Generators and Relations for Real Stabilizer Operators

Justin Makary, Neil J. Ross, and Peter Selinger
Department of Mathematics and Statistics
Dalhousie University, Halifax, Canada

Real stabilizer operators, which are also known as real Clifford operators, are generated, through composition and tensor product, by the Hadamard gate, the Pauli Z gate, and the controlled-Z gate. We introduce a normal form for real stabilizer circuits and show that every real stabilizer operator admits a unique normal form. Moreover, we give a finite set of relations that suffice to rewrite any real stabilizer circuit to its normal form.

1 Introduction

Stabilizer operators, which are also known as *Clifford* operators, play a fundamental role in the study of fault-tolerant quantum computation [13]. Stabilizer operators are generated, under composition and tensor product, by the scalar $e^{i\pi/4}$, the Hadamard gate H, the phase gate S, and the controlled-Z gate CZ. For $n \geq 0$, the set of stabilizer operators on n qubits forms a subgroup of the unitary group $\mathrm{U}(2^n)$ and is denoted $\mathscr{C}(n,\mathbb{C})$. Quantum circuits for stabilizer operators have been extensively studied [1, 4, 6, 9, 14, 15, 16]. In particular, [15] gave a finite presentation of stabilizer operators by introducing a normal form for stabilizer circuits together with a finite collection of relations that suffice to rewrite any stabilizer circuit to its normal form.

In the present paper, we study *real* stabilizer operators which are generated by the scalar (-1) and the gates H, Z, and CZ. The group of n-qubit real stabilizer operators $\mathscr{C}(n,\mathbb{R})$ is the intersection of $\mathscr{C}(n,\mathbb{C})$ and the orthogonal group $\mathrm{O}(2^n)$.

Our contributions are as follows. We define a normal form for real stabilizer circuits and we prove that every real Clifford operator admits a unique normal form. We then introduce a finite collection of relations between real stabilizer circuits and show that the relations are complete. The completeness of the relations is established by formulating a rewrite system to transform any real stabilizer circuit into its normal form. Our work follows the methods of [15] but the focus on real operators requires a distinct notion of normal form. In order to conveniently describe these normal forms, we introduce a *typing* for quantum circuits.

Restrictions such as the one considered here were previously studied in the context of randomized benchmarking [10], graphical languages [5, 17], and exact synthesis [3]. Real stabilizers were explicitly investigated in [7, 8, 10, 12]. In particular, [7] provides a complete set of circuit equalities for real stabilizer circuits with ancillas. The presence of ancillas, however, implies that the circuits discussed in [7] do not always correspond to orthogonal operators. In contrast, the circuits discussed here always represent orthogonal operators.

The paper is organized as follows. In Section 2, we examine the structure of the real Pauli and Clifford groups. In Section 3, we review the diagrammatic language of quantum circuits and introduce annotated and typed circuits. In Section 4, we define normal forms and prove that every real stabilizer operator admits a unique normal form. We state our relations in Section 5 and propose a system for rewriting any real stabilizer circuit to its normal form. We discuss future work in Section 6.

M. Backens, C. Heunen (Eds.): Quantum Physics and Logic (QPL) 2021
EPTCS 343, 2021, pp. 14–36, doi:10.4204/EPTCS.343.2

© Justin Makary, Neil J. Ross & Peter Selinger
This work is licensed under the
Creative Commons Attribution License.

2 The Real Pauli and Clifford Groups

We denote the transpose of the matrix A by $A^\intercal$. A matrix A is symmetric if $A = A^\intercal$ and orthogonal if $A^{-1} = A^\intercal$. Following [15], for two matrices A and B, we write $A \bullet B$ for ABA^{-1}. Throughout, we use the terms "operator" and "matrix" interchangeably, assuming that operators are always represented with respect to the standard (computational) basis.

The Pauli matrices X and Z, the Hadamard matrix H and the controlled-Z matrix CZ are defined as

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad \text{and} \quad CZ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}.$$

We note that X and Z are orthogonal and symmetric so that $X^2 = Z^2 = I$. Moreover, X and Z anticommute: $XZ = -ZX$. This implies that $(XZ)^2 = -1$ so that XZ is orthogonal but not symmetric.

Definition 2.1. The *real Pauli group on n qubits* $\mathscr{P}(n,\mathbb{R})$ is defined as

$$\mathscr{P}(n,\mathbb{R}) = \{\pm(P_1 \otimes \ldots \otimes P_n) \mid P_i \in \{I,X,Z,XZ\}\}.$$

In what follows, we drop the adjective "real" and simply refer to $\mathscr{P}(n,\mathbb{R})$ as the Pauli group. In addition, we write $\mathscr{P}(n)$ for $\mathscr{P}(n,\mathbb{R})$. We note that the n-qubit Pauli group $\mathscr{P}(n)$ spans the vector space of real $2^n \times 2^n$ matrices. The proposition below records an important property of Pauli operators.

Proposition 2.2. *Let $P = (-1)^a(P_1 \otimes \ldots \otimes P_n)$ with $P_i \in \{I,X,Z,XZ\}$. Then $P^2 = I$ if and only if there are evenly many i such that $P_i = XZ$.*

Proof. If $P_i \in \{I,X,Z\}$ then $P_i^2 = I$ and if $P_i = XZ$ then $P_i^2 = -1$. Hence, for any $P \in \mathscr{P}(n)$, $P_i^2 = (-1)^d I$ where d is the number of components for which $P_i = XZ$. Thus, $P^2 = I$ if and only if d is even. □

Definition 2.3. The *real Clifford group on n qubits* $\mathscr{C}(n,\mathbb{R})$ is the normalizer of $\mathscr{P}(n)$ in $\mathrm{O}(2^n)$. That is,

$$\mathscr{C}(n,\mathbb{R}) = \{U \in \mathrm{O}(2^n) \mid U \bullet P \in \mathscr{P}(n) \text{ for all } P \in \mathscr{P}(n)\}.$$

As with the Pauli group, we drop the adjective "real" when referring to $\mathscr{C}(n,\mathbb{R})$ in what follows and, for brevity, write $\mathscr{C}(n)$ for $\mathscr{C}(n,\mathbb{R})$. Since the Clifford group is the normalizer of the Pauli group, we have that $C \bullet P \in \mathscr{P}(n)$ for every Clifford C and every Pauli P. Furthermore, conjugation is a group automorphism of $\mathscr{P}(n)$. Note that $H \in \mathscr{C}(1)$, $CZ \in \mathscr{C}(2)$, and $\mathscr{P}(n) \subseteq \mathscr{C}(n)$.

Proposition 2.4. *Let $C \in \mathscr{C}(n)$. If $C \bullet P = P$ for all $P \in \mathscr{P}(n)$, then $C = \pm 1$.*

Proof. By assumption, $CPC^{-1} = P$, for all $P \in \mathscr{P}(n)$. Since $\mathscr{P}(n)$ spans the space of $2^n \times 2^n$ real matrices, it follows that for any $2^n \times 2^n$ operator N, $CNC^{-1} = N$. Thus, C commutes with every real matrix and is therefore a scalar. Because the only scalars in $\mathrm{O}(2^n)$ are ± 1, we get $C = \pm 1$. □

Corollary 2.5. *If C and D are two elements of $\mathscr{C}(n)$ that act identically on $\mathscr{P}(n)$, then $C = \pm D$.*

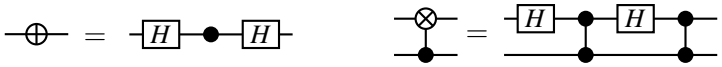
Proof. Since C and D act identically on $\mathscr{P}(n)$, we have $(D^{-1}C) \bullet P = D^{-1} \bullet C \bullet P = D^{-1} \bullet D \bullet P = P$. Thus, by Proposition 2.4, $D^{-1}C = \pm 1$. Hence $C = \pm D$. □

3 Annotated and Typed Circuits

We assume that the reader is familiar with the language of quantum circuits [13]. In this section, we introduce certain decorations which will be convenient in discussing circuits.

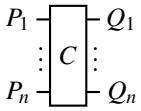
The Hadamard gate, the Pauli Z gate, and the controlled-Z gates are represented below.

For brevity, we introduce some *derived* gates which are shorthand for certain Clifford circuits.



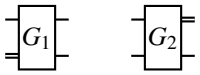
The derived gate on the left is the Pauli X gate. We call the derived gate on the right the CXZ gate, an abbreviation for *controlled-XZ*.

We introduce *annotations* on circuits to concisely indicate the action of a Clifford operator on a Pauli operator under conjugation. When $C \in \mathscr{C}(n)$, and $P = P_1 \otimes \cdots \otimes P_n$, $Q = Q_1 \otimes \cdots \otimes Q_n \in \mathscr{P}(n)$, we write

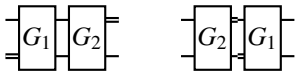


to indicate that $C \bullet P = Q$.

It will be useful for our purposes to *type* circuits. The notion of a *typed gate* coincides with the usual notion of gate, with the difference that the wires of the gate can be of *simple type* or of *double type*, as shown in the two examples below.



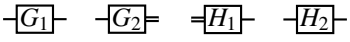
The type of wires does not affect the vertical composition of gates, but two gates can only be composed horizontally if the types of the corresponding wires are the same. For example, below, the composition on the left is well-defined but the composition on the right is not.



Typed circuits are constructed from typed gates with this restriction. The typing of gates and circuits is meant to constrain the construction of circuits.

A typed gate is defined in two stages. In the first stage, a standard gate is specified, for example by associating a diagram to a matrix or to a circuit made from preexisting gates. In the second stage, types are associated to the input and output wires of the gate. Note that any typed circuit can still be viewed as an un-typed circuit by simply *forgetting* about the types of the wires.

