AND-gates in ZX-calculus: QBC-completeness and phase gadgets

Anthony Munson
Department of Physics, Harvard University
anthonymunson@college.harvard.edu

Bob Coecke and Quanlong Wang
Department of Computer Science, University of Oxford
Cambridge Quantum Computing Ltd.
bob.coecke, quanlong.wang@cs.ox.ac.uk

In this paper we exploit the utility of the triangle symbol in ZX-calculus, and its role within the ZX-representation of AND-gates in particular. First, we derive a decomposition theorem for large phase gadgets, something that is of key importance to recent developments in quantum circuit optimisation and T-count reduction in particular. Then, using the same rule set, we prove a completeness theorem for quantum Boolean circuits (QBCs), which adds to the plethora of complete reasoning systems under the umbrella of ZX-calculus.

1 Introduction

The ZX-calculus [6, 7] is a universal graphical language for qubit theory, which comes equipped with simple rewriting rules that enable one to transform diagrams representing one quantum process into another quantum process. More broadly, it is the work-horse of categorical quantum mechanics, which aims for a high-level formulation of quantum theory [1, 9].

Recently ZX-calculus has been completed by Ng and Wang [20], that is, provided with sufficient additional rules so that any equation between matrices in Hilbert space can be derived in ZX-calculus. This followed earlier completions by Backens for stabiliser theory [2] and one-qubit Clifford+T circuits [3], and by Jeandel, Perdrix and Vilmart for general Clifford+T theory [15].

This paper concerns with the 'utility' of ZX-rules. While in principle the rules in [20] are sufficient to any other rule, it is by no means guaranteed that it is in any way intuitive, easy, or even realistic to do so. While the original rules of [6, 7] have been inherited by all ZX-calculi, comparing [20] with two more recent universal completeness results [16, 21] one immediately notices that the additional rules that give completeness are entirely different in each of the papers, and their relationship is by no means obvious.

Consequently, the new game in town is to match rules on their utility, and in some cases we will need to derive new rules. In fact, the new rule of the completeness theorem of [21] was in fact discovered/derived by two of the current authors with the particular purpose of quantum circuit simplification in mind [10], and this utility preceded the completeness result. One ingredient of the axiomatisation of the original universal completeness result [20] is a new primitive of ZX-calculus, the triangle, which has some clearly appealing features, but hasn't really been exploited yet.

We will explore one utility of the triangle, namely the role of standard rules governing the AND-gate when translated as ZX-rules. In its simplest form the ZX-encoding of the AND-gate directly involves the triangle (see [9] Exercise 12.10). We in particular derive two results:

Decomposition of phase gadgets. Recently ZX-calculus has been used to outperform all other methods in the area of circuit optimisation [19, 17, 11]. Key to these for the purpose of T-gate reductions are so-called 'phase gadgets' named by Kissinger and van de Wetering [19], and were independently introduced by de Beaudrap and Wang, summarised in [11]. Decomposing larger $\pi/4$-phase gadgets into

Submitted to:
QPL 2019

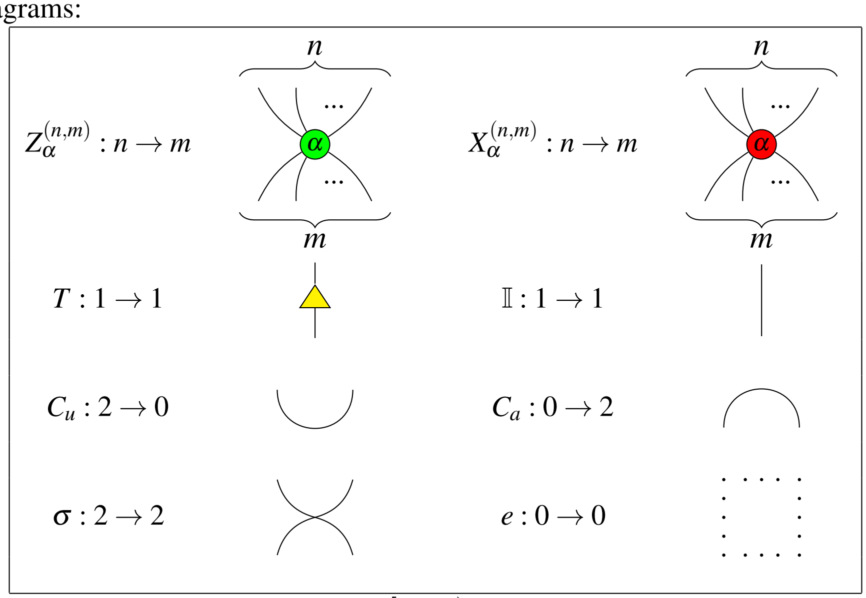
smaller ones (less than 4 lines) is vital for reducing T-count further than reduction effect of phase gadget fusion. In this paper, we derive a general decomposition theorem for arbitrary phase gadget in terms of AND-gates. As a consequence, we simply derive the powerful decomposition of $\pi/4$-phase gadgets.

ZX-completeness for quantum Boolean circuits. Using the same rule set, we prove a completeness theorem for quantum Boolean circuits. Circuit relations by Iwama, Kambayashi and Yamashita that achieve this have been known for a while [14], also Cockett and Comfort have proved Iwama et al.'s rules in the symmetric monoidal category, TOF, generated by the Toffoli gate and computational ancillary bits [5]. We obtain our ZX-completeness result by proving Iwama et al.'s rules in the ZX-calculus with the rule set established in this paper, without any resort to having a Toffoli gate as the generator. This work does place results in circuit re-writing all under the umbrella of ZX-calculus. One particular advantage of this is the availability of automation tools which already has proved to be very useful for the above mentioned circuit optimisation results [18].

Other work. An early motivation for the GHZ/W-calculus [8], now completed by Hadzihasanovic [12, 13] and known as ZW-calculus, was extended control operations, which is also one of the motivational upshots of the triangle symbol. The triangle symbol entered the ZX-picture when ZW-calculus was translated to the ZX-context. A very recent ZX-alike calculus is ZH-calculus [4], which also allows easy representation of the AND-gate, even easier than what we use in this paper, however, with the triangle symbol, one could realise a seamless connection with the traditional ZX-calculus. For now, ZX-calculus is (still) the umbrella under which quantum circuit optimisation is outperforming all competition, and were most completeness theorems have been stated, so a study of the AND-gate within this context is more than justified.

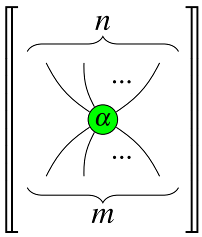
2 ZX-calculus generators

The ZX-calculus lives in a compact closed category whose objects are the natural numbers $\mathbb{N}$ and whose monoidal product is addition, $a \otimes b = a + b$. A general morphism $k \to l$ in this category is simply a k-input, l-output diagram generated, via finite sequential and parallel composition, by the following elementary diagrams:

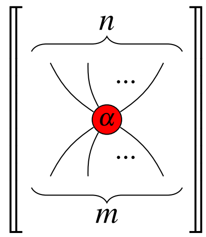


where e represents the empty diagram, and $\alpha \in [0, 2\pi)$. Throughout this paper, all the diagrams are read from top to bottom, and non-zero scalars are ignored.

Each generating diagram $D : k \to l$ above has a standard interpretation as a linear map between Hilbert spaces, $[\![D]\!] : (\mathbb{C}^2)^{\otimes k} \to (\mathbb{C}^2)^{\otimes l}$. By endowing each tensor factor $\mathbb{C}^2$ with its standard inner product and by identifying its elements $(1,0)$ and $(0,1)$ as the qubit Z-basis states $|0\rangle$ and $|1\rangle$, we can present each map $[\![D]\!]$ as a matrix:

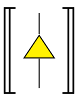
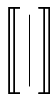
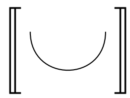


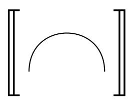
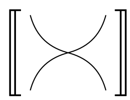
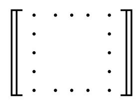
$= |0\rangle^{\otimes m}\langle 0|^{\otimes n} + e^{i\alpha}|1\rangle^{\otimes m}\langle 1|^{\otimes n}$;



$= |+\rangle^{\otimes m}\langle +|^{\otimes n} + e^{i\alpha}|-\rangle^{\otimes m}\langle -|^{\otimes n}$,

where $|+\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)$ and $|-\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big)$ are the qubit X-basis states:

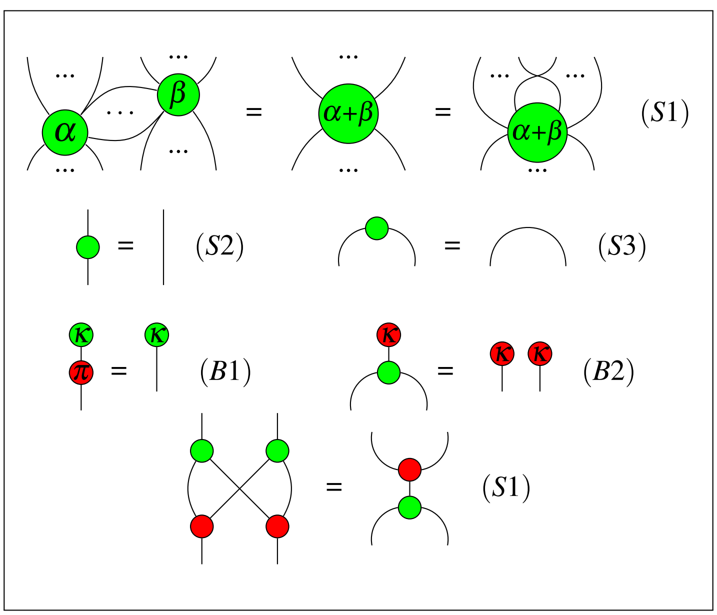

$= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$;

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

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


$= \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$;

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

$= 1$.

