Equational reasoning for quantum circuits: (in higher dimensions)

Colin Blake

MOCQUA team, Inria / LORIA, Université de Lorraine

Supervisors: Miriam Backens & Simon Perdrix

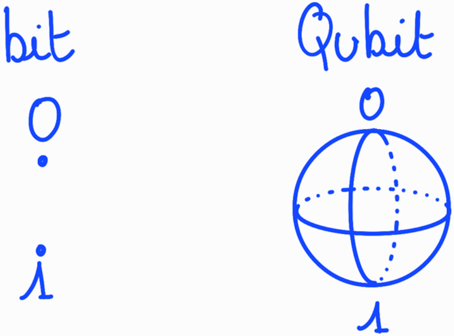
Slides : Colin Blake & Doriane Bedier

26 March 2026

Inria

UNIVERSITÉ DE LORRAINE

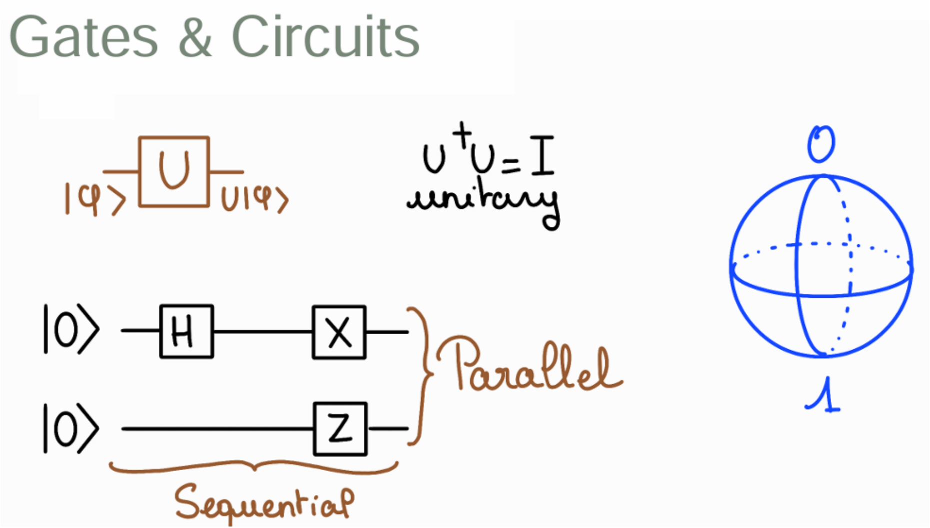
States

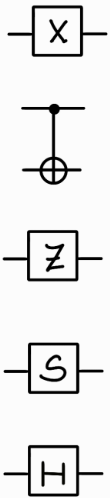


$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$\Pr(0) = |\alpha|^2$$

$$\Pr(1) = |\beta|^2$$


Gates & Circuits
|φ⟩
U
U|φ⟩
U†U = I
unitary
0
1
|0⟩
H
X
|0⟩
Z
Parallel
Sequential



$$|x\rangle \to |x \oplus 1\rangle$$

$$|x, y\rangle \to |x, x \oplus y\rangle$$

$$|x\rangle \to (-1)^x |x\rangle$$

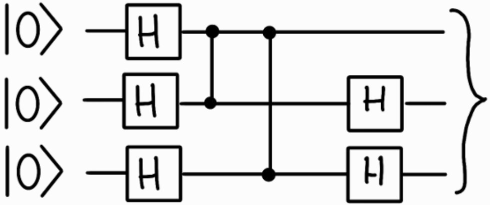
$$|x\rangle \to (i)^x |x\rangle$$

$$|x\rangle \to \frac{1}{\sqrt{2}} \sum_{y=0}^{1} (-1)^{xy} |y\rangle$$

Entanglement

$$|\varphi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

$$|\phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$



$$\frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

Why do we rewrite circuits?

- **Optimisation**: fewer expensive gates, ...
- **Mapping**: Adapt to hardware, ...
- **Verification**: Prove it is the intended matrix, ...

Why do we rewrite circuits?