By abuse of notation, we will sometimes use a single circuit to concisely specify a family of (typed) circuits. As an illustration, consider the typed gates below.



Then the diagram

represents the family of circuits in which the gate on the left-hand side is one of G_1 or G_2 and the gate on the right-hand side is one of H_1 or H_2 subject to the condition that the circuit is a well-formed typed circuit. There are two circuits in this specific family, which are represented below.

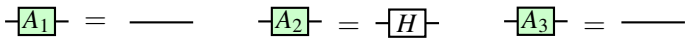
4 Normal Forms for Real Stabilizer Circuits

We now introduce *normal forms* for stabilizer operators. That is, we specify a family of circuits and show that every stabilizer operator is represented by a unique element of this family.

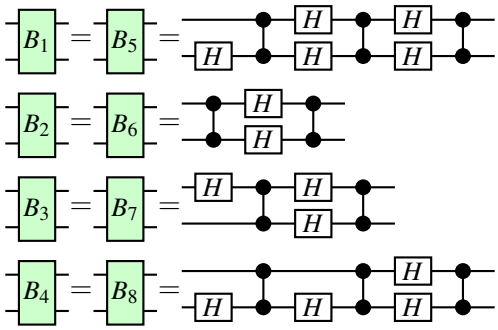
4.1 Derived Generators

We start by introducing *derived generators*, which will serve as the basic building blocks for our normal forms. As discussed in Section 3, we introduce these derived generators in two stages: first we define the gates as (un-typed) circuits and then we specify the types of their wires. There are five kinds of derived generators: A, B, C, D, and E.

Definition 4.1. The *derived generators of kind A* are defined below.

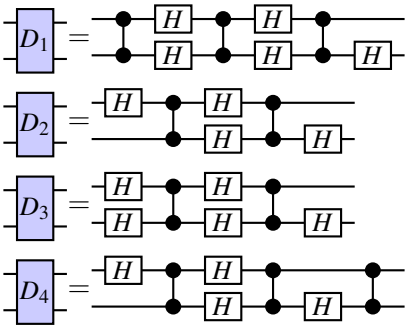


Definition 4.2. The *derived generators kind B* are defined below.



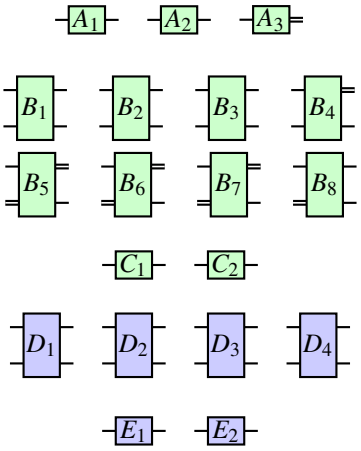
Definition 4.3. The *derived generators of kind C* are defined below.

Definition 4.4. The *derived generators of kind D* are defined below.

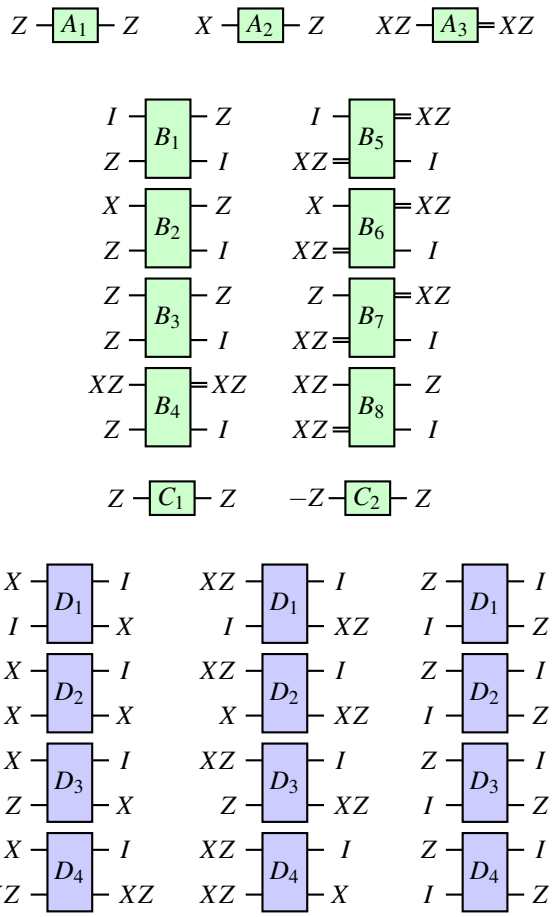


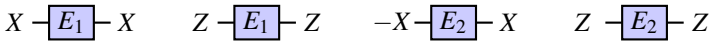
Definition 4.5. The *derived generators of kind E* are defined below.

Definition 4.6. The *typed derived generators of kind A, B, C, D, and E* are defined below.



Proposition 4.7. *The following annotated circuits record the action of the derived generators of kind A, B, C, D, and E on certain Pauli operators.*





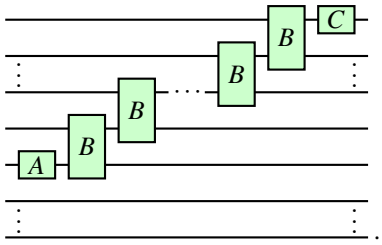
In each case, the specified gate is the unique derived generator of its kind and type that performs the specified action.

Proof. By computation. □

4.2 Normal forms

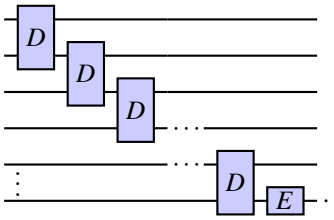
We now describe normal forms.

Definition 4.8. A typed n-qubit circuit is a *Z-circuit* if it is of the form

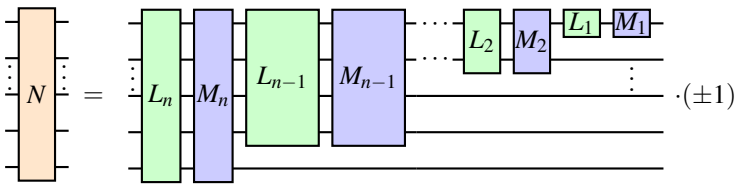


In accordance with the convention introduced in Section 3, the circuit in Definition 4.8 denotes a family of well-formed typed circuits. The types of the derived generators of kind B then imply, for example, that if the first B gate is B_4, then the second B gate can only be B_5, B_6, B_7, or B_8.

Definition 4.9. A typed n-qubit circuit is an *X-circuit* if it is of the form



Definition 4.10. A typed n-qubit circuit is *normal* if it is of the form



where, for $1 \leq i \leq n$, L_i is a Z-circuit, and M_i is an X-circuit.

The propositions below establish that every automorphism of $\mathscr{P}(n)$ is represented by a unique normal Clifford circuit. Given an automorphism ϕ of $\mathscr{P}(n)$ one can construct a Z-circuit L and an X-circuit M such that $(ML)^{-1}$ acts as ϕ^{-1} on $I \otimes \cdots \otimes I \otimes Z$ and $I \otimes \cdots \otimes I \otimes X$. To obtain a normal form for ϕ it then suffices to first construct L and M and then to recursively proceed with the automorphism $\phi' = \phi(ML)^{-1}$. The proofs can be found in Appendix C.

Proposition 4.11. *Let P be a n-qubit Pauli operator, with $P = P_1 \otimes P_2 \otimes \cdots \otimes P_n$, $P^2 = I$, and $P \neq \pm I$. Then there exists a unique Z-circuit L such that $L \bullet P = Z \otimes I \otimes \cdots \otimes I$.*

Proposition 4.12. *Let Q be an n-qubit Pauli operator with $Q = Q_1 \otimes Q_2 \otimes \cdots \otimes Q_n$, $Q^2 = I$, $Q \neq \pm I$, and Q anticommutes with $Z \otimes I \otimes \cdots \otimes I$. Then there exists a unique X-circuit M such that $M \bullet Q = I \otimes \cdots \otimes I \otimes X$.*

Proposition 4.13. *Every X-circuit M satisfies $M \bullet (Z \otimes I \otimes \cdots \otimes I) = I \otimes \cdots \otimes I \otimes Z$.*

Proposition 4.14. *Let P and Q be Pauli operators such that $P^2 = Q^2 = I$, $P, Q \neq \pm I$, and P and Q anticommute. Then there exists a unique pair of a Z-circuit L and a X-circuit M such that $ML \bullet P = I \otimes \cdots \otimes I \otimes Z$ and $ML \bullet Q = I \otimes \cdots \otimes I \otimes X$.*

Proposition 4.15. *Let $\phi : \mathscr{P}(n) \to \mathscr{P}(n)$ be an automorphism of the Pauli group. Then there exists a normal circuit C such that for all P, $C \bullet P = \phi(P)$. Moreover, the normal form C is unique up to a scalar ± 1.*

By the existence part of Proposition 4.15, every automorphism of the Pauli group can be represented as a circuit over -1, H, Z, and CZ. Thus, all of these automorphisms are stabilizers. Conversely, as remarked in Section 2, every stabilizer is an automorphism of the Pauli group. Hence, Proposition 4.15 indeed establishes that every stabilizer admits a unique normal form. Note that this also proves that stabilizers are generated by -1, Z, H, and CZ.

By Proposition 4.15, there is a bijection between stabilizer operators and normal forms. We can therefore count the number of n-qubit normal forms to compute the cardinality of $\mathscr{C}(n)$.

Corollary 4.16. *There are exactly $2 \cdot \prod_{i=1}^{n} (4^i + 2^i - 2)(2 \cdot 4^{i-1})$ real stabilizer operators on n qubits.*

Proof. See Appendix D □

5 Relations for Real Stabilizer Circuits

We now introduce relations for real Clifford circuits and describe an algorithm for converting any n-qubit Clifford circuit to its normal form, using finitely many applications of the relations. To normalize circuits, it is sufficient to have relations to

1. rewrite the empty circuit into the normal form for the identity and
2. rewrite a circuit consisting of a single gate appearing on the left of a normal form into a normal form.