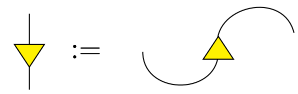
We can extend these matrix interpretations to general ZX-diagrams simply by demanding that the composition operations for ZX-diagrams are compatible with those for matrices, namely that $[\![D_1 \circ D_2]\!] = [\![D_1]\!] \circ [\![D_2]\!]$ and $[\![D_1 \otimes D_2]\!] = [\![D_1]\!] \otimes [\![D_2]\!]$ for every suitable pair of ZX-diagrams D_1 and D_2.

3 ZX-calculus rules

Here is the fragment of stabilizer-style ZX-calculus rules that we will make use of in this paper, where $\alpha, \beta \in [0,\ 2\pi)$, $\kappa \in \{0, \pi\}$. All of these rules also hold when the colours red and green swapped.

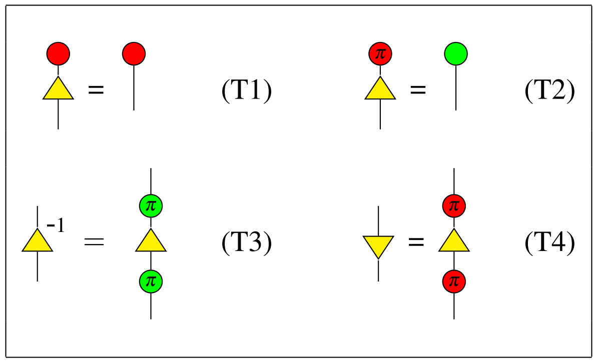


Noting that we haven't mentioned adjoints, we represent the transpose as follows:

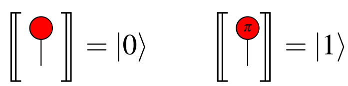


(1)

We will make use of the following simple triangle rules of the universal complete rules of [20]:



These rules represent the fact that the triangle breaks down of unitarity, or equivalently, the non-preservation of unitarity, more specifically, given that the red spider states $X_{\alpha}^{(0,1)}$ are the qubit Z-basis states:



(2)

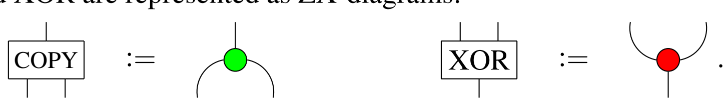
we have:

- Rules (T1) and (T2) show that the triangle turns orthonormal states into unbiased states.
- Rules (T3) and (T4) show that the inverse of the triangle is not equal to its adjoint.

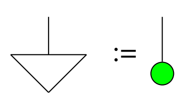
This breakdown of unitarity greatly extends expressiveness, for example, for control operations where a basis can be used to switch between unbiased vectors.

4 ZX rules on AND-gates

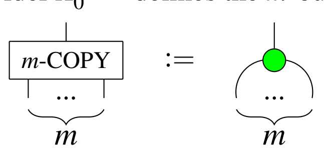
The interpretation (2) also enables us to view each red spider state as a diagrammatic representation of a classical bit value. As such, the standard ZX-rules (S1) and (B2) easily demonstrate how the classical processes COPY and XOR are represented as ZX-diagrams:



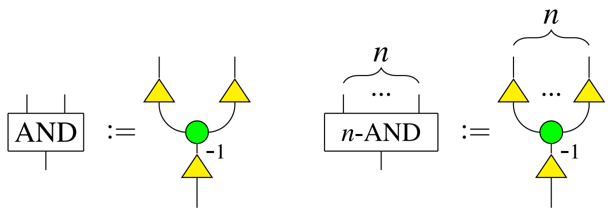
Also, the unit of the copy process can be seen as a classical deleting process:



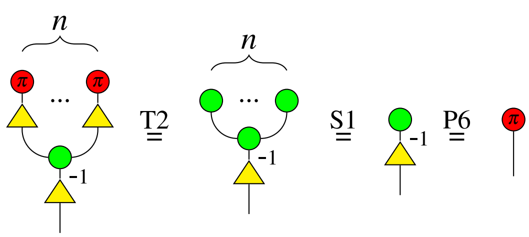
Proposition 1 shows how the green spider $X_0^{(1,m)}$ defines the m-output generalized COPY for any $m \geq 1$:



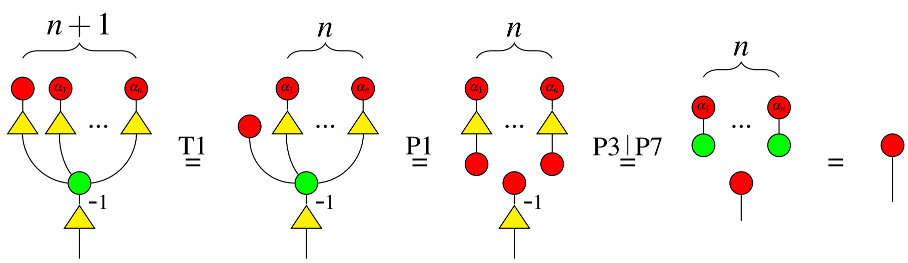
As illustrated in [22], we can represent the AND process and its generalization, the n-AND:



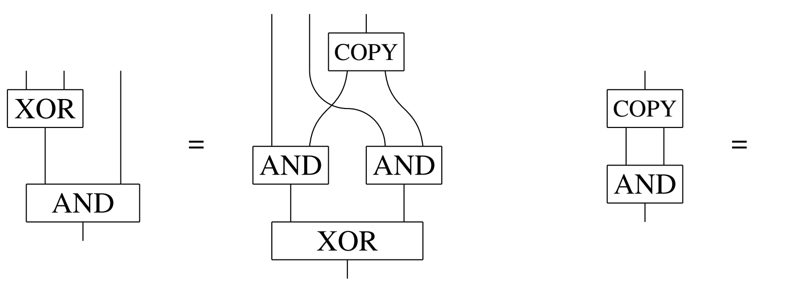
It is straightforward to see that these diagrams give a proper representation of the n-input generalized AND. For, by Proposition 6, the 0-AND process simply returns $|1\rangle$; and, for all $n \geq 0$, the $(n+1)$-AND process returns $|1\rangle$ whenever its input bit string consists solely of $|1\rangle$ states:



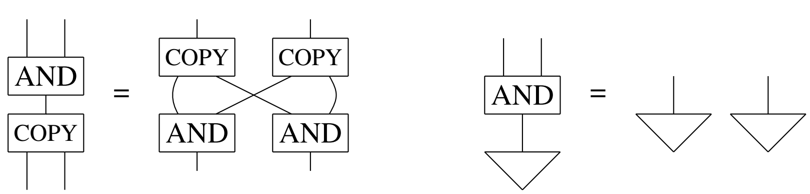
and returns $|0\rangle$ whenever its input bit string contains at least one $|0\rangle$ state:



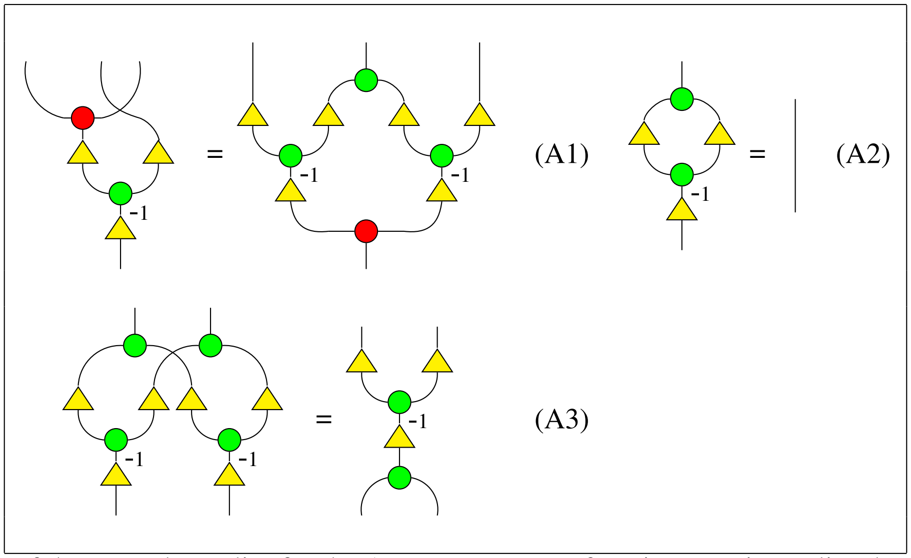
where $\alpha_i \in \{0, \pi\}, i = 1, \cdots, n$. By identifying the COPY, XOR, and AND in ZX-diagrams, we have demonstrated that the ZX-calculus has all the machinery necessary to represent Boolean algebra. In light of this fact, we expect that the Boolean identities $(p \oplus q) \cdot r = (p \cdot r) \oplus (q \cdot r)$ and $p \cdot p = p$ to hold:



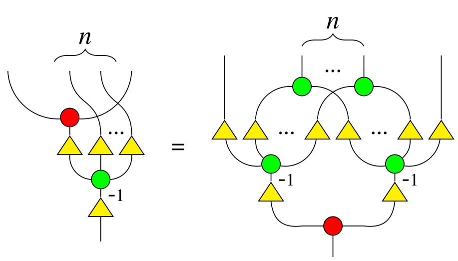
Furthermore, AND is actually a function map, so a homomorphism for COPY and its unit (see e.g., [9]):



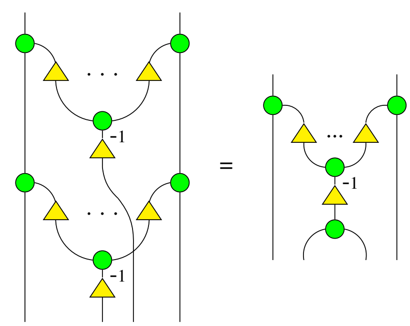
In terms of ZX-diagrams, these equations for AND translate as:



The ZX form of the second equality for the AND process as a function map is not listed as a rule, since it can be derived from other rules (see Proposition 8 in the Appendix). The rules (A1) and (A3) have the following useful generalisations whose proofs can be found in the Appendix:



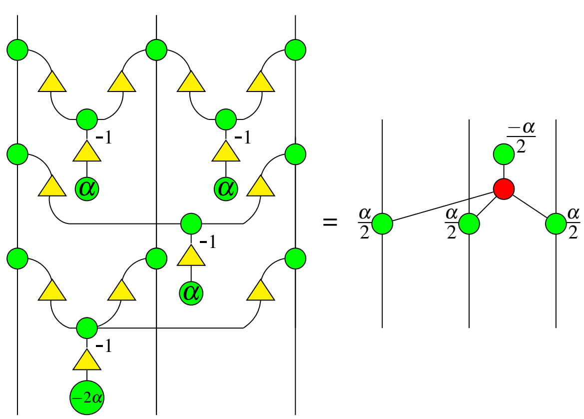
$(L2)$



$(L3)$

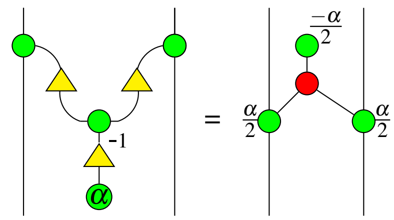
5 AND-gates and phase gadgets

In this section, using the AND-gate representation, we derive a decomposition theorem for large $\pi/4$-phase gadgets into smaller phase gadgets, which has been shown to be very useful in reducing T-count with ZX-calculus [11]. For this purpose, in addition to the rules listed in the figures of previous section, we assume the following decomposition of small phase gadgets using AND-gates:



(3)

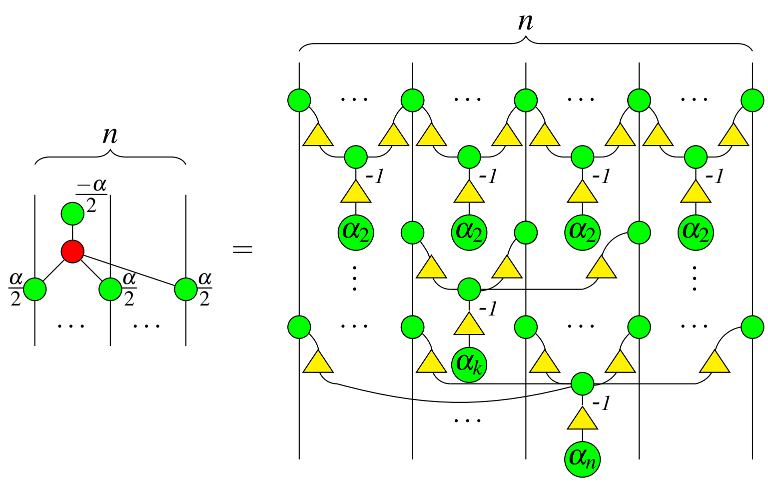
where $\alpha \in [0, 2\pi)$. Its correctness can be verified by plugging the standard basis (in ZX form) onto the top of the leftmost line on both sides. If we plug and respectively onto the bottom and top of the leftmost lines of both sides of (3), then we get:



(4)

The following theorem gives the decomposition of phase gadget in terms of AND-gates, as is proved in the Appendix.

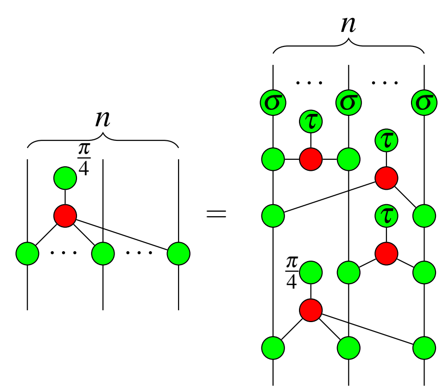
Theorem 5.1. *For any $\alpha \in [0, 2\pi)$, $n \geq 2$, we have:*



(5)

where for each $k \in \{2, \cdots, n\}$ lines of the RHS of (5), there locates one and only one k-AND gate plugged with a phase with angle $\alpha_k = (-1)^k 2^{k-2}\alpha$. Clearly $\alpha_{k+1} = -2\alpha_k$.

Corollary 5.2.



(6)

where $n \geq 3$, for the RHS of (6), on each line, there is a 1-line gadget with phase angle $\sigma = \frac{(n-2)(n-3)\pi}{8}$, for every two of the n lines, there is a 2-line gadget with phase angle $\tau = \frac{(3-n)\pi}{4}$, and for every three of the n lines, there is a 3-line gadget with phase angle $\frac{\pi}{4}$.

Proof. Since the angle of the phase gadget is $\frac{\pi}{4}$, we let $\alpha = -\frac{\pi}{2}$ in (5). Then on the RHS of (5), $\alpha_k = 0, \forall k \geq 4$. Thus all the k-AND gates plugged with phase α_k and $k \geq 4$ become identities, which means we just have phase-plugged 2-AND gates and 3-AND gates left in the RHS of (5). Now if we replace all phase-plugged 2-AND gates and 3-AND gates by the phase gadgets in (4) and (3) respectively, after phase gadget fusion, we then have the equality (6). Obviously, it can be generalised to the decomposition of $\frac{\pi}{2^k}$-phase gadget for any $k \geq 0$. □

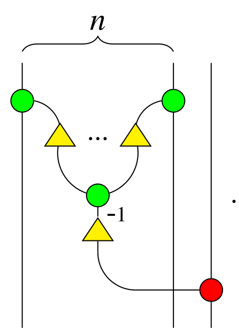
6 CNOT-based Quantum Boolean Circuits

In [14] a quantum Boolean circuit is defined as follows:

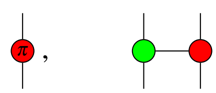
- A *quantum Boolean circuit* of size M over qubits $|x_1\rangle, ..., |x_N\rangle$ is a sequence of CNOT gates $[t_1, C_1] \cdots [t_i, C_i] \cdots [t_M, C_M]$ where $1 \leq t_i \leq N$ and $C_i \subseteq \{1, ..., N\}$.

In this section, we obtain the ZX-completeness result for quantum Boolean circuits by proving in ZX-calculus the complete set of six transformation rules presented in [14].