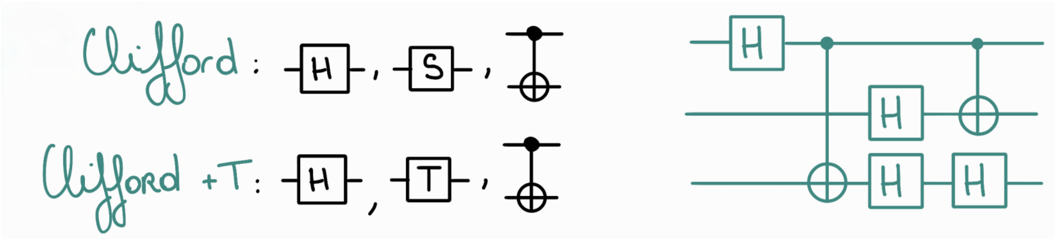
- **Optimisation**: fewer expensive gates, ...
- **Mapping**: Adapt to hardware, ...
- **Verification**: Prove it is the intended matrix, ...

Algebraic viewpoint :

- Circuits come with "equations"
- A good rule set lets you transform safely & automatically

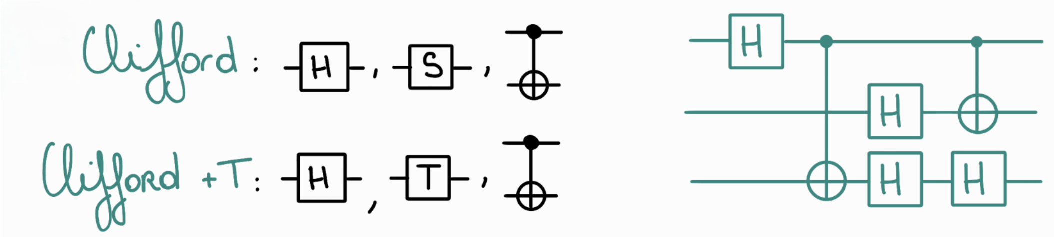
Gate set & Circuit family

- A **gate set**: allowed primitives
- A **circuit family**: all you can do with it



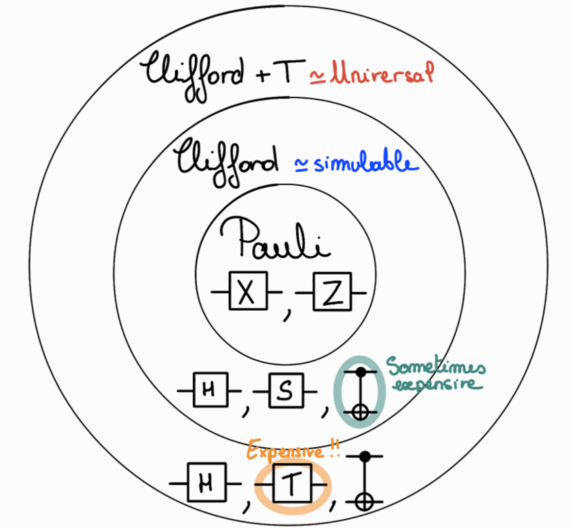
Gate set & Circuit family

- A **gate set**: allowed primitives
- A **circuit family**: all you can do with it



- **Expressiveness**: What unitaries can you build?
- **Reasoning**: Do we have a "usable" rewrite system?

Expressiveness ladder



In fault tolerant setting, gates have different prices

- Clifford : "easy"
- 

: require *magic state distillation*

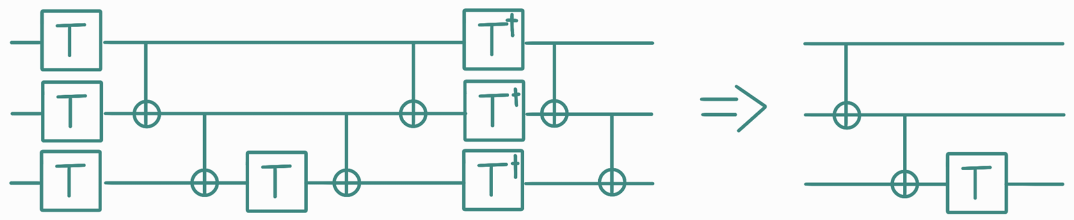
$\leadsto$ we want to reduce the **T-count**