Indeed, one can then start with an arbitrary circuit, append the normal form for the identity to the right of it, and iteratively merge the gates of the initial circuit into the normal form on its right.

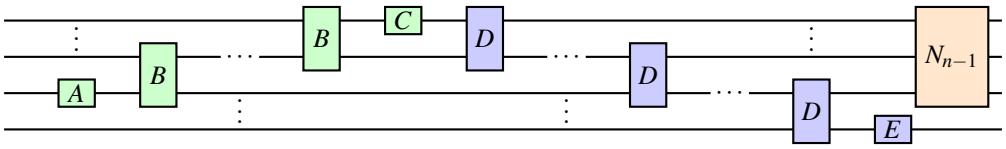
Definition 5.1. The *typed relations* for real stabilizers are given in Appendix B.

The typed relations describe all situations in which one of H, Z, CZ, X, or CXZ appears to the left of a normal form. Because these gates act on no more than two qubits, there are only finitely many cases to consider. The difficulty arises because the right-hand side of a relation may contain multiple gates. As a result, we are led to consider cases where a circuit appears on the left-hand side of a rule. This process increases the number of cases to consider and could, in principle, fail to terminate. However, a careful analysis shows that this is not the case. In total, 139 relations are contained in Appendix B.

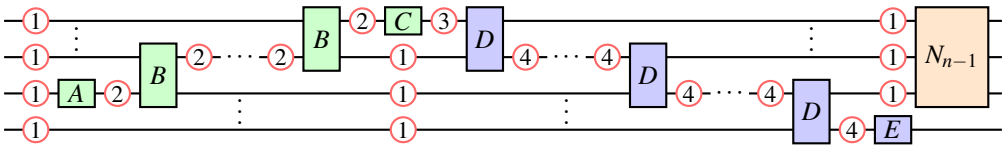
5.1 Normalization

We start by labelling normal circuits. This labelling is convenient to refer to specific parts of a circuit and will be useful to describe our rewrite system.

Definition 5.2. Consider an n-qubit normal circuit



where N_{n-1} is assumed to be a normal form on $(n-1)$ qubits. We assign labels to specific wires in order to produce a *labelled normal form*



where $N_{(n-1)}$ is recursively labelled in the same manner.

Definition 5.3. *Dirty normal forms* are obtained from normal forms by adding gates according to the following scheme.

- An H gate can be placed on a wire labelled 1 or on a double wire labelled 2.
- A Z gate can be placed on a wire labelled 1, 2, 3, or 4.
- An X gate can be placed on a wire labelled 1 or 2.
- A CZ gate can be placed on adjacent wires, provided that the bottom wire is labelled 1, and either the top wire is labelled 1 or 3 or the top wire is a double wire labelled 2.
- A CXZ gate can be placed on adjacent wires, provided that the bottom wire is labelled 1, and the top wire is a double wire labelled 2.

When discussing dirty normal forms, we call the H, Z, X, CZ, and CXZ gates *dirty*, while the gates of kind A, B, C, D, and E are called *clean*.

Intuitively, dirty normal forms are circuits "during the normalization process". We now explain how the relations can be used to transform dirty normal forms into clean ones.

Lemma 5.4. *Any dirty normal form can be converted to its normal form by applying the typed relations of Definition 5.1 a finite number of times.*

Proof. By Definition 5.3, every dirty gate occurs before a clean gate. Thus, if dirty gates remain in the circuit, a dirty gate must occur immediately before a clean one. The left-hand side of the typed relations of Definition 5.1 contain all cases of a dirty gate occurring immediately before a clean gate. Hence, as long as dirty gates remain, one of the rules can be applied. Moreover, each rule takes a dirty normal form to a dirty normal form. We now show that this procedure terminates in a finite number of steps. To this end, we associate a sequence of nonnegative integers numbers to each dirty normal form. Suppose a dirty normal form has t clean gates, indexed $1,\ldots,t$ left to right. Now define the sequence $s=(s_1,\ldots,s_t)$ where s_i is the number of dirty gates that occur before the i-th clean gate. A left-to-right application of

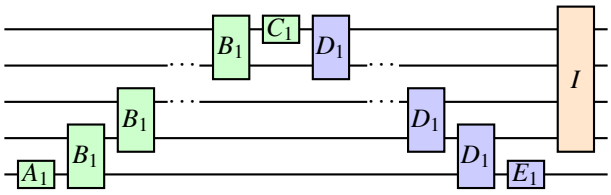
one of the typed relations decreases s lexicographically. The length of this sequence might not remain constant through the normalization process but it is bounded by the maximum possible number of clean gates in a circuit. For a normal form on n-qubits, this bound is given by

$$\sum_{i=1}^{n} 2i+1 = n^2+2n.$$

Hence, this process terminates in a finite number of rewrites. □

Proposition 5.5. *Any Clifford circuit can be rewritten into its normal form using the typed relations of Definition 5.1.*

Proof. The normal form of the identity operator on n qubits is



where I denotes the normal form for the identity on $n-1$ qubits. Using the typed relations of Definition 5.1, we can rewrite the empty circuit on n wires into the normal form for the identity. Now consider a Clifford circuit C. Expanding the wires on the right of C into the normal form for the identity, we obtain a dirty normal form. We can then convert this dirty normal form into a normal form using Lemma 5.4, which completes the proof. □

5.2 A Reduced Set of Relations

Propositions 4.15 and 5.5 jointly show that real stabilizers are presented by the generators (-1), H, Z, and CZ and the typed relations of Definition 5.1 (where each derived generator is replaced by its definition and types are forgotten). This presentation is highly redundant and, in this final section, we provide a reduced set of relations.

Definition 5.6. The *reduced relations* for real stabilizers are given in Figure 1.

Proposition 5.7. *Any Clifford circuit can be rewritten into its normal form using the reduced relations of Definition 5.6.*

Proof. It suffices to show that the reduced relations of Definition 5.6 imply the typed relations of Definition 5.1. The derivations can be found in the supplement to this paper [11]. □

An alternative set of reduced relations is given in Appendix A. This last collection of relations is stated in terms of the (-1), H, Z, CZ, X, and CX gates and is included because it makes for an arguably more intuitive presentation.

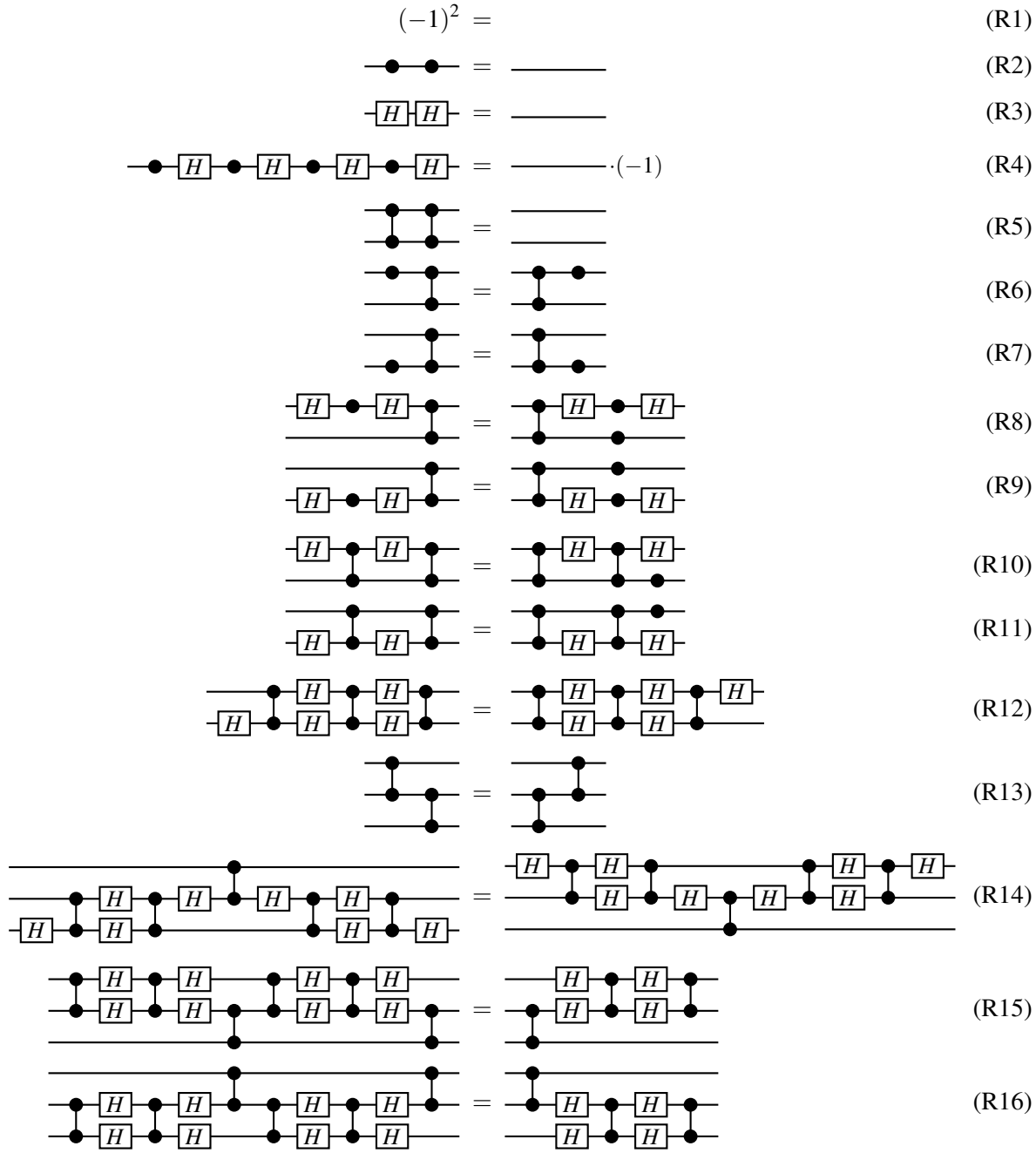


Figure 1: A set of reduced relations for real stabilizers.

