One rig to control them all

Chris Heunen[1], Robin Kaarsgaard[2], and Louis Lemonnier[1]

[1]University of Edinburgh
[2]University of Southern Denmark

Abstract

Controlled commands—computations whose execution depends on a separate input—play a central role in reversible Boolean circuits and quantum circuits. However, existing formalisms typically treat control only implicitly, entangled with other aspects of computation. From a semantic perspective, control is most naturally expressed in semisimple rig categories, which—unlike standard circuit models such as props—support both parallel and conditional composition.

We present a construction that freely adjoins an explicit syntactic notion of control to a circuit theory specified as a suitable prop, subject to eight universally quantified equations. Our main result is that these equations are sound and complete for the intended semantics of control: the resulting theory satisfies a universal property, identifying it exactly as the circuit subtheory of the free semisimple rig completion. The proof combines coherence for rig categories with a new method based on induction over Gray codes.

We illustrate the usefulness of the framework by showing that it simplifies several existing sound and complete axiomatisations of quantum circuits, isolating a small and conceptually clean set of generators and equations. In addition, the same equations yield a sound and complete axiomatisation of the multiply controlled Toffoli gate set, that is universal for reversible Boolean circuits.

This is an extended abstract of a preprint available on the arXiv [16] and to appear in LICS'26.

1 Introduction

Many computations contain *controlled* commands, that is, commands that are executed depending on the value of some memory cell. By *control* we mean the aspects of a computation that govern these dependencies. Typically, the controlled command acts on one part of memory, and the controlling memory cell resides in another part of memory. To be more precise, for example, consider controlled negation in reversible Boolean circuits: the target bit is flipped depending on the value of the control bit. The goal of this article is to identify, separate, and study in isolation, this notion of control.

Traditional control flow is often mixed up with other computational aspects of circuits. For example, in reversible Boolean or quantum circuits, multi-controlled gates such as the Toffoli gate are integral to universality and not treated differently than other, uncontrolled, gates [23]. Yet separating out the controlled aspects of a computation has several benefits.

(i) Multi-controlled gates are of foundational importance in many computational theories, including Boolean logic [24], reversible computation [23, 22], and quantum computation [21]. Isolating their control logic can help to better *understand* these theories.

(ii) In quantum hardware, (multi-)controlled gates are among the most costly ones to perform physically [2, 26, 8]. Separating out the control aspects can help find better optimisation strategies [1]. In general, partitioning off control aspects can help to *optimise* computations in a generic way that is independent of the 'base circuit theory' and therefore more efficient to apply.

(iii) Several recent results about logical completeness for quantum computation rely on elaborate families of equations [4, 3, 18, 11, 13]. Cordoning off control aspects can *simplify*, and thereby clarify the core status of some and make them more modular.

This article addresses these three challenges by introducing a theory of control governed by a handful of equations (see Figure 1). We argue that these equations completely capture control as follows.

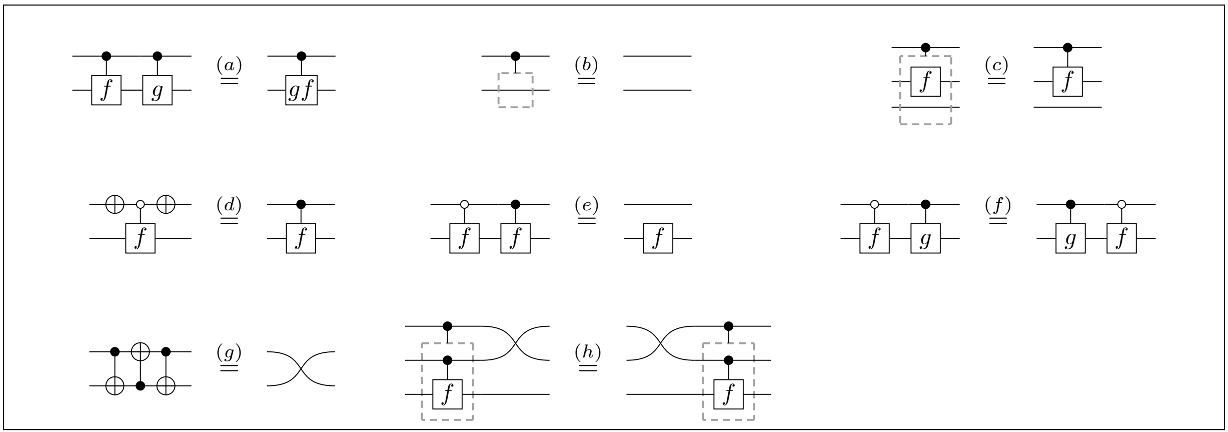

Figure 1: Control equations.