In fault tolerant setting, gates have different prices

- Clifford : "easy"
- 

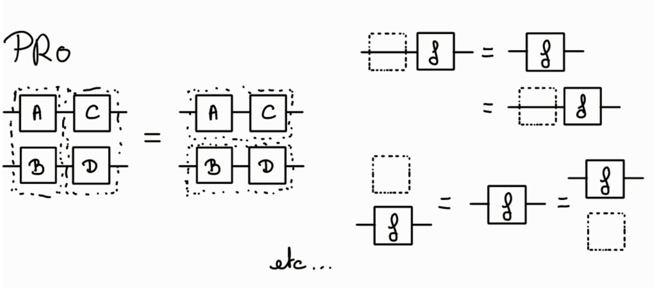
 : require *magic state distillation*

$\rightsquigarrow$ we want to reduce the **T-count**

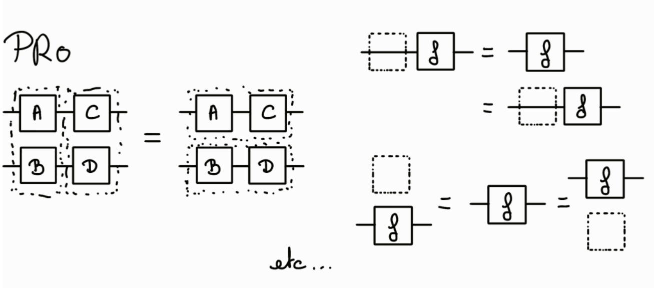


This is where complete theories + normal forms are used

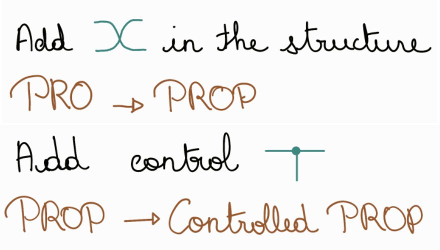
Categories



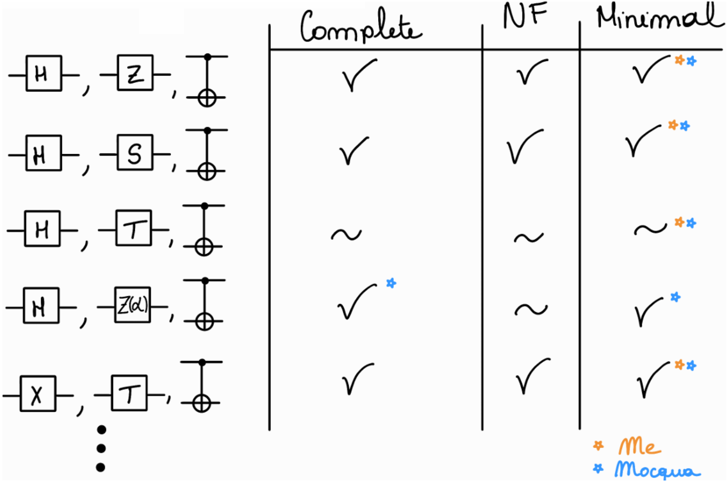
Categories



PRo
A
C
B
D
etc...

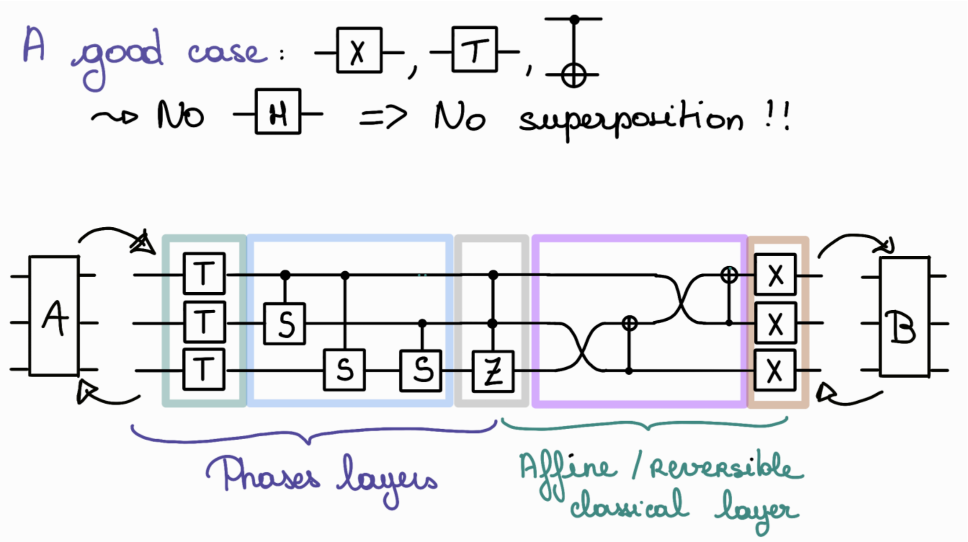


Add in the structure
PRO → PROP
Add control
PROP → Controlled PROP



∼ means only partial results or hidden technicalities.