6 Conclusion

In this paper, we defined a normal form for real stabilizer circuits, showed that every real stabilizer operator admits a unique normal form, and introduced a set of relations that suffices to rewrite any real stabilizer circuit into its normal form. This yields a presentation by generators and relations of real stabilizer operators. Our results add to the growing family of quantum operators for which such presentations are known (see [2, 15] for unitary quantum circuits and, for example, [4, 7, 17] in more general contexts). Our approach in this work followed that of [15]. However, we did not leverage the presentation given in [15] for complex stabilizers in any systematic way. We plan to explore this connection in future work, with the hope of devising more general methods for the construction of presentations such as the one provided here.

References

[1] Scott Aaronson & Daniel Gottesman (2004): *Improved simulation of stabilizer circuits*. Physical Review A 70, p. 052328, doi:10.1103/PhysRevA.70.052328. Also available from arXiv:quant-ph/0406196.

[2] Matthew Amy, Jianxin Chen & Neil J. Ross (2018): *A finite presentation of CNOT-dihedral operators*. In: Proceedings of the 14th International Conference on Quantum Physics and Logic, QPL 2017, Nijmegen, Electronic Proceedings in Theoretical Computer Science 266, pp. 84–97, doi:10.4204/EPTCS.266.5.

[3] Matthew Amy, Andrew N. Glaudell & Neil J. Ross (2020): *Number-theoretic characterizations of some restricted Clifford+T circuits*. Quantum 4, p. 252, doi:10.22331/q-2020-04-06-252. Also available from arXiv:1908.06076.

[4] Miriam Backens (2014): *The ZX-calculus is complete for stabilizer quantum mechanics*. New Journal of Physics 16(9), p. 093021, doi:10.1088/1367-2630/16/9/093021. Also available from arXiv:1307.7025.

[5] Miriam Backens & Aleks Kissinger (2019): *ZH: A complete graphical calculus for quantum computations involving classical non-linearity*. In: Proceedings of the 15th International Conference on Quantum Physics and Logic, QPL 2018, Halifax, Electronic Proceedings in Theoretical Computer Science 287, pp. 23–42, doi:10.4204/EPTCS.287.2.

[6] Sergey Bravyi & Dmitri Maslov (2021): *Hadamard-free circuits expose the structure of the Clifford group*. IEEE Transactions on Information Theory 67(7), pp. 4546–4563, doi:10.1109/TIT.2021.3081415. Also available from arXiv:2003.09412.

[7] Cole Comfort (2019): *Circuit relations for real stabilizers: Towards TOF+H*. Available from arXiv:1904.10614.

[8] Ross Duncan & Simon Perdrix (2014): *Pivoting makes the ZX-calculus complete for real stabilizers*. In: Proceedings of the 10th International Conference on Quantum Physics and Logic, QPL 2013, Electronic Proceedings in Theoretical Computer Science 171, pp. 50–62, doi:10.4204/EPTCS.171.5.

[9] Daniel Gottesman (1998): *The Heisenberg representation of quantum computers*. Available from arXiv:quant-ph/9807006.

[10] A. K. Hashagen, S. T. Flammia, D. Gross & J. J. Wallman (2018): *Real randomized benchmarking*. Quantum 2, p. 85, doi:10.22331/q-2018-08-22-85. Also available from arXiv:1801.06121.

[11] Justin Makary, Neil J. Ross & Peter Selinger (2021): *Supplement: Generators and relations for real stabilizer operators*. Available as an ancillary file from this paper's arXiv page.

[12] G. Nebe, E. M. Rains & N. J. A. Sloane (2001): *The invariants of the Clifford groups*. Designs, Codes and Cryptography 24, doi:10.1023/A:1011233615437. Also available from arXiv:math/0001038.

[13] Michael A. Nielsen & Isaac L. Chuang (2000): *Quantum Computation and Quantum Information*. Cambridge Series on Information and the Natural Sciences, Cambridge University Press, doi:10.1017/CBO9780511976667.

[14] Narayanan Rengaswamy, Robert Calderbank, Swanand Kadhe & Henry D. Pfister (2019): *Logical Clifford synthesis for stabilizer codes*. Available from arXiv:1907.00310.

[15] Peter Selinger (2015): *Generators and relations for n-qubit Clifford operators*. Logical Methods in Computer Science 11(10), pp. 1–17, doi:10.2168/LMCS-11(2:10)2015.

[16] Maarten Van Den Nest (2010): *Classical simulation of quantum computation, the Gottesman-Knill theorem, and slightly beyond*. Quantum Information & Computation 10(3), pp. 258–271, doi:10.26421/QIC10.3-4-6.

[17] Renaud Vilmart (2018): *A ZX-calculus with triangles for Toffoli-Hadamard, Clifford+T, and beyond*. In: Proceedings of the 15th International Conference on Quantum Physics and Logic, QPL 2018, Halifax, Electronic Proceedings in Theoretical Computer Science 287, pp. 313–344, doi:10.4204/EPTCS.287.18.

A An Alternative Reduced Set of Relations

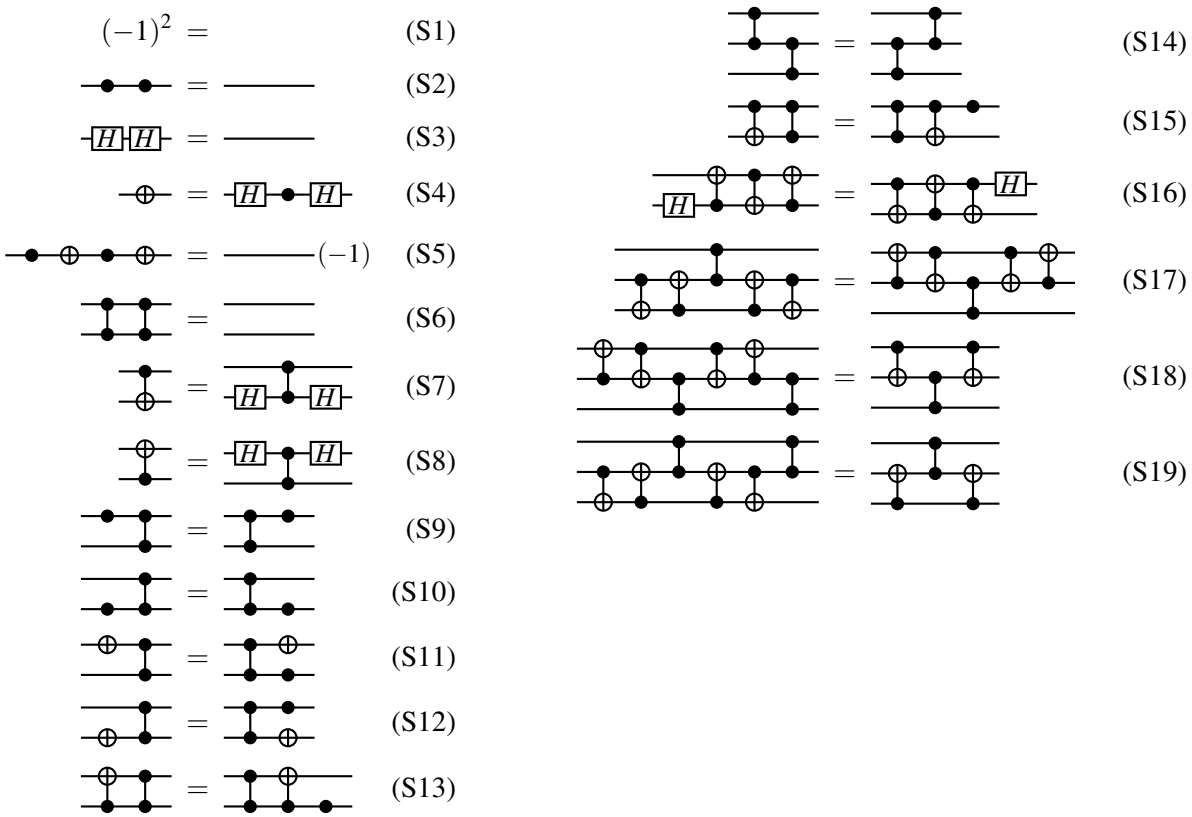


Figure 2: An alternative set of reduced relations for real stabilizers.

