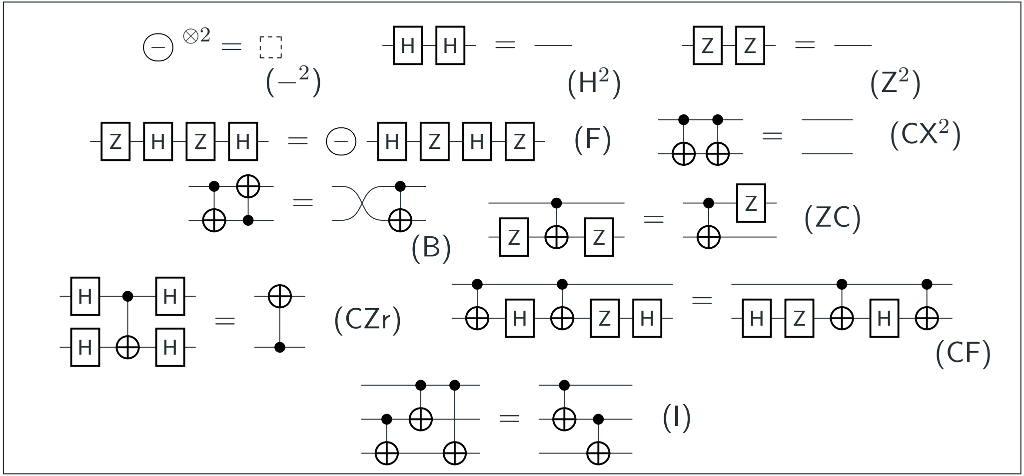
$$\mathcal{S} \vdash A = B \quad \Longrightarrow \quad F(A) = F(B).$$

Applying this to $A = L$, $B = R$ would contradict $F(L) \neq F(R)$.
Countermodel/soundness direction of the Birkhoff-style argument.