Normal forms



Clifford example

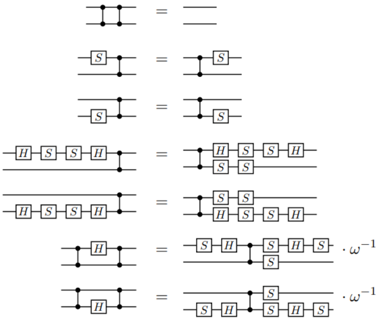
(a) Equations for $n \geqslant 0$:

$$\omega^8 = 1$$

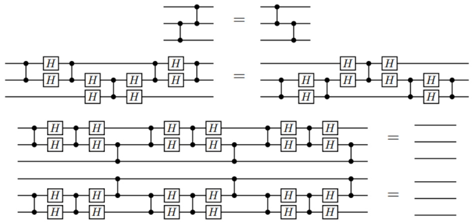
(b) Equations for $n \geqslant 1$:

$$\begin{aligned} H^2 &= 1 \\ S^4 &= 1 \\ SHSHSH &= \omega \end{aligned}$$

(c) Equations for $n \geqslant 2$:

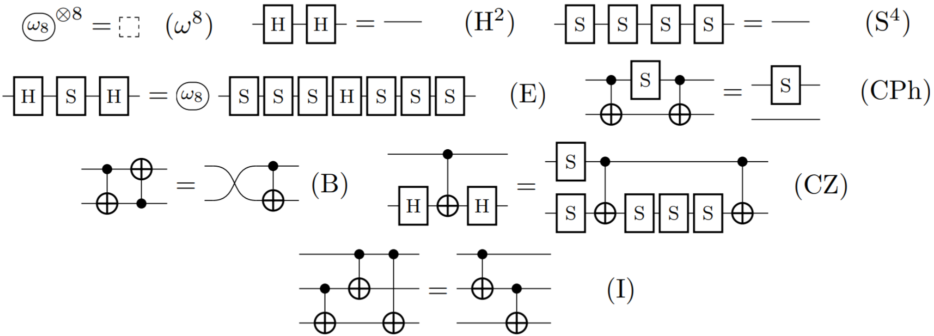


(d) Equations for $n \geqslant 3$:



P. Selinger, *Generators and relations for n-qubit Clifford operators*, Logical Methods in Computer Science 11(2:10), 2015.

Clifford example



fragment	earlier complete presentation	reduced PROP core	minimality status
qubit Clifford	15 rules in [18]	8 rules in [6]	minimal
real Clifford	16 rules in [16]	10 rules in [6]	minimal
qutrit Clifford	18 rules in [14]	10 rules in [6]	minimal up to 2 qutrit wires
Clifford+T on up to 2 qubits	18 rules in [3]	11 rules in [6]	minimal up to 1 qubit
Clifford+CS on up to 3 qubits	17 rules in [4]	14 rules in [6]	minimal up to 2 qubits
CNOT-dihedral	13 rules in [1]	11 rules in [6]	minimal

Qudits: What and why?

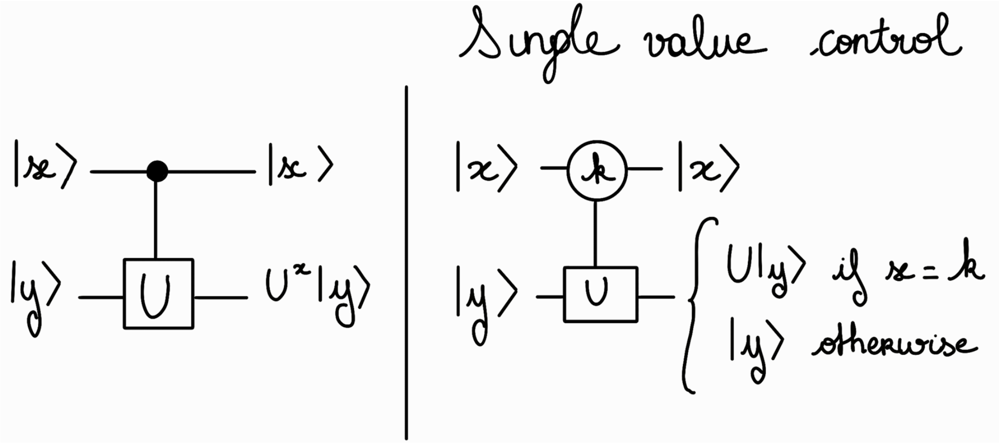
$$|\varphi\rangle = \sum_{k=0}^{d-1} \alpha_k |k\rangle$$