B Typed Relations

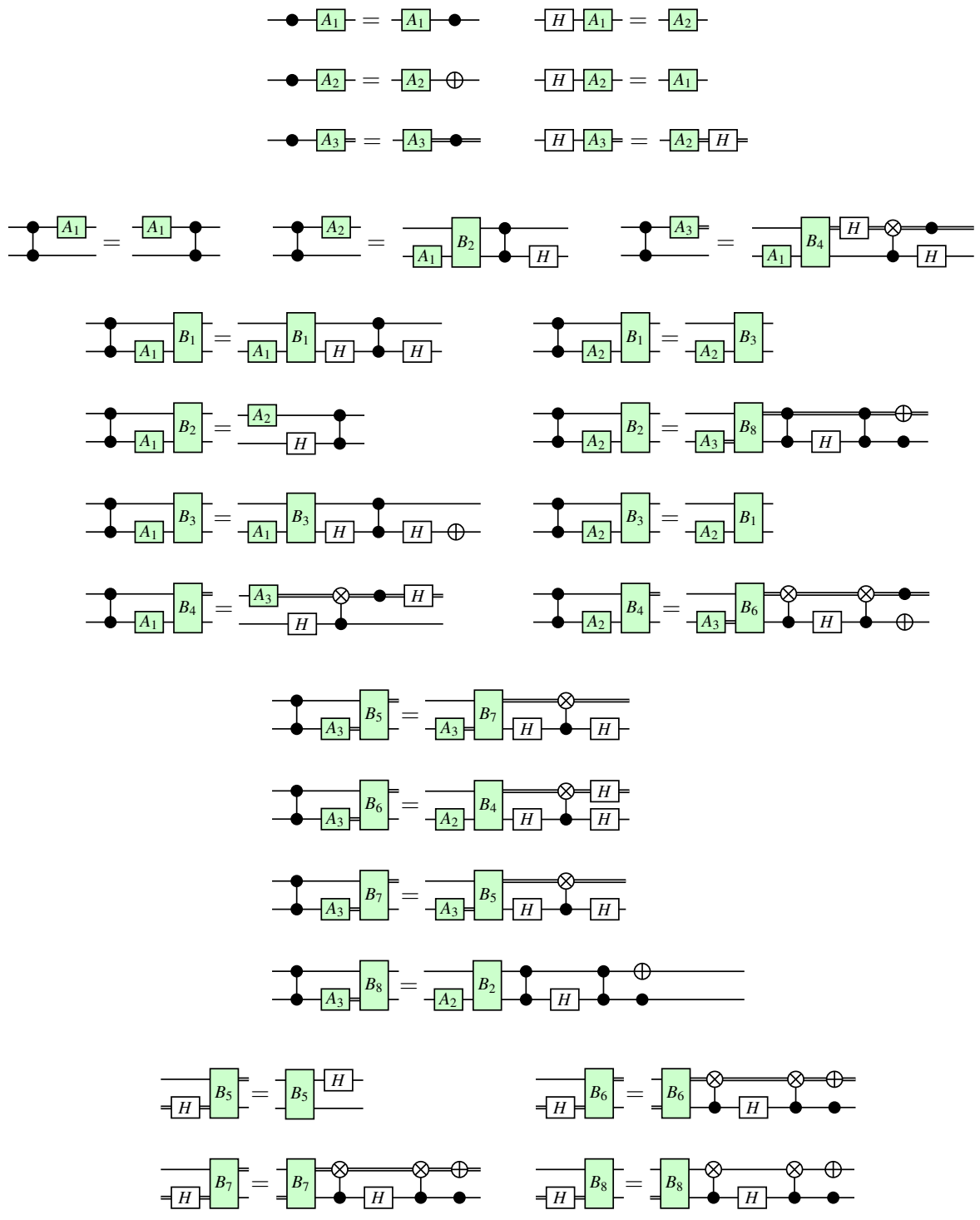


Figure 3: Rewrite rules for normal forms, part I.

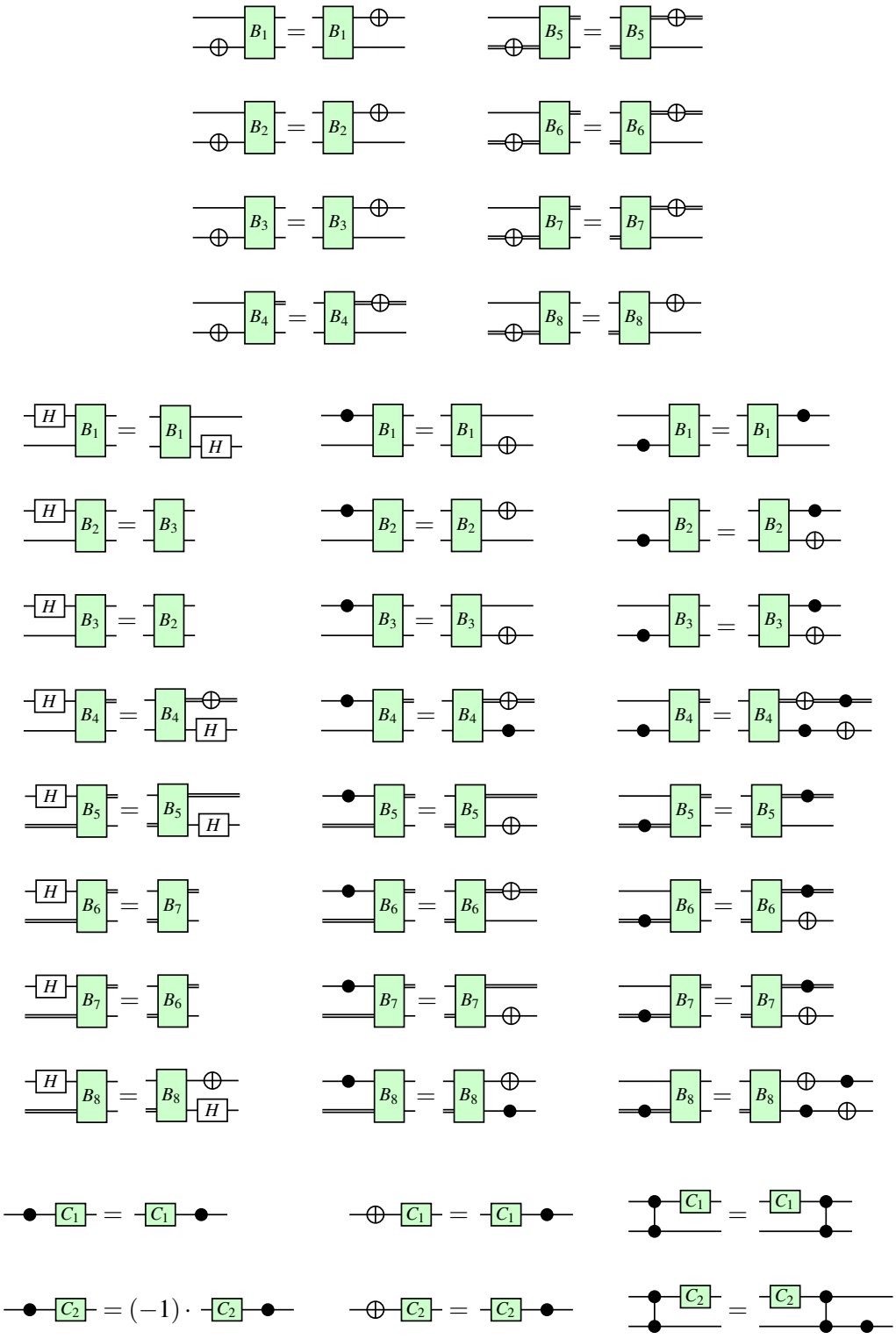


Figure 4: Rewrite rules for normal forms, part II.

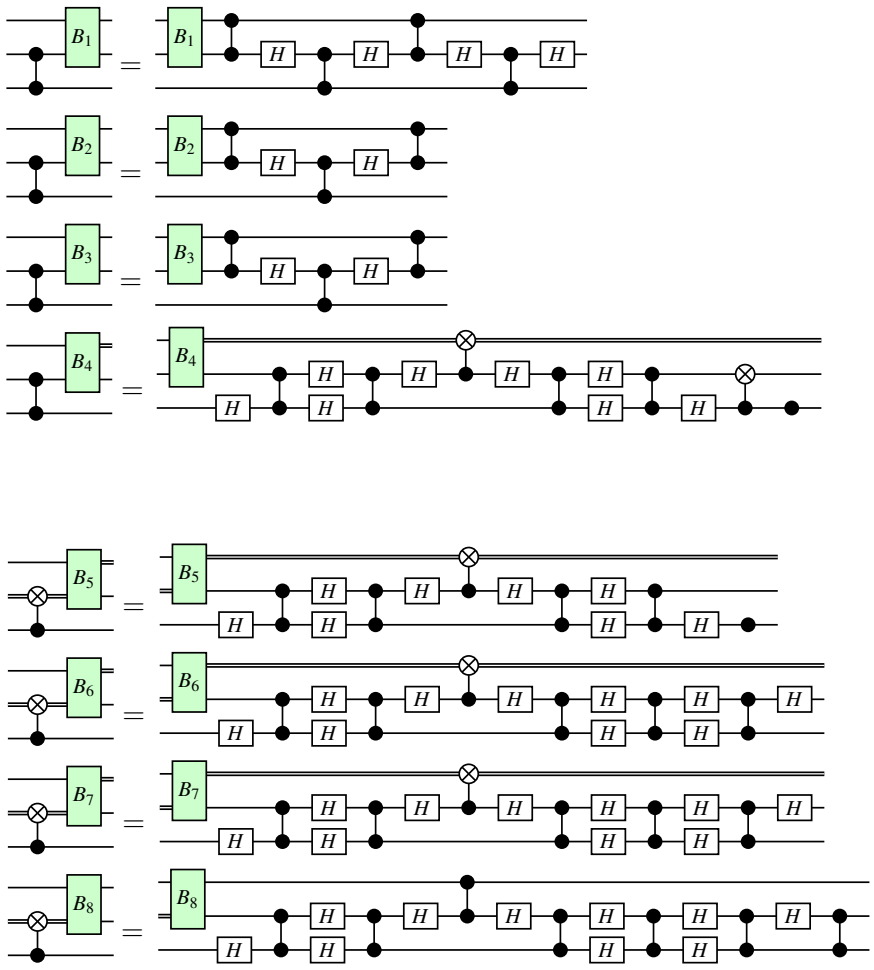


Figure 5: Rewrite rules for normal forms, part III.