The ZX-diagram for a CNOT gate is simply (see e.g., [22]):



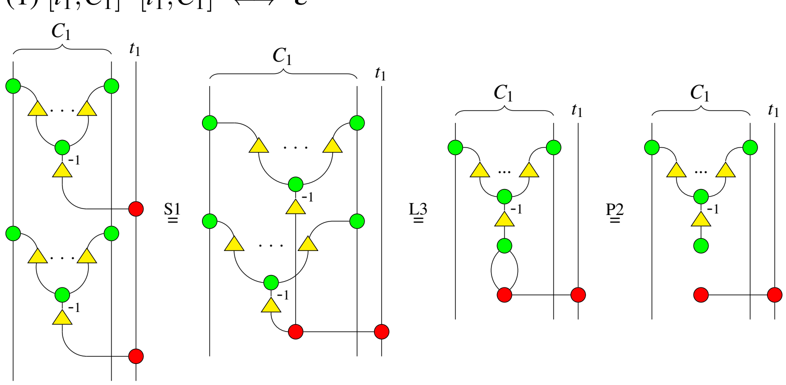
As a check to this definition, the reader can verify that in the $n = 0$ and $n = 1$ cases, this representation reduces to the NOT gate and the standard CNOT gate, as expected:

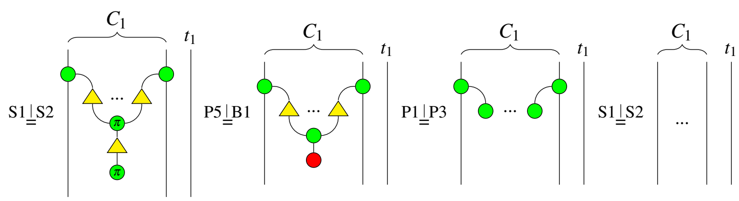


Theorem 6.1. *Let ε represent the 'identity' gate and $\Longleftrightarrow$ denote a transformation. If D_1 and D_2 are any two CNOT-based circuits expressed as ZX-diagrams, then $ZX \vdash D_1 = D_2$.*

Proof. It suffices to prove that each of the six transformation rules, expressed as ZX-diagrams, are derivable using only the rule set given in the tables above.

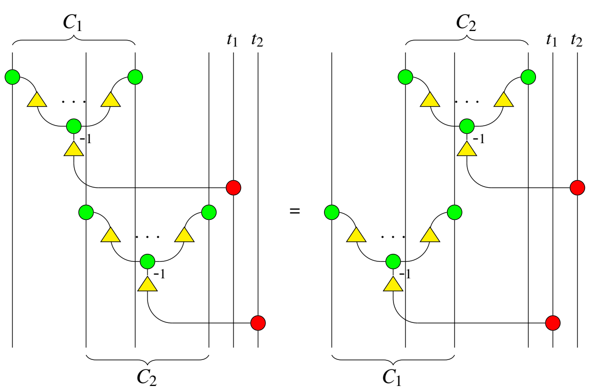
(1) $[t_1, C_1] \cdot [t_1, C_1] \Longleftrightarrow \varepsilon$



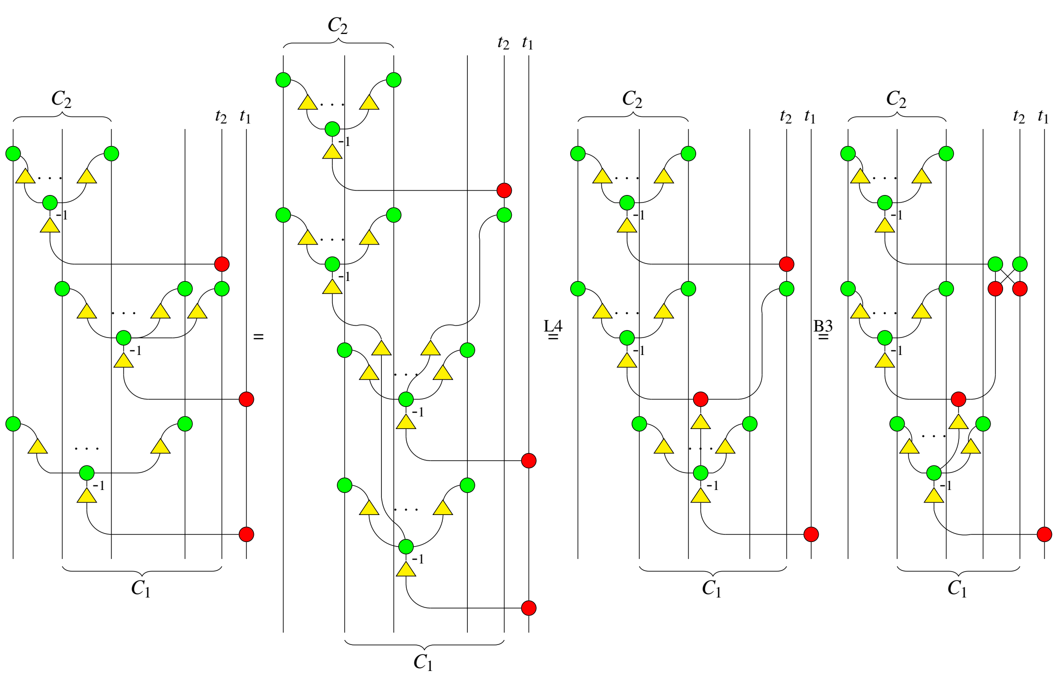


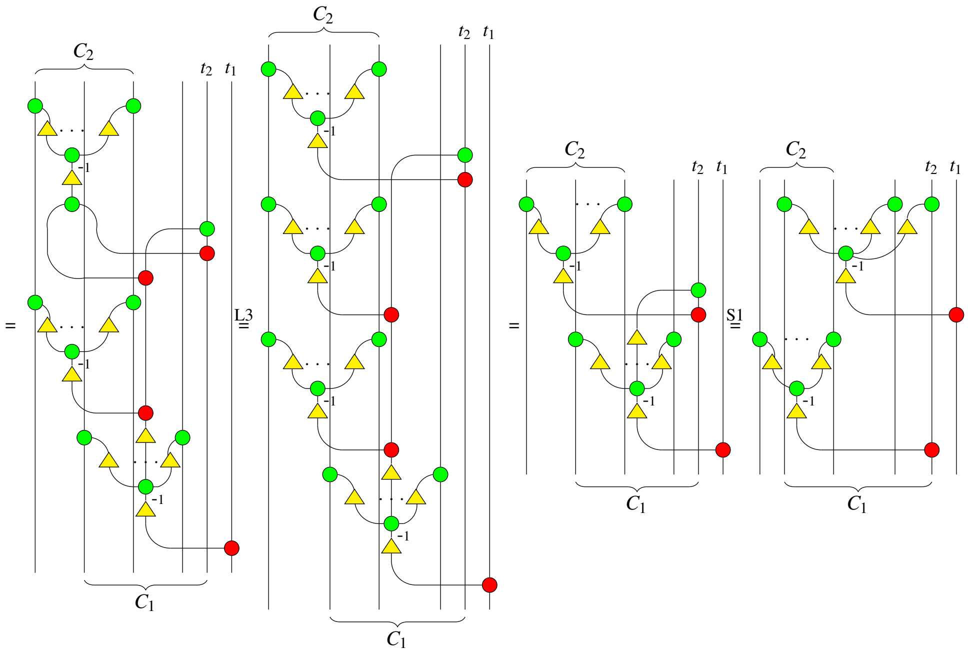
(2) $[t_1, C_1] \cdot [t_2, C_2] \iff [t_2, C_2] \cdot [t_1, C_1]$, if $t_1 \notin C_2$ and $t_2 \notin C_1$

This is a simple consequence of (S1). The case in which $t_1 \neq t_2$ is shown below.



(3) $[t_1, C_1] \cdot [t_2, C_2] \iff [t_2, C_2] \cdot [t_1, C_1] \cdot [t_1, C_1 \cup C_2 - \{t_2\}]$ if $t_1 \notin C_2$ and $t_2 \in C_1$

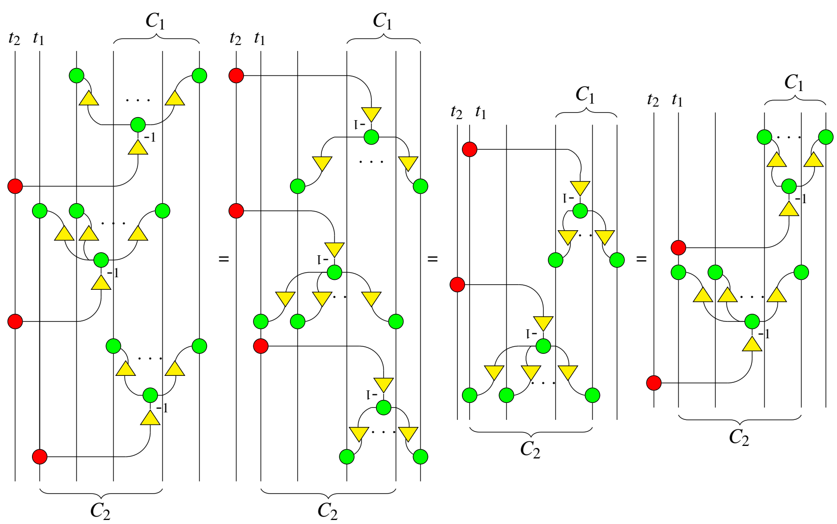




The second-to-last equality comes from rule 1.