- Some platforms are naturally *higher-dimensional*
- Potential *advantages* in *compilation*, *error correction*, . . .
- Conceptually: have *dimension-robust theories* not only "dimension 2 nice coincidences"

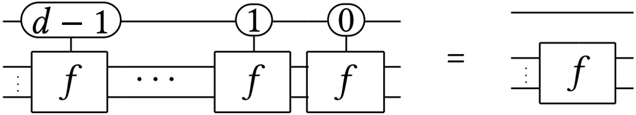
Gates

X	$\lvert x\rangle \to \lvert x \oplus 1\rangle$	$\lvert x\rangle \to \lvert x + 1 \bmod d\rangle$
	$\lvert x, y\rangle \to \lvert x, x \oplus y\rangle$	$\lvert x, y\rangle \to \lvert x, x + y \bmod d\rangle$
Z	$\lvert x\rangle \to (-1)^x \lvert x\rangle$	$\lvert x\rangle \to \omega^x \lvert x\rangle$
S	$\lvert x\rangle \to (i)^x \lvert x\rangle$	$\lvert x\rangle \to \omega^{\binom{x}{2}} \lvert x\rangle$
$X^{a,b}$	N/A	$\lvert a\rangle \leftrightarrow \lvert b\rangle$ $\lvert x\rangle \to \lvert x\rangle$ if $x \notin \{a, b\}$
H	$\lvert x\rangle \to \frac{1}{\sqrt{2}} \sum_{y=0}^{1} (-1)^{xy} \lvert y\rangle$	$\lvert x\rangle \to \frac{1}{\sqrt{d}} \sum_{y=0}^{d-1} \omega^{xy} \lvert y\rangle$

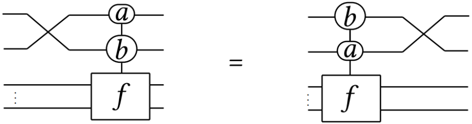
Control?



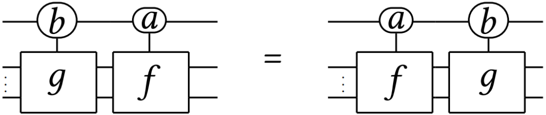
Polycontrolled PROPs



$$C_0(f) \circ C_1(f) \circ \cdots \circ C_{d-1}(f) = \mathrm{id}_1 \otimes f$$



$$C_{ab}(f) \circ (\sigma_{1,1} \otimes \mathrm{id}_n) = (\sigma_{1,1} \otimes \mathrm{id}_n) \circ C_{ba}(f)$$



$$C_a(f) \circ C_b(g) = C_b(g) \circ C_a(f)$$

Which dimension are we interested?

3: smallest $d > 2$, "easy" sandbox

all: this is the goal, but usually hard

primes: $\mathbb{Z}/p\mathbb{Z}$ is a field ⇝ good properties

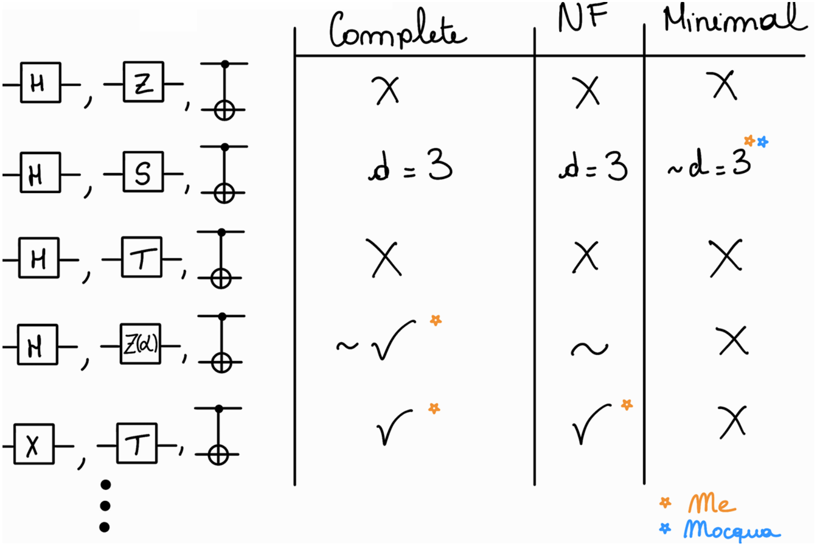
$\mathbb{Z}/d\mathbb{Z}$ is a ring with zero-divisors.