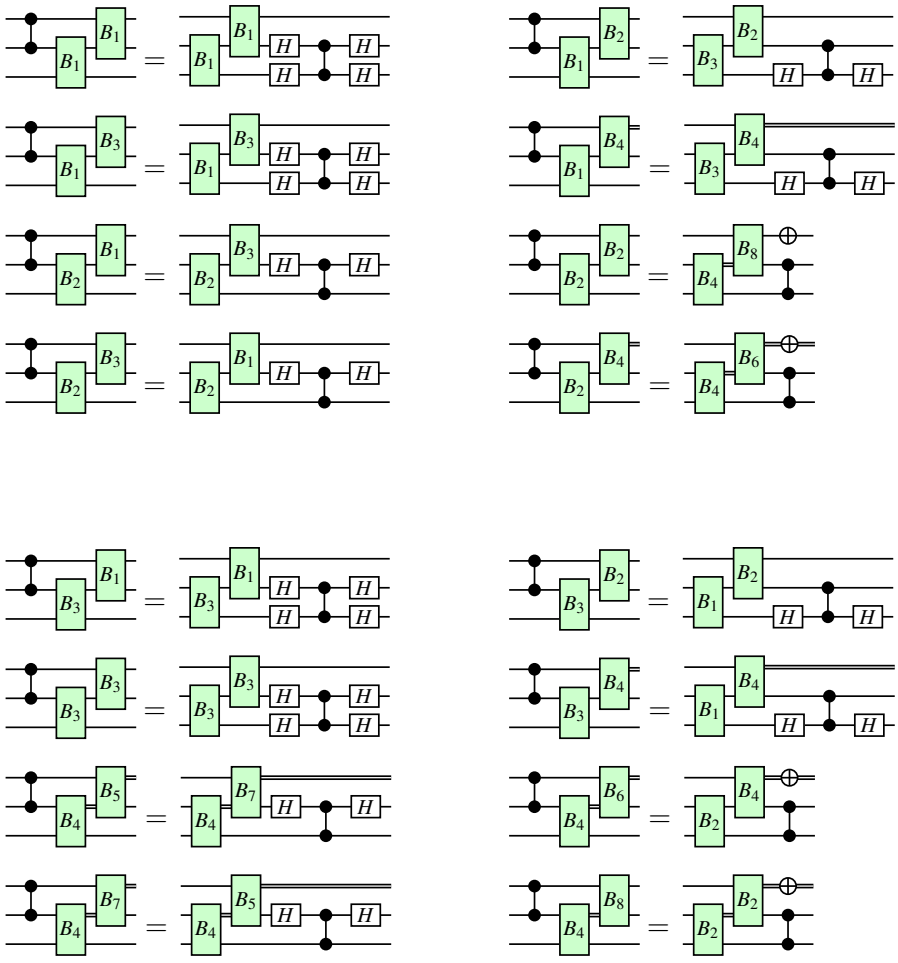


Figure 6: Rewrite rules for normal forms, part IV.

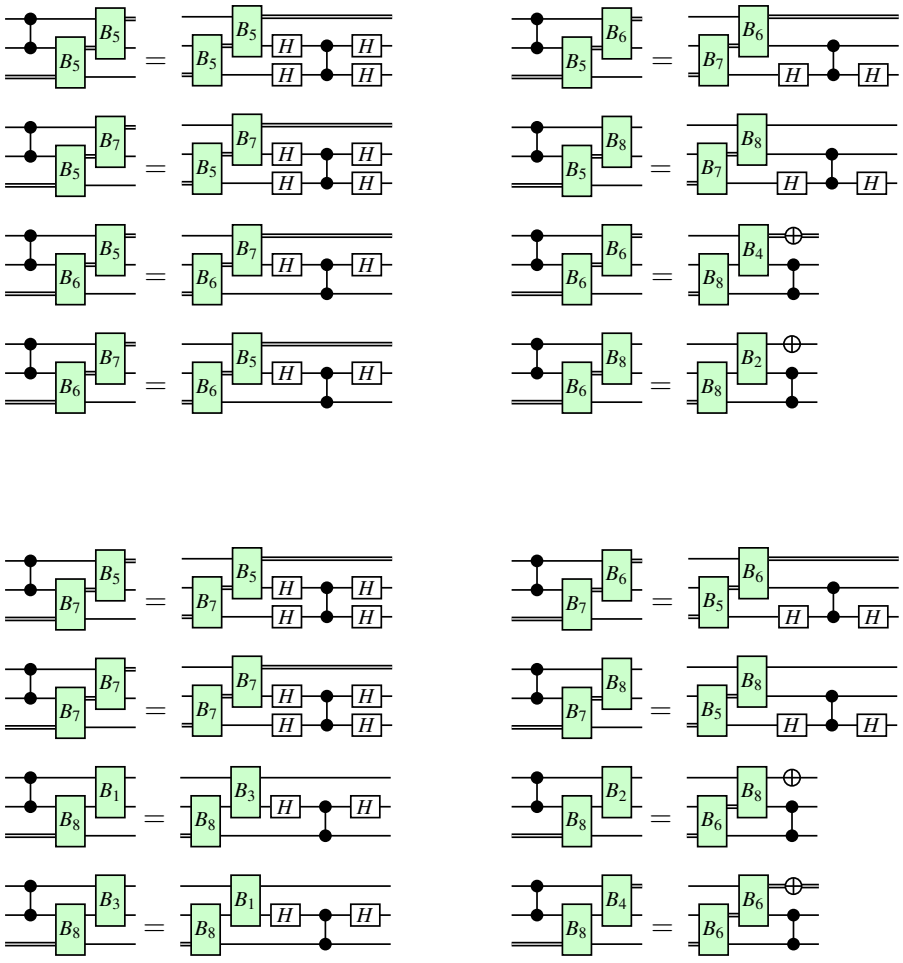


Figure 7: Rewrite rules for normal forms, part V.

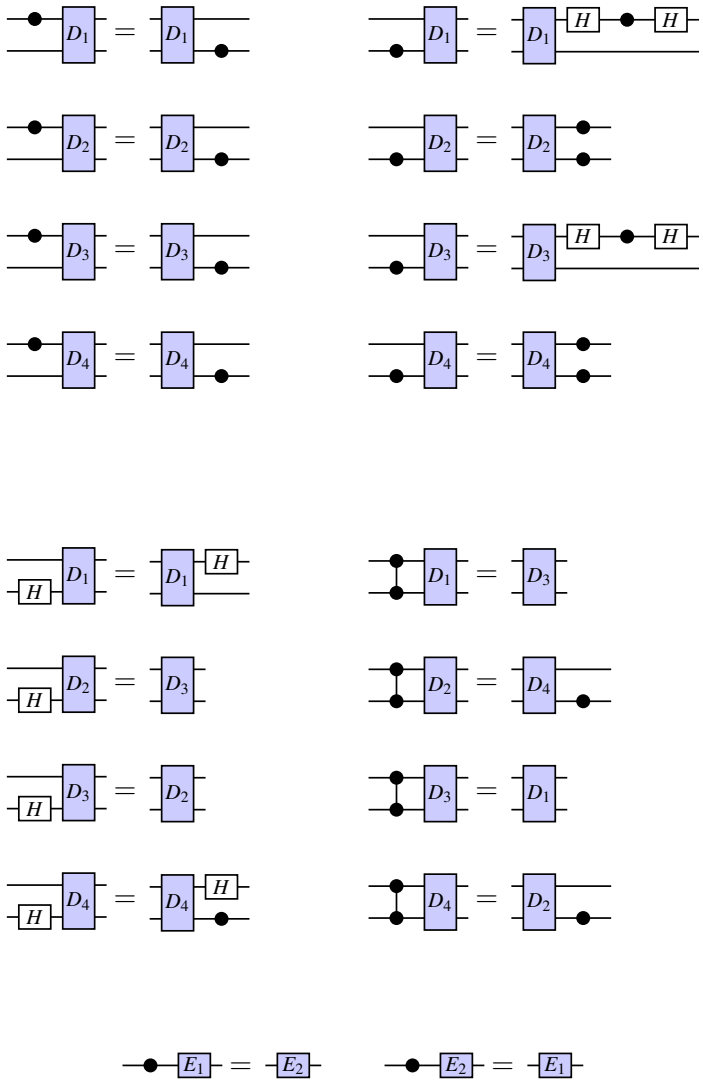


Figure 8: Rewrite rules for normal forms, part VI.