(i) The equations have clear computational interpretations, and several have appeared in the literature before [20, 22]. Additionally, we show that the equations are canonical in a strong way, by relating them to the natural mathematical notion of a *rig category* [17, 25]. Starting with an arbitrary 'base circuit theory', we syntactically construct a new 'controlled circuit theory'. We do this in the most general setting possible, using *prop*s [19, 14, 5]. The construction has a universal property: roughly, it is the free rig category on the base prop.

(ii) The coherence theorems for rig categories [17, 25], and the fact that the control theory (of Figure 1) consists of only eight unquantified equations, can give rise to many optimisation strategies.

(iii) The equations simplify related work. The first works on complete equational theories for quantum circuits [11, 9, 10] contain a notion of *structural* equations, without a mathematical account of this notion. The same holds for [4, 3, 18]. This article fills that gap by showing that the structure of control is exactly that of rig categories. Our work similarly structures and elucidates a line of research on quantum programming languages taking semantics in rig categories [7, 15, 6, 13].

These results also substantiate the claim in the title, that rig structure encapsulates controlled computation, and only controlled computation. Thus rig categories form the minimum model of computation: the ability to compose instructions sequentially (with $\circ$), to consider data in parallel (with $\otimes$), and to use one piece of data to condition computations on another (using $\oplus$).

2 Controlled props

A *controllable prop* $(\mathbf{P}, +, 0, x)$, or *crop* for short, is a prop $(\mathbf{P}, +, 0)$ whose morphisms are endomorphisms and in which one morphism $x\colon 1 \to 1$ is a distinguished involution, referred to as the *NOT gate*.

Definition 1 (Controlled prop)**.** Given a controllable prop $(\mathbf{P}, +, 0, x)$, we extend it to a new prop with endofunctors C^0 and C^1 such that if $f\colon n \to n$, then $C^b(f)\colon 1 + n \to 1 + n$, and that, for all n and $f, f_1, f_2\colon n \to n$, we have equations:

(a) composition: $C^1(g \circ f) = C^1(g) \circ C^1(f)$;

(b) identity: $C^1(\mathrm{id}_n) = \mathrm{id}_{n+1}$;

(c) strength: $C^1(f + \mathrm{id}_m) = C^1(f) + \mathrm{id}_m$;

(d) colour change: $(x + \mathrm{id}_n) \circ C^0(f) \circ (x + \mathrm{id}_n) = C^1(f)$;

(e) complementarity: $C^0(f) \circ C^1(f) = \mathrm{id}_1 + f$;

(f) commutativity: $C^0(f_1) \circ C^1(f_2) = C^1(f_2) \circ C^0(f_1)$;

(g) "swap": $C^1(x) \circ \mathsf{swap}_{1,1} \circ C^1(x) \circ \mathsf{swap}_{1,1} \circ C^1(x) = \mathsf{swap}_{1,1}$;

(h) "swap" coherence: $(\mathsf{swap}_{1,1} \otimes \mathrm{id}_n) \circ C^1(C^1(f)) = C^1(C^1(f)) \circ (\mathsf{swap}_{1,1} \otimes \mathrm{id}_n)$.

Figure 1 gives a diagrammatic account of the above equations. Write $\mathbf{cP}$ for this new prop, that we call the *controlled prop* of $\mathbf{P}$. Note that $(\mathbf{cP}, +, 0, x)$ is itself a controllable prop.

3 Rigged props thanks to Kronecker

In the context of matrices, the Kronecker product can be computed with direct sums only. Given a matrix M, the matrix $I_n \otimes M$ is obtained as the block-diagonal matrix $M \oplus \cdots \oplus M$. This hints at the fact that any theory around the direct sum can simulate the one of a tensor product, given some more coherence. To this effect, given a controllable prop $(\mathbf{P}, +, 0, x)$ with a set of generators G, and a set of relations R, we introduce its *rigged crop* $(\overline{\mathbf{P}}, \oplus, 0)$, as the prop generated by:

$$\overline{G} = \left\{ \overline{g} \colon 2^k \to 2^l \;\mid\; g \colon k \to l \in G \right\} \tag{1}$$

with equations both imported from $\mathbf{P}$ and for the coherence of $\otimes$.