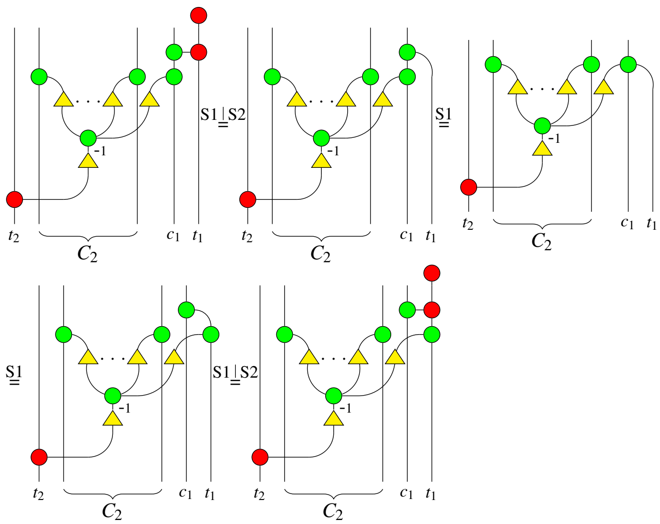
(4) $[t_1, C_1] \cdot [t_2, C_2] \iff [t_2, C_1 \cup C_2 - \{t_1\}] \cdot [t_2, C_2] \cdot [t_1, C_1]$ if $t_1 \in C_2$ and $t_2 \notin C_1$

This follows immediately from rule 3:

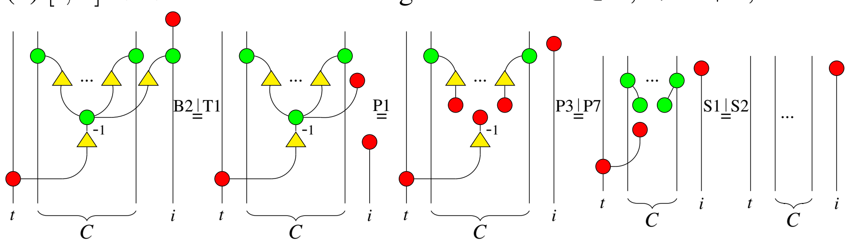


(5) $[t_1, \{c_1\}] \cdot [t_2, C_2 \cup \{c_1\}] \iff [t_1, \{c_1\}] \cdot [t_2, C_2 \cup \{t_1\}]$ if $t_1 > n+1$ and no CNOT_{t_1} before $[t_1, \{c_1\}]$

Note that we must assume $t_1 \neq t_2$ for the generalized CNOT gate $[t_2, C_2 \cup \{t_1\}]$ to be well-defined.



(6) $[t,C] \iff \varepsilon$ if there is an integer i such that $i \in C$, $i > n+1$, and there is no CNOT$_i$ before $[t,C]$



□

Acknowledgements

AM thanks the Mellon Mays Undergraduate Fellowship Program for its generous support of his research. BC and QW are grateful for an EPSRC IAA in collaboration with Cambridge Quantum Computing Ltd.

References

[1] S. Abramsky and B. Coecke. A categorical semantics of quantum protocols. In Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science (LICS), pages 415–425, 2004. arXiv:quant-ph/0402130.

[2] M. Backens. The ZX-calculus is complete for stabilizer quantum mechanics. New Journal of Physics, 16:093021, 2014. arXiv:1307.7025.

[3] Miriam Backens. The zx-calculus is complete for the single-qubit clifford+t group. In Bob Coecke, Ichiro Hasuo, and Prakash Panangaden, editors, Proceedings of the 11th workshop on Quantum Physics and Logic, volume 172 of Electronic Proceedings in Theoretical Computer Science, pages 293–303. Open Publishing Association, 2014.

[4] Miriam Backens and Aleks Kissinger. Zh: A complete graphical calculus for quantum computations involving classical non-linearity. In Peter Selinger and Giulio Chiribella, editors, Proceedings of the 15th International Conference on Quantum Physics and Logic, Halifax, Canada, 3-7th June 2018, volume 287 of Electronic Proceedings in Theoretical Computer Science, pages 23–42. Open Publishing Association, 2019.

[5] J.R.B. Cockett and Cole Comfort. The category tof. In Peter Selinger and Giulio Chiribella, editors, Proceedings of the 15th International Conference on Quantum Physics and Logic, Halifax, Canada, 3-7th June 2018, volume 287 of Electronic Proceedings in Theoretical Computer Science, pages 67–84. Open Publishing Association, 2019.

[6] B. Coecke and R. Duncan. Interacting quantum observables. In Proceedings of the 37th International Colloquium on Automata, Languages and Programming (ICALP), Lecture Notes in Computer Science, 2008.

[7] B. Coecke and R. Duncan. Interacting quantum observables: categorical algebra and diagrammatics. New Journal of Physics, 13:043016, 2011. arXiv:quant-ph/09064725.

[8] B. Coecke and A. Kissinger. The compositional structure of multipartite quantum entanglement. In Automata, Languages and Programming, Lecture Notes in Computer Science, pages 297–308. Springer, 2010. arXiv:1002.2540.

[9] B. Coecke and A. Kissinger. Picturing Quantum Processes. A First Course in Quantum Theory and Diagrammatic Reasoning. Cambridge University Press, 2017.

[10] B. Coecke and Q. Wang. Zx-rules for 2-qubit Clifford+T quantum circuits. In Jarkko Kari and Irek Ulidowski, editors, Reversible Computation - 10th International Conference, RC 2018, Leicester, UK, September 12-14, 2018, Proceedings, volume 11106 of Lecture Notes in Computer Science, pages 144–161. Springer, 2018.

[11] Niel de Beaudrap and Quanlong Wang. A heuristic to reduce $\pi/4$-phase-parity circuits. submitted to QPL2019, 2019.

[12] A. Hadzihasanovic. A diagrammatic axiomatisation for qubit entanglement. In Proceedings of the 30th Annual IEEE Symposium on Logic in Computer Science (LICS), 2015. arXiv:1501.07082.

[13] A. Hadzihasanovic. The algebra of entanglement and the geometry of composition. PhD thesis, University of Oxford, 2017.

[14] Kazuo Iwama, Yahiko Kambayashi, and Shigeru Yamashita. Transformation rules for designing cnot-based quantum circuits. In Proceedings of the 39th annual Design Automation Conference, pages 419–424. ACM, 2002.

[15] Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. A complete axiomatisation of the zx-calculus for clifford+ t quantum mechanics. arXiv preprint arXiv:1705.11151, 2017.

[16] Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. Diagrammatic reasoning beyond clifford+ t quantum mechanics. arXiv preprint arXiv:1801.10142, 2018.

[17] A. Kissinger and A. Meijer-van de Griend. Cnot circuit extraction for topologically-constrained quantum memories. arXiv preprint arXiv:1904.00633, 2019.

[18] A. Kissinger and J. Wetering. Pyzx: Large scale automated diagrammatic reasoning. arXiv preprint arXiv:1904.04735, 2019.

[19] A. Kissinger and J. Wetering. Reducing t-count with the zx-calculus. arXiv preprint arXiv:1903.10477, 2019.

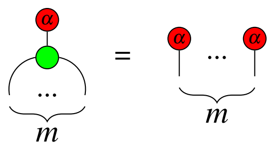
[20] Kang Feng Ng and Quanlong Wang. A universal completion of the zx-calculus. arXiv preprint arXiv:1706.09877, 2017.

[21] R. Vilmart. A near-optimal axiomatisation of zx-calculus for pure qubit quantum mechanics. arXiv preprint arXiv:1812.09114, 2018.

[22] Quanlong Wang. Completeness of the ZX-calculus. PhD thesis, University of Oxford, 2018.

Appendix: Propositions, Lemmas and Proofs

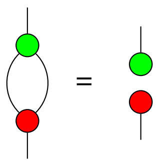
Proposition 1

For $m \geq 1$, 

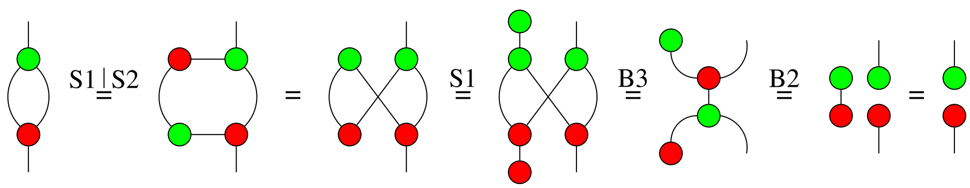
(P1)

Proof. Using S1 we can decompose an $R_Z^{(1,m)}$ diagram into an $(m-1)$-fold composition of $R_Z^{(1,2)}$ diagrams. Repeatedly applying B2 then yields the desired result.

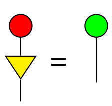
Proposition 2



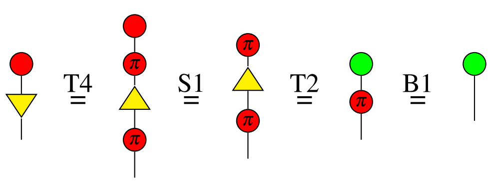
(P2)

Proof. 

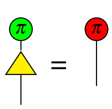
Proposition 3



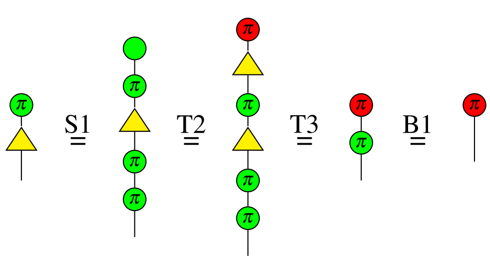
(P3)

Proof. 