→ more cases

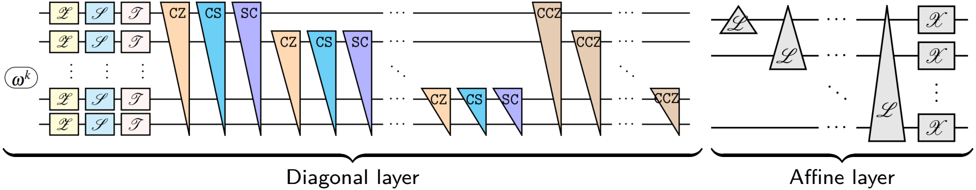
→ difficult to keep local

→ special cases.

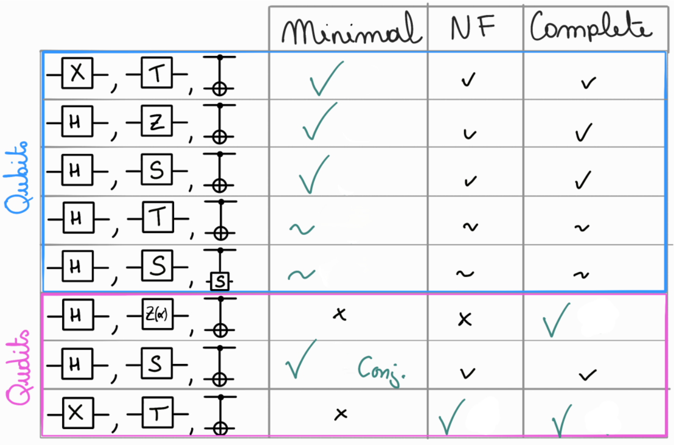
State of the art



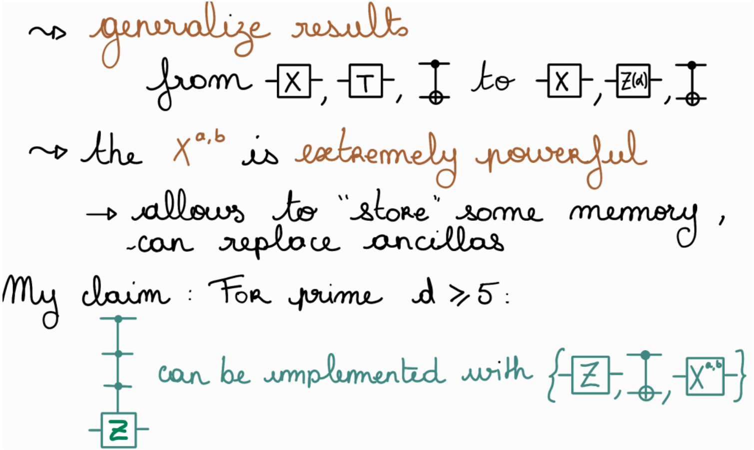
The normal form example



Recap



Next steps



~> generalize results
from X, T, to X, Z(α),
~> the X^{a,b} is extremely powerful
-> allows to "store" some memory,
can replace ancillas
My claim : For prime d ≥ 5 :
can be implemented with {Z, , X^{a,b}}
Z

Questions and discussion are very welcome.

To discover more about these ideas, you can start with these preprints:

Completeness for Prime-Dimensional Phase-Affine Circuits
arXiv:2603.06466

Polycontrolled PROPs for Qudit Circuits: A Uniform Complete Equational Theory for Arbitrary Finite Dimension
arXiv:2602.09873

Simpler Presentations for Many Fragments of Quantum Circuits
arXiv:2602.09874

The links are clickable in the PDF.