Theorem 2. *The category $(\overline{\mathbf{P}}, \otimes, 1, \oplus, 0)$ is semisimple bipermutative.*

We are interested in objects in $\overline{\mathbf{P}}$ that are powers of 2. Given how generators in $\mathbf{P}$ are mapped into $\overline{\mathbf{P}}$, the embedding $\mathbf{P} \hookrightarrow \overline{\mathbf{P}}$ corestricts to an embedding $\mathbf{P} \hookrightarrow \overline{\mathbf{P}}_2$.

Corollary 3. *Given a controllable prop $(\mathbf{P}, +, 0, x)$, and a strict monoidal functor $F \colon \mathbf{P} \to \mathbf{Q}$ to a semisimple bipermutative category with $F(x) = \gamma_{1,1}$, there is a unique prop morphism $\overline{F}_2 \colon \overline{\mathbf{P}}_2 \to \mathbf{Q}_2$ such that $\overline{F}_2$ preserves the NOT gate and the following diagram commutes.*

$$\begin{tikzcd}
\mathbf{P} \arrow[r, hook] \arrow[dr, "F"'] & \overline{\mathbf{P}}_2 \arrow[d, dashed, "\overline{F}_2"] \\
& \mathbf{Q}_2
\end{tikzcd}$$

Theorem 4. *The props $\mathbf{cP}$ and $\overline{\mathbf{P}}_2$ are crop isomorphic.*

4 Applications

A complete equational theory for quantum circuits was an open question that was solved only recently [11], referring to some equations as *structural*. We show here that these equations are structural in a formal and categorical sense: they are only about control, and follow directly from the structure of a rig category.

Let $(\mathbf{Z}, +, 0)$ be the prop generated by $\alpha \colon 0 \to 0$ for $\alpha \in \mathbb{R}$, and $Z(\alpha) \colon 1 \to 1$ for $\alpha \in \mathbb{R}$, and $H \colon 1 \to 1$ satisfying

$$(2\pi) = \square \tag{2}$$

$$(\alpha_1)\ (\alpha_2) = (\alpha_1 + \alpha_2) \tag{3}$$

$$-\boxed{Z(\alpha_1)}-\boxed{Z(\alpha_2)}- = -\boxed{Z(\alpha_1 + \alpha_2)}- \tag{4}$$

$$-\boxed{H}-\boxed{H}- = \text{———} \tag{5}$$

$$-\boxed{H}-\boxed{Z(\alpha_1)}-\boxed{H}-\boxed{Z(\alpha_2)}-\boxed{H}- = -\boxed{Z(\beta_1)}-\boxed{H}-\boxed{Z(\beta_2)}-\boxed{H}-\boxed{Z(\beta_3)}- \quad (\beta_0) \tag{6}$$

where (6) is the well-known Euler decomposition, in which β_0, β_1, β_2 and β_4 can be computed from α_1 and α_2 deterministically. We choose the crop $(\mathbf{Z}, +, 0, HZ(\pi)H)$ and can now form its controlled prop $\mathbf{cZ}$. Interestingly, the prop $\mathbf{cZ}$ is not immediately the prop of unitary operations: for a given α, the morphisms $C^1(\alpha)$ and $Z(\alpha)$ have the same semantics in unitaries but are still different in $\mathbf{cZ}$. We need to quotient further with the following equation:

$$-\boxed{Z(\alpha)}- = -\overset{(\alpha)}{\bullet}- \tag{7}$$

and we write $\mathbf{cZ}_{/\simeq}$ for this category. From this point, it is simple to show that we have equivalent equations to the complete equational theory for quantum circuits [12], and therefore $\mathbf{cZ}_{/\simeq}$ is isomorphic to the category of unitaries on qubits.

Theorem 5. *Equations* (2)*,* (3)*,* (5)*,* (6) *together with the control equations of Figure 1 and equation* (7)*, are sound and complete for quantum circuits.*

References

[1] S. Balauca and A. Arusoaie. Efficient constructions for simulating multi controlled quantum gates. In *International Conference on Computer Science*, volume 13353 of *Lecture Notes in Computer Science*, pages 179–194. Springer, 2022.

[2] A. Barenco, C. H. Bennett, R. Cleve, D. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter. Elementary gates for quantum computation. *Physical Review A*, 5:3457–3467, 1995.

[3] X. Bian and P. Selinger. Generators and relations for $U_n(\mathbb{Z}[\frac{1}{2}, i])$. In *Quantum Physics and Logic*, volume 343 of *Electronic Proceedings in Theoretical Computer Science*, pages 145–164, 2021.

[4] X. Bian and P. Selinger. Generators and relations for 2-qubit Clifford+T operators. *Electronic Proceedings in Theoretical Computer Science*, 394:13–28, 2023.