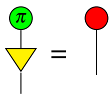
Proposition 4



(P4)

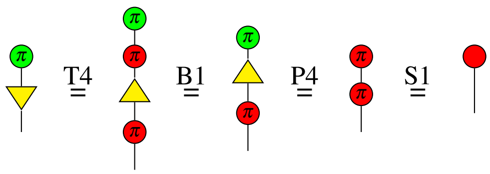
Proof. 

Proposition 5

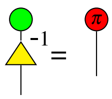


(P5)

Proof.

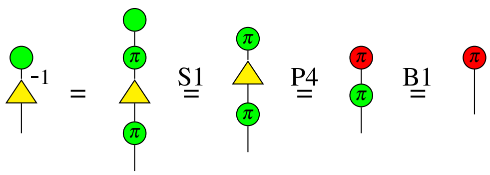


Proposition 6

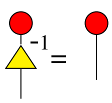


(P6)

Proof.

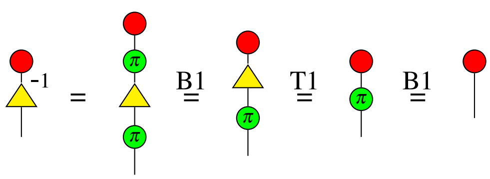


Proposition 7

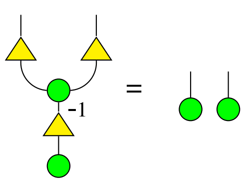


(P7)

Proof.

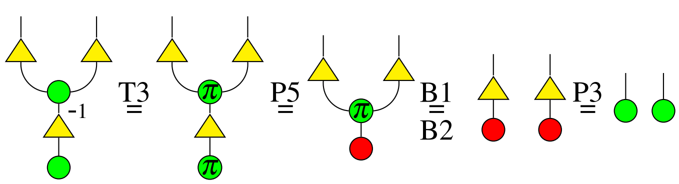


Proposition 8



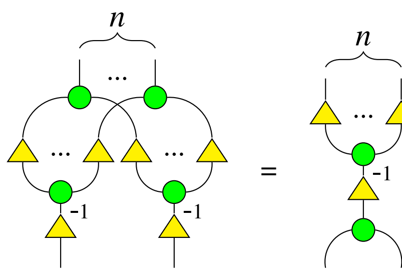
(P8)

Proof.



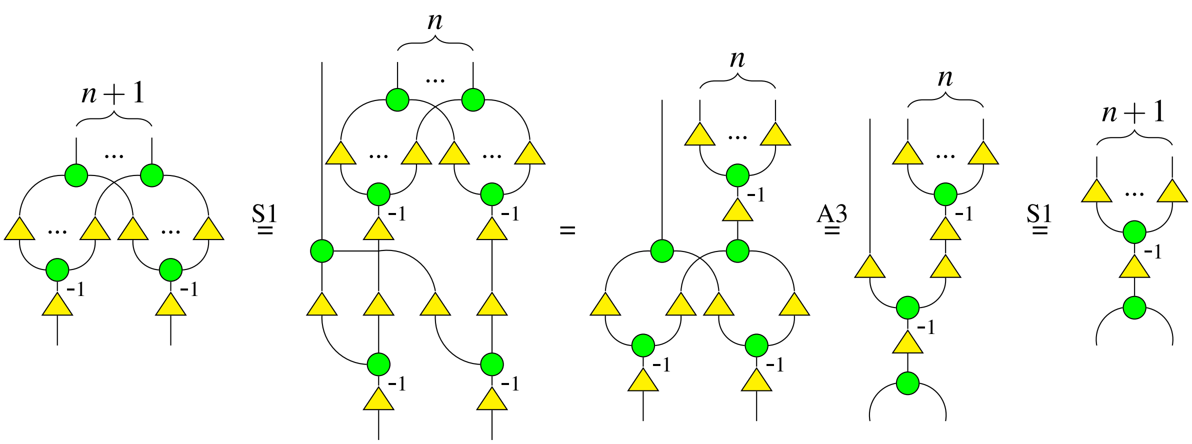
Lemma 1

For all $n \geq 0$,



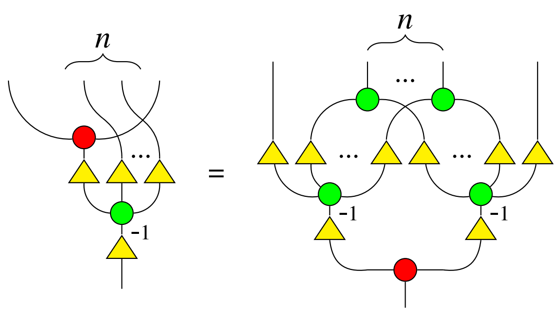
(L1)

Proof. The $n = 0$ case follows from B2 and P6, the $n = 1$ case follows from (S2) and (T3), and the $n = 2$ case is simply A1. The lemma is true in all other cases, since whenever it holds for some $n \geq 2$, it is also valid for $n+1$:



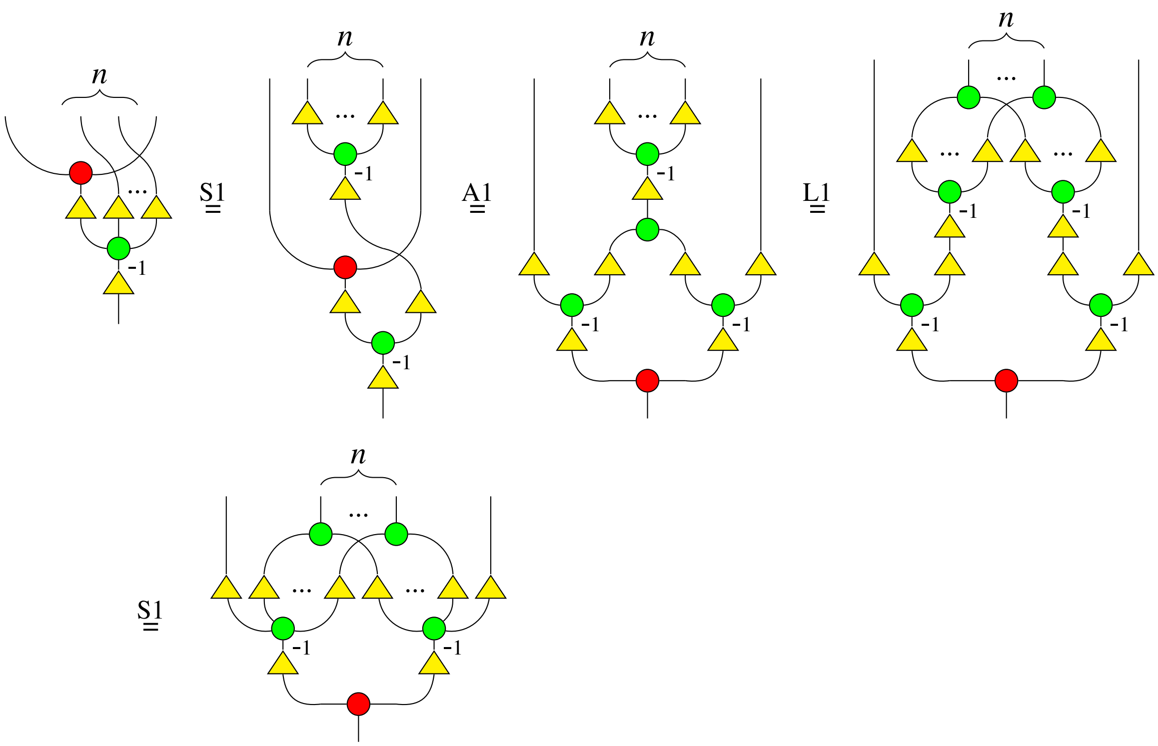
Lemma 2

For all $n \geq 0$,

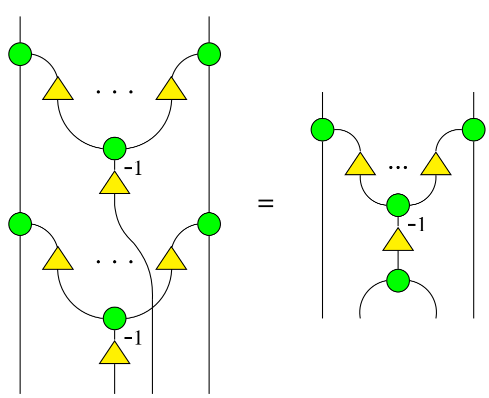


(L2)

Proof. The $n = 0$ case follows from S2 and T3. We obtain all other cases by applying Lemma 1:

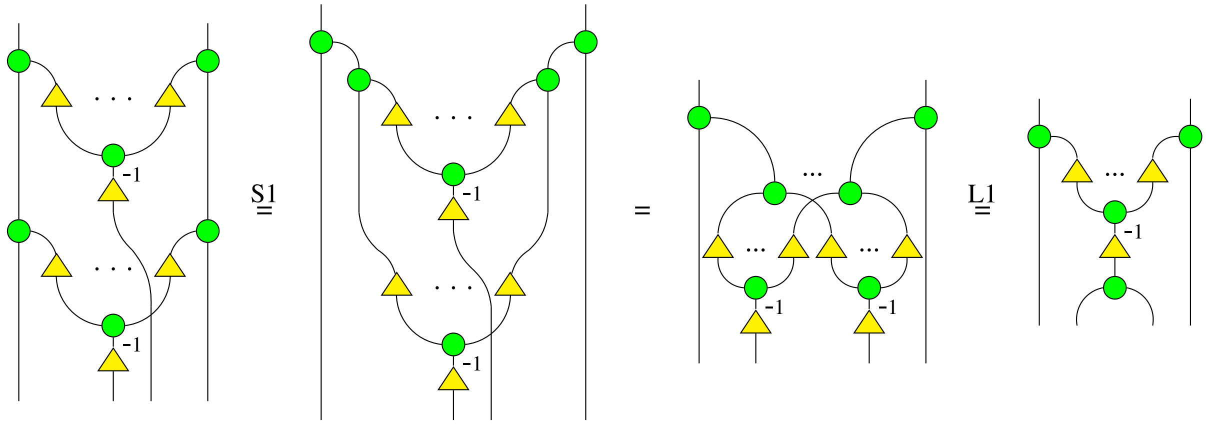


Lemma 3

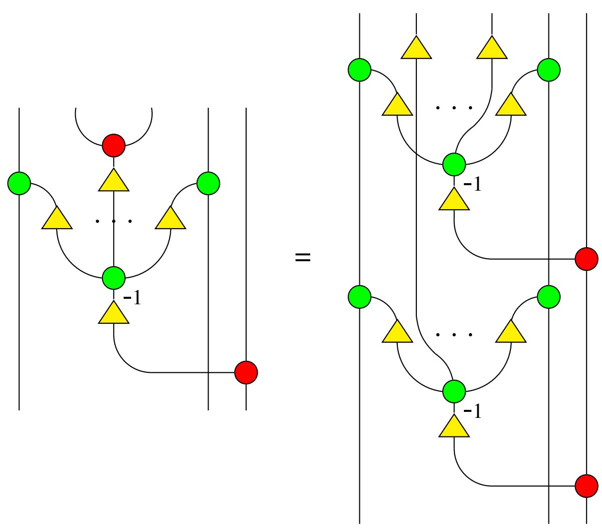


(L3)

Proof.

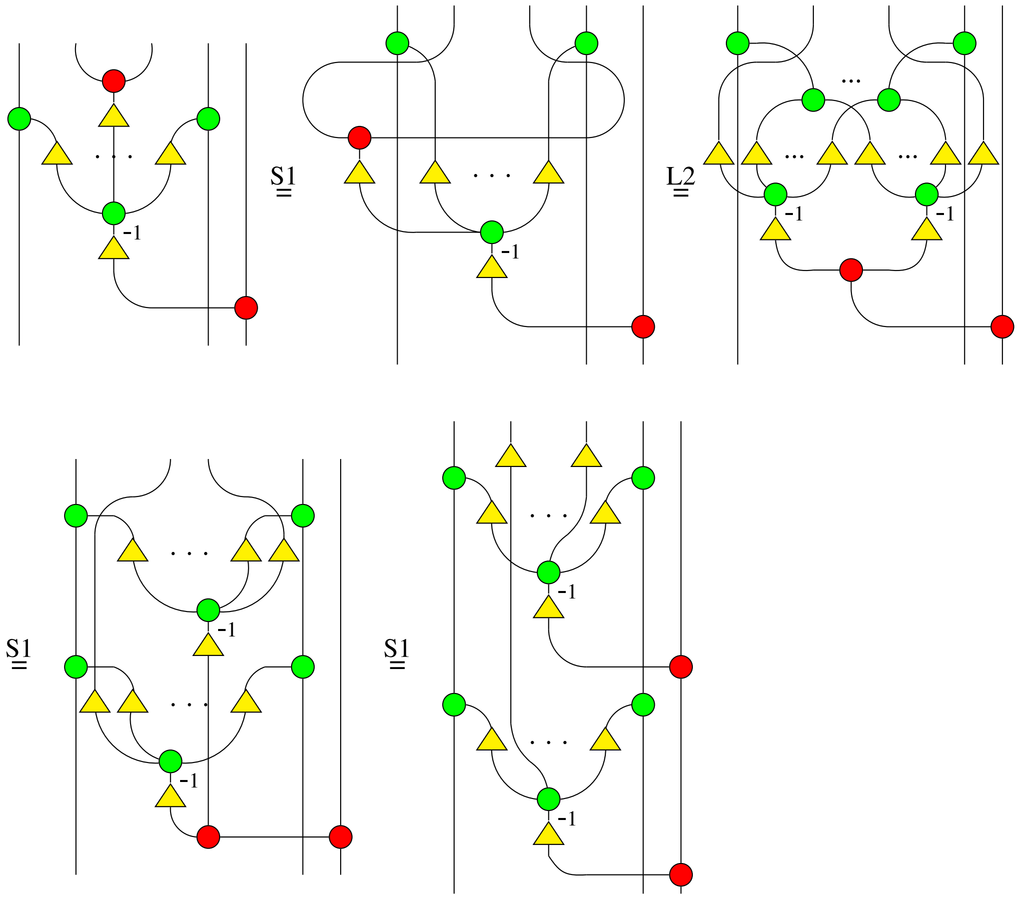


Lemma 4



(L4)

Proof.

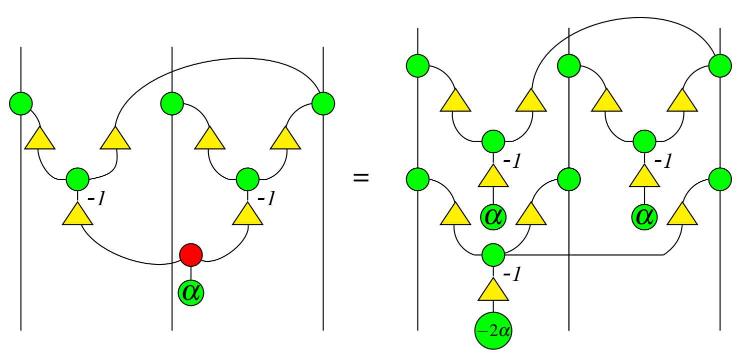


□

Proof of Theorem 5.1

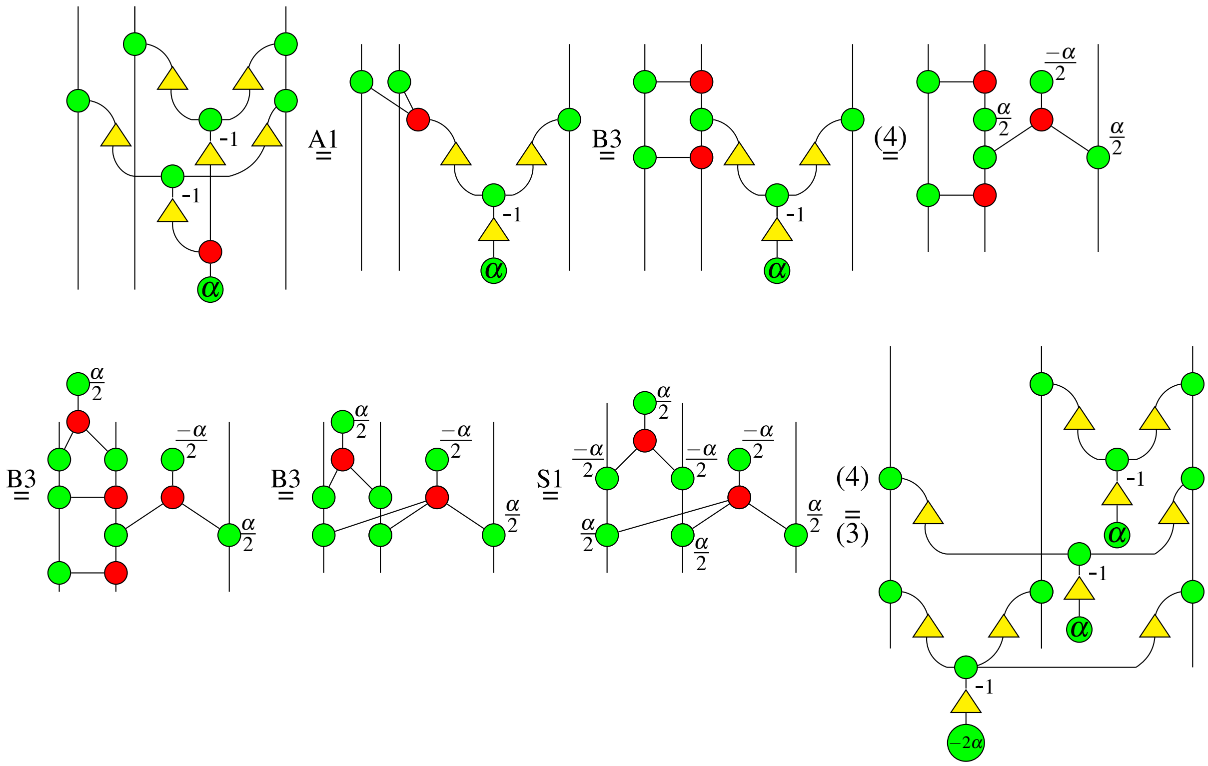
First, we need the following lemmas.