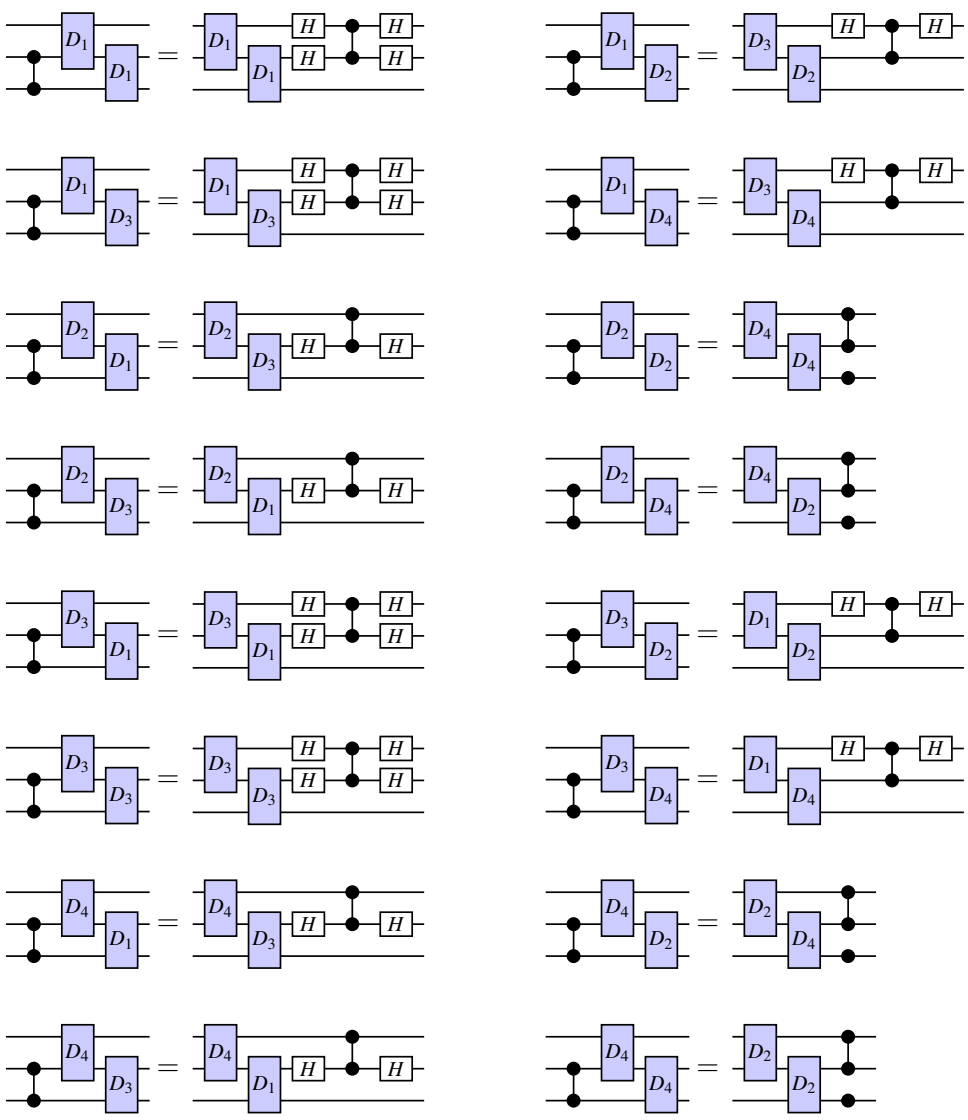


Figure 9: Rewrite rules for normal forms, part VII.

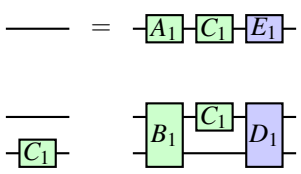
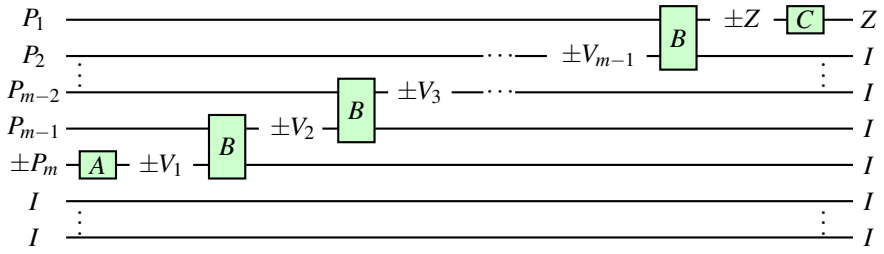


Figure 10: Rewrite rules for normal forms, part VIII.

C Proofs of Propositions 4.11, 4.12, 4.13, 4.14, and 4.15

Proposition 4.11 Let P be a n-qubit Pauli operator, with $P = P_1 \otimes P_2 \otimes \cdots \otimes P_n$, $P^2 = I$, and $P \neq \pm I$. Then there exists a unique Z-circuit L such that $L \bullet P = Z \otimes I \otimes \cdots \otimes I$.

Proof. Since $P \neq \pm I$, there is an index m such that $P_m \neq \pm I$. Let m be the largest such index. Then $P_m = \pm X, P_m = \pm Z$, or $P_m = \pm XZ$. With this, we consider the following diagram.



In the above diagram, the V_s are Pauli operators such that $V_s \in \{Z, XZ\}$ and are determined in the following way. By Proposition 4.7, if $P_m = \pm X, \pm Z$, there is a unique A gate A_g with output of single type such that $A_g \bullet P_m = \pm Z$. If $P_m = \pm XZ$, there is a unique A gate A_r with output of double type such that $A_r \bullet P_m = \pm XZ$. So the A gate is uniquely determined. Furthermore after the application of the A gate, we either have $V_1 = \pm XZ$ on a wire of double type or $V_1 = \pm Z$ on a wire of single type. We will further use the actions in Proposition 4.7 to move these Z or XZ Pauli operators up the qubits.

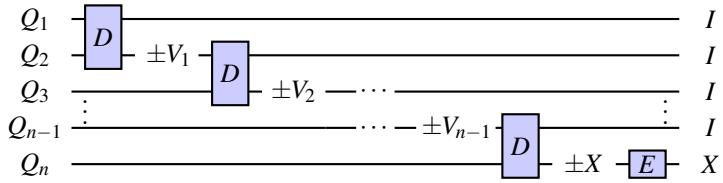
By inspection of these actions, we see that for each choice of $P_{m-1} \otimes V_1$, there is a unique B gate B_j such that $B_j \bullet P_{m-1} \otimes V_1 = V_2 \otimes I$ and $V_2 = Z$ or $V_2 = XZ$. If $V_2 = Z$, the output wire is of single type, and if $V_2 = XZ$, the output wire is of double type. We can continue this process up to the top qubit and this will produce a Z-circuit if we can ensure that the top output wire is of single type. Since $P^2 = I$, there are evenly many indices i such that $P_i = XZ$, which are in effect cancelled out by an application of B_8, switching back to Z along a wire of single type. Thus we will always end up constructing a circuit C such that $C \bullet P = \pm Z \otimes I \otimes \ldots \otimes I$, to which there is a unique C-gate C_k such that $C_k \bullet \pm Z = Z$. This completes the proof of existence.

Note that every choice of gate is unique with respect to kind and type. If our normal form was constructed the same way in the absence of types, uniqueness with respect to kind would be sufficient for a unique Z-circuit. Here, with uniqueness with respect to kind and type, we must prove that no two Z-circuits describing an action as above can have different typing schemes. Consider two Z-circuits C and D that correspond to the diagram above, such that $C \bullet P = D \bullet P = Z \otimes I \otimes \ldots \otimes I$. We now show that they have the same typing schemes. Note that both A gates in C and D must satisfy $A \bullet P_m = \pm V_1$, where $V_1 = \pm Z, \pm XZ$. A_2 is the only A gate such that $A \bullet \pm X = \pm Z$, and the equations $A \bullet \pm Z = \pm Z$ and $A \bullet XZ = \pm XZ$ both have two A gates with these properties, A_1 and A_3. Both of these gates are different with respect to output type, but represent the same actions. When an A_1 is chosen as the A gate, there is an even number of gates from the set $\{B_4, B_8\}$ which appear to its right, as these B gates switch the type up the ladder. If A_3 is chosen as the A gate, then there is an odd number of gates from the set $\{B_4, B_8\}$ which appear to its right. Thus it is not possible for both circuits C and D to start with the different A gates A_1 and A_3 respectively, as it is not possible for both resulting circuits to have $C \bullet P = D \bullet P = Z \otimes I \ldots \otimes I$ with a different number of occurrences of a given local action. Hence, C and D share the same A gate, and have the same starting type. Note that if the input type is given, there are four choices of possible local actions of $B \bullet P_{m-j} \otimes V_j = V_{j+1} \otimes I$, corresponding to B_1, B_2, B_3, B_4 in the case of a single type, and

B_5, B_6, B_7, B_8 in the case of a double type. Since the output type of A is given, and we must satisfy the equations $B \bullet P_{m-j} \otimes V_j = V_{j+1} \otimes I$, there are four choices for four possibilities at each choice of B, which all describe different actions. Here we see that with a shared A gate, both Z-circuits C and D must also have the same B gates, and thus the same typing scheme, ending in a single type, with the corresponding unique choice of a C gate such that $C \bullet \pm Z = Z$. Hence we have that C and D have the same typing scheme. Since the typing schemes must be the same, all local actions must coincide. Hence the two Z-circuits are equal. This proves uniqueness. □

Proposition 4.12 Let Q be an n-qubit Pauli operator with $Q = Q_1 \otimes Q_2 \otimes \cdots \otimes Q_n$, $Q^2 = I$, $Q \neq \pm I$, and Q anticommutes with $Z \otimes I \otimes \cdots \otimes I$. Then there exists a unique X-circuit M such that $M \bullet Q = I \otimes \cdots \otimes I \otimes X$.

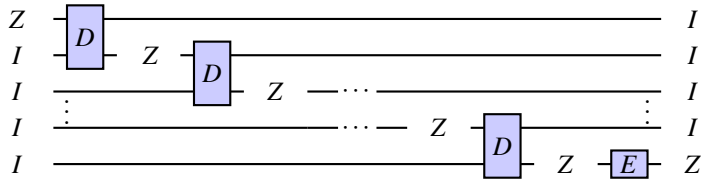
Proof. Since Q anticommutes with $Z \otimes I \otimes \cdots \otimes I$, we have $Q_1 = \pm XZ$ or $Q_1 = \pm X$. With this, consider the diagram



where the V_s are Pauli operators such that $V_s \in \{X, XZ\}$, and are determined by the Q_i as in **Proposition 4.11**. By **Proposition 4.7**, the D gates push X and XZ gates down the qubits until we encounter $XZ \otimes XZ$, at which point we apply D_4. There is always a unique D gate to perform the needed action, leaving $V_1 = X, XZ$. We continue the same process down to the bottom qubit. Again since $Q^2 = I$, by **Proposition 2.2**, there are evenly many indices t such that $Q_t = XZ$. These occurrences of XZ get cancelled out in pairs, ensuring that we are left with an $\pm X$ on the bottom qubit. By **Proposition 4.7**, there is a unique E gate E_h such that $E_h \bullet \pm X = X$. Thus we are left with $I \otimes \cdots \otimes I \otimes X$ and our circuit is an X-circuit. Furthermore, since each gate was unique with respect to kind, the circuit is uniquely determined. □

Proposition 4.13 Every X-circuit M satisfies $M \bullet (Z \otimes I \otimes \cdots \otimes I) = I \otimes \cdots \otimes I \otimes Z$.