[5] F. Bonchi, B. Sobociński, and F. Zanasi. Interacting Hopf algebras. *Journal of Pure and Applied Algebra*, 221(1):144–184, 2017.

[6] J. Carette, C. Heunen, R. Kaarsgaard, and A. Sabry. With a few square roots, quantum computing is as easy as Π. *Proceedings of the ACM on Programming Languages*, 8, 2024.

[7] J. Carette and A. Sabry. Computing with semirings and weak rig groupoids. In *European Symposium on Programming*, volume 9632 of *Lecture Notes in Theoretical Computer Science*, pages 123–148. Springer, 2016.

[8] Z. Chen, W. Liu, Y. Ma, W. Sun, R. Wang, H. Wang, H. Xu, G. Xue, H. Yan, Z. Yang, J. Ding, Y. Gao, F. Li, Y. Zhang, Z. Zhang, Y. Jin, H. Yu, J. Chen, and F. Yan. Efficient implementation of arbitrary two-qubit gates using unified control. *Nature Physics*, 21:1489–1496, 2025.

[9] A. Clément, N. Delorme, and S. Perdrix. Minimal equational theories for quantum circuits. In *Logic in Computer Science*, pages 27:1–27:14. ACM/IEEE, 2024.

[10] A. Clément, N. Delorme, S. Perdrix, and R. Vilmart. Quantum circuit completeness: Extensions and simplifications. In *Computer Science Logic*, volume 288 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 20:1–20:23, 2024.

[11] A. Clément, N. Heurtel, S. Mansfield, S. Perdrix, and B. Valiron. A complete equational theory for quantum circuits. In *Logic in Computer Science*, pages 1–13. ACM/IEEE, 2023.

[12] N. Delorme and S. Perdrix. Diagrammatic reasoning with control as a constructor, applications to quantum circuits, 2025. arXiv:2508.21756.

[13] W. Fang, C. Heunen, and R. Kaarsgaard. Hadamard-Π: Equational quantum programming. arXiv:2506.06835, 2025.

[14] D. R. Ghica and A. Jung. Categorical semantics of digital circuits. In *Formal Methods in Computer-Aided Design*, pages 41–48, 2016.

[15] C. Heunen and R. Kaarsgaard. Quantum information effects. *Proceedings of the ACM on Programming Languages*, 6, 2022.

[16] C. Heunen, R. Kaarsgaard, and L. Lemonnier. One rig to control them all, 2025. arXiv:2510.05032.

[17] M. L. Laplaza. Coherence for distributivity. In G. M. Kelly, M. Laplaza, G. Lewis, and Saunders Mac Lane, editors, *Coherence in Categories*, pages 29–65. Springer, 1972.

[18] S. M. Li, N. J. Ross, and P. Selinger. Generators and relations for the group $\mathrm{O}_n(\mathbb{Z}[1/2])$. In *Quantum Physics and Logic*, volume 343 of *Electronic Proceedings in Theoretical Computer Science*, pages 210–264, 2021.

[19] S. Mac Lane. Categorical algebra. *Bulletin of the American Mathematical Society*, 71:40–106, 1965.

[20] R. Sharma and S. Archour. Optimizing ancilla-based quantum circuits with SPARE. *Proceedings of the ACM on Programming Languages*, 9, 2025.

[21] V. V. Shende, S. S. Bullock, and I. L. Markov. Synthesis of quantum logic circuits. In *Asia and South Pacific Design Automation Conference*, pages 272–275. ACM, 2005.

[22] M. K. Thomsen, R. Kaarsgaard, and M. Soeken. Ricercar: a language for describing and rewriting reversible circuits with ancillae and its permutation semantics. In *Reversible Computing*, pages 200–215, 2015.

[23] T. Toffoli. Reversible computing. In *International Colloquium on Automata, Languages, and Programming*, Lecture Notes in Computer Science, pages 632–644. Springer, 1980.

[24] H. Vollmer. *Introduction to circuit complexity.* Springer, 1999.

[25] D. Yau. *Bimonoidal Categories, E_n-Monoidal Categories, and Algebraic K-Theory: Volume I: Symmetric Bimonoidal Categories and Monoidal Bicategories*, volume 283 of *Mathematical Surveys and Monographs.* American Mathematical Society, 2024.

[26] N. Yu, R. Duan, and M. Ying. Five two-qubit gates are necessary for implementing the Toffoli gate. *Physical Review A*, 88:010304, 2013.