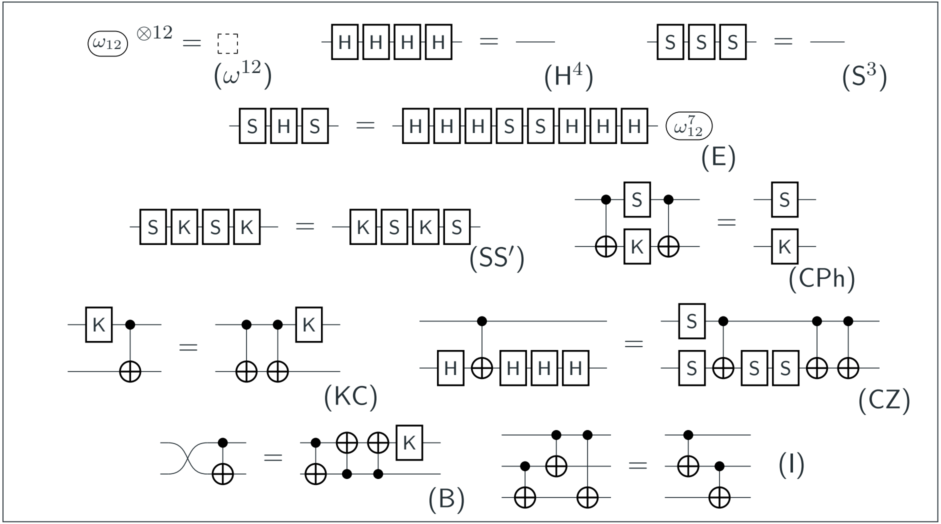
Backup 2: qubit Clifford



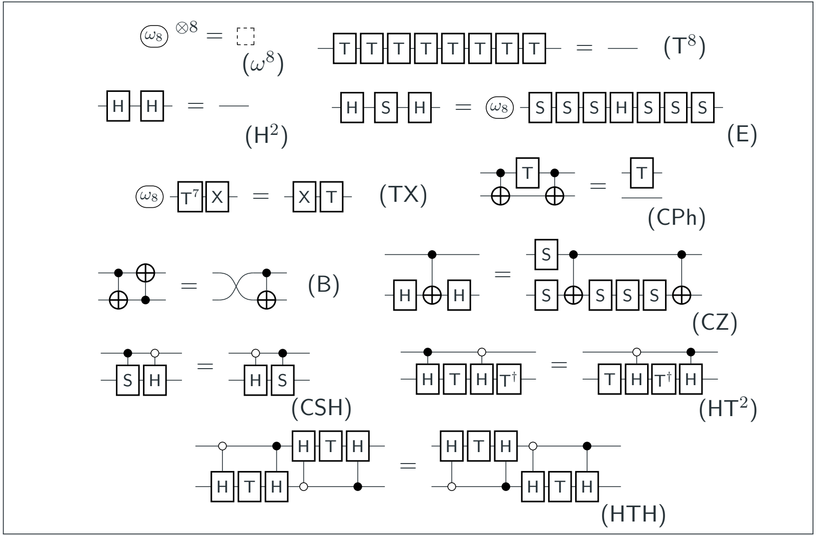
Backup 3: real Clifford



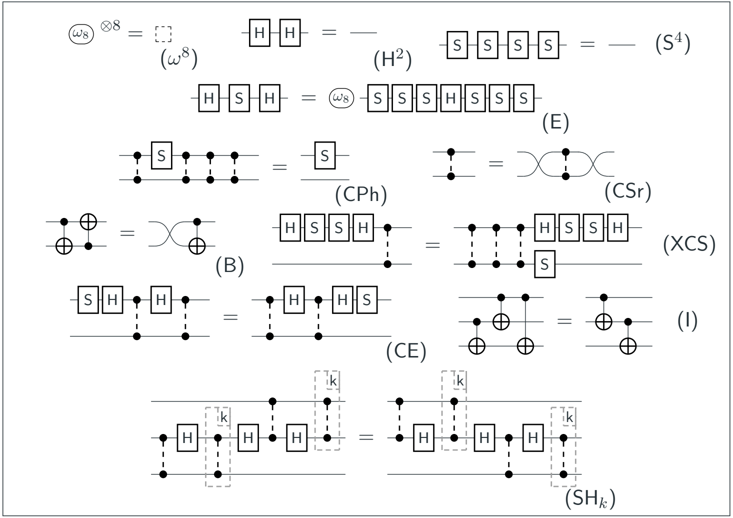
Backup 4: qutrit Clifford



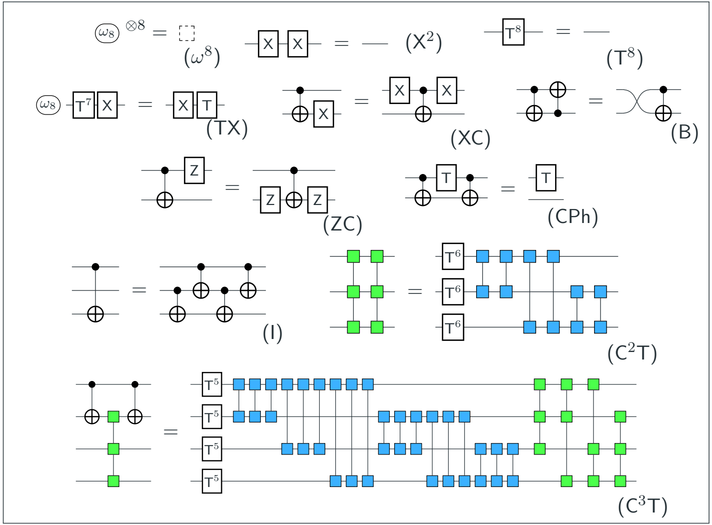
Backup 5: Clifford+T relations



Backup 6: Clifford+CS relations



Backup 7: CNOT-dihedral relations



Backup 8: separators I

qubit Clifford

relation	separator
ω^8	$?\omega_8$
H^2	$?H$
S^4	$?S$
E	$\#\{H\}_{[2]}$
CPh	$?CX$
B	$\#\{SWAP\}_{[2]}$
CZ	$\#\{CX, SWAP\}_{[2]}$
I	$\arg\det_2$