Lemma 6.2. *For any $\alpha \in [0, 2\pi)$, we have:*



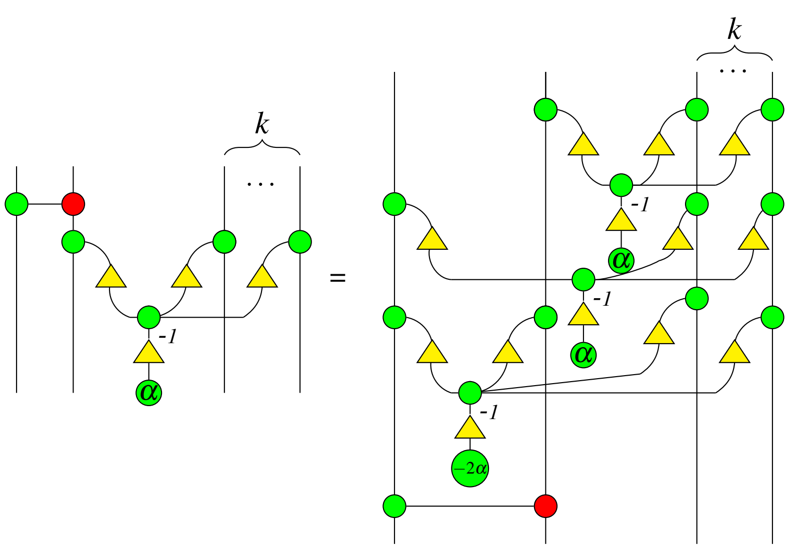
(7)

Proof.



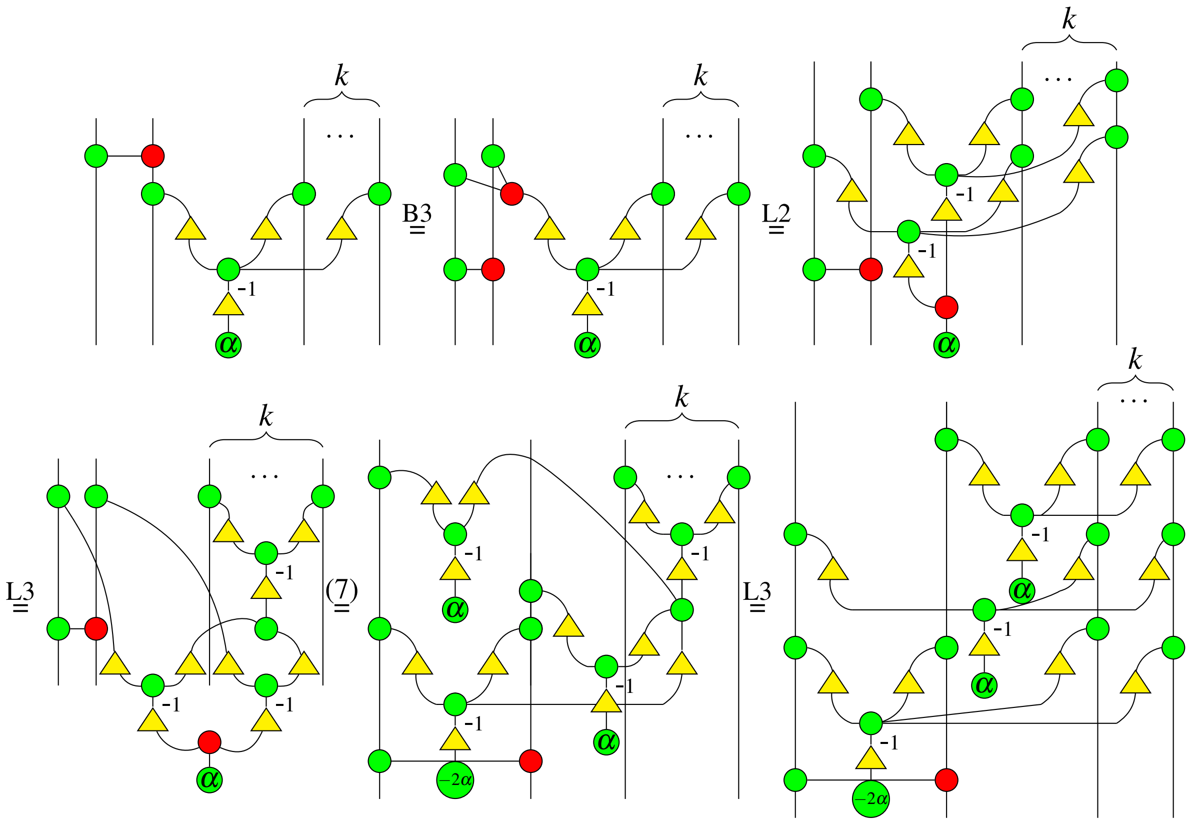
□

Lemma 6.3. *For any* $\alpha \in [0, 2\pi)$, $k \geq 1$, *we have*



(8)

Proof.

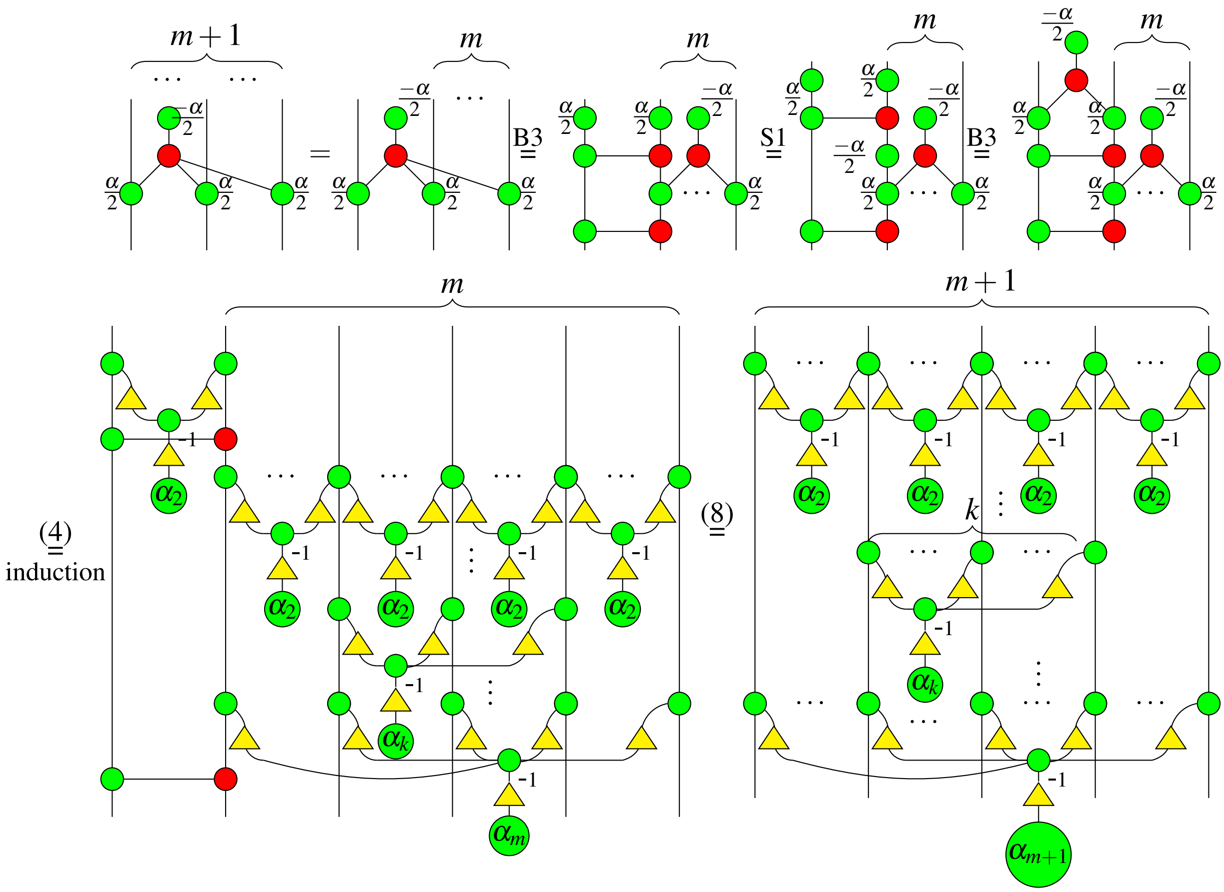


□

Now we are ready to prove Theorem 5.1.

Proof. We prove by induction on n. If $n = 2$, it is just the equality (4) which can be derived from (3).

Assume that (5) holds for $n = m$. Then for $n = m+1$, we have



Therefore, (5) holds for $n = m+1$. This completes the proof. □