real Clifford

relation	separator
$-^2$	$?-$
H^2	$?H$
Z^2	$?Z$
F	$\#\{\omega\}_{[2]}$
CX^2	$?CX$
B	$\#\{SWAP\}_{[2]}$
ZC	$\#\{Z\}_{[2]}$
CF	$Z \mapsto I$
CZr	$H \mapsto I$
I	$\arg\det_2$

qutrit Clifford

relation	separator
ω^{12}	$?\omega_{12}$
H^4	$?H$
S^3	$?S$
E	$\#\{H\}_{[2]}$
SS'	$S \mapsto SX$
CPh	$?CX$
B	$\#\{SWAP\}_{[2]}$
CZ	$\#\{S\}_{[3]}$
KC	$\#\{CX\}_{[2]}$
I	–

Backup 9: separators II

Clifford+T

relation	separator
ω^8	$?\omega_8$
H^2	$?H$
T^8	$?T$
E	$\#\{H\}_{[2]}$
TX	$\#\{H, T, \omega\}_{[2]}$
CPh	$?CX$
B	$\#\{SWAP\}_{[2]}$
CZ	$\#\{CX, SWAP\}_{[2]}$
CSH	–
HT^2	–
HTH	–

Clifford+CS

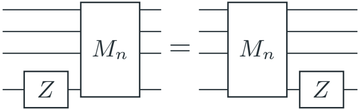
relation	separator
ω^8	$?\omega_8$
H^2	$?H$
S^4	$?S$
E	$\#\{H\}_{[2]}$
CPh	$?CX$
B	$\#\{SWAP\}_{[2]}$
XCS	$\#\{S, H\}_{[2]}$
CSr	$CS \mapsto CS_z$
CE	$CS \mapsto CS_{zz}$
I	$\arg\det_2$
SH_k	–

CNOT-dihedral

relation	separator
ω^8	$?\omega_8$
T^8	$?T$
X^2	$?X$
TX	$\#\{\omega\}_{[2]}$
XC	$\#\{X\}_{[2]}$
CPh	$?CX$
B	$\#\{SWAP\}_{[2]}$
ZC	$\#\{T, \omega, \omega\}_{[8]}$
I	$\#\{CX, SWAP\}_{[2]}$
C^2T	$\#\{T, \omega, \omega\}_{[4]}$
C^3T	$\arg\det_3$

Backup 10: Spin separation

Rule $(19)_n$, $n \geq 5$



$$M_n = \mathrm{MCZ}_{n-1} \otimes I$$

$$\begin{tikzcd} & \mathrm{Spin}(2^n) & \\ u \arrow[dr] & & -u \arrow[dl] \\ & A \in SO(2^n) & \end{tikzcd}$$

The matrix forgets the central sign.

For commuting orthogonal involutions,

$$\widehat{A}\widehat{B} = (-1)^{pq-r}\widehat{B}\widehat{A}.$$

$$p = \dim E_-(Z) = 2^{n-1},$$
$$q = \dim E_-(M_n) = 2,$$
$$r = \dim\big(E_-(Z) \cap E_-(M_n)\big) = 1.$$
$$pq - r = 2^n - 1 \equiv 1 \pmod 2.$$

$$\widehat{Z}\widehat{M_n} = -\widehat{M_n}\widehat{Z}.$$

Rules (1)–(18)

$m \leq 3 \implies K = 2^{n-m} \implies 4 \mid K \ (n \geq 5) \implies$ Spin sign $+1$