Proof. The claim follows from the actions described in **Proposition 4.7** with respect to the diagram below.



□

Proposition 4.14 Let P and Q be Pauli operators such that $P^2 = Q^2 = I$, $P, Q \neq \pm I$, and P and Q anticommute. Then there exists a unique pair of a Z-circuit L and a X-circuit M such that

$$ML \bullet P = I \otimes \cdots \otimes I \otimes Z \qquad \textit{and} \qquad ML \bullet Q = I \otimes \cdots \otimes I \otimes X$$

Proof. By **Proposition 4.11**, there is a unique Z-circuit L such that $L \bullet P = Z \otimes I \otimes \cdots \otimes I$. Since P and Q both square to the identity and anticommute, so do $L \bullet P$ and $L \bullet Q$. Thus by **Proposition 4.12**, there exists a unique X-circuit M such that $M \bullet (L \bullet Q) = ML \bullet Q = I \otimes I \otimes \cdots \otimes X$ and, by **Proposition 4.13**,

$ML \bullet P = M \bullet (L \bullet P) = M \bullet (Z \otimes I \otimes \cdots \otimes I) = I \otimes I \otimes \cdots \otimes Z$. This proves existence. For uniqueness, we assume that L' and M' are two other circuits satisfying the conditions of the proposition. Since $M'L' \bullet P = I \otimes \cdots \otimes I \otimes Z$, and $M' \bullet (Z \otimes I \otimes \cdots \otimes I) = I \otimes \cdots \otimes I \otimes Z$, we can deduce that $L' \bullet P = Z \otimes I \otimes \cdots \otimes I$. Therefore $L' = L$ by the uniqueness of **Proposition 4.11**, and since $M' \bullet L \bullet Q = M \bullet L \bullet Q = X \otimes I \otimes \cdots \otimes I$, we have that $M' = M$ by the uniqueness of **Proposition 4.12**. □

Proposition 4.15 Let $\phi : \mathscr{P}(n) \to \mathscr{P}(n)$ be an automorphism of the Pauli group. Then there exists a normal circuit C such that for all P, $C \bullet P = \phi(P)$. Moreover, the normal form C is unique up to a scalar ± 1.

Proof. We proceed by induction on n. When $n = 0$, the Pauli operators are the scalars ± 1. Thus in this case ϕ is the identity. Choosing $C = 1$, we get $C \bullet P = \phi(P)$. Uniqueness up to scalar follows from the fact that when $n = 0$, the Clifford operators are the scalars ± 1. Now suppose that our claim is true for $n-1$ and consider the case of n. First we will prove existence. Let $P = \phi^{-1}(I \otimes \ldots \otimes I \otimes Z)$ and $Q = \phi^{-1}(I \otimes \ldots \otimes I \otimes X)$. Then $PQ = \phi^{-1}(I \otimes \ldots \otimes I \otimes ZX)$. Since $I \otimes \ldots \otimes I \otimes Z$ and $I \otimes \ldots \otimes I \otimes X$ anticommute, so do P and Q. By**Proposition 4.14**, there exists a unique X-circuit M and a unique Z-circuit L such that $ML \bullet P = I \otimes \ldots \otimes I \otimes Z = \phi(P)$ and $ML \bullet Q = I \otimes \ldots \otimes I \otimes X = \phi(Q)$. We now define a new automorphism $\phi' : \mathscr{P}(n) \to \mathscr{P}(n)$ by

$$\phi'(U) = \phi((ML)^{-1} \bullet U)$$

for all n-qubit Pauli operators U. Note that $I \otimes \cdots \otimes I \otimes Z$, $I \otimes \cdots \otimes I \otimes X$ and $I \otimes \cdots \otimes I \otimes ZX$ are all fixed points of ϕ', since

$$\begin{aligned}\phi'(I \otimes \cdots \otimes I \otimes Z) &= \phi((ML)^{-1} \bullet (I \otimes \cdots \otimes I \otimes Z) \\ &= \phi((ML)^{-1} \bullet (ML) \bullet P) = \phi(P) = I \otimes \cdots \otimes I \otimes Z\end{aligned}$$

and similarly for $I \otimes \cdots \otimes I \otimes X$. Now let R be an $(n-1)$-qubit Pauli operator. Since $R \otimes I$ commutes with $I \otimes \cdots \otimes I \otimes Z$ and $I \otimes \cdots \otimes I \otimes X$, the same is true of $\phi'(R \otimes I)$. Hence $\phi'(R \otimes I) = V \otimes I$ for some $V \in \mathscr{P}(n-1)$. It follows that there exists an automorphism $\phi'' : \mathscr{P}(n-1) \to \mathscr{P}(n-1)$ such that, for every $R \in \mathscr{P}(n-1)$, $\phi'(R \otimes I) = \phi''(R) \otimes I$. Since $I \otimes \cdots \otimes I \otimes Z$ and $I \otimes \cdots \otimes I \otimes X$ are fixed points of ϕ', we then have $\phi' = \phi'' \otimes I$.

By the induction hypothesis, there exists a normal $n-1$ qubit Clifford circuit C' such that for all $R \in \mathscr{P}(n-1)$, $C' \bullet R = \phi''(R)$. Let $C = (C' \otimes I)ML$. Since $ML \bullet U = (\phi')^{-1}(\phi(U))$, we see that

$$C \bullet U = (C' \otimes I)ML \bullet U = (C' \otimes I) \bullet ((\phi')^{-1}(\phi(U)) = (C' \otimes I) \bullet ((\phi'')^{-1} \otimes I)(\phi(U)) = \phi(U)$$

This proves existence.

To prove uniqueness, suppose that D is another Clifford circuit in normal form such that $D \bullet U = \phi(U)$ for all $U \in \mathscr{P}(n)$. By the definition of normal form, $D = (D' \otimes I)M'L'$ where M' is an X-circuit, L' is a Z-circuit, and D' is a normal Clifford circuit on $n-1$ qubits. Since $(D' \otimes I)M'L' \bullet P = D \bullet P = \phi(P) = I \otimes \cdots \otimes I \otimes Z$, we have

$$M'L' \bullet P = (D' \otimes I)^{-1}(I \otimes \cdots \otimes I \otimes Z) = I \otimes \cdots \otimes I \otimes Z.$$

From the uniqueness of **Proposition 4.14**, $M' = M$ and $L' = L$. Then, by the induction hypothesis, C' and D' are equal up to a scalar of ± 1. Thus the same is true of C and D. This proves uniqueness. □

D Proof of Corollary 4.16

Corollary 4.16 There are exactly $2 \cdot \prod_{i=1}^{n} (4^i + 2^i - 2)(2 \cdot 4^{i-1})$ real stabilizer operators on n qubits.

Proof. First note that by **Definition 4.8**, the A gate on the left of a normal form will determine the input type of the first possible B gate. Then the choice of each B gate is dependent of the output type of the previous gate.

There are four gates with a single input type, B_1, B_2, B_3, and B_4, and four gates with a double input type, B_5, B_6, B_7, and B_8. The gates B_1, B_2, B_3, B_5, B_6, and B_7 have the output type of the top wire matching that of the input type of the bottom wire. The gates B_4 and B_8 on the other hand, swap between double and single types. Thus, if the last chosen gate had a single output wire type, then we must choose one of B_1, B_2, B_3, or B_4. Similarly, one of B_5, B_6, B_7, or B_8 must be chosen if the previous gate had a double output wire type.

Now to end with a circuit that is normal, the top output wire of the last B gate must be green. This means that if we start with an A_1 gate or an A_2 gate, then we start on a green wire and we must choose evenly many type-swapping gates (B_4 and B_8) in our construction. Moreover, the first one of which must be a B_4 gate and the last one of which must be a B_8. If we start with an A_3 gate, then we start on a double wire type and we must choose oddly many type-swapping gates, the first one of which must be a B_8 gate, and the last one of which must be a B_4 gate.

In general, the number of Z-circuits starting with an A_1 gate or an A_2 gate is exactly

$$4 \cdot \sum_{m=1}^{n} \sum_{k=0}^{\lfloor \frac{m-1}{2} \rfloor} \binom{m-1}{2k} 3^{m-2k-1} = \sum_{m=1}^{n} 2^{m-1}(2^m + 2)$$

and the number of Z-circuits that starting with an A_3 gate is exactly

$$2 \cdot \sum_{m=1}^{n} \sum_{k=0}^{\lfloor \frac{m-1}{2} \rfloor} \binom{m-1}{2k+1} 3^{m-2(k+1)} = \sum_{m=1}^{n} 2^{m-2}(2^m - 2).$$

This produces a total of

$$\sum_{m=1}^{n} 2^{m-1}(2^m + 2) + \sum_{m=1}^{n} 2^{m-2}(2^m - 2) = \sum_{m=1}^{n} (2^{m-1}(2^m + 2) + 2^{m-2}(2^m - 2)) = 4^n + 2^n - 2$$

Z-circuits. By **Definition 4.9**, there are exactly $2 \cdot 4^{n-1}$ X-circuits on n qubits. Since there are exactly 2 scalars, by **Definition 4.10**, there are exactly

$$2 \cdot \prod_{i=1}^{n} (4^i + 2^i - 2)(2 \cdot 4^{i-1})$$

normal circuits. By Proposition 4.15, these are in bijection with the elements of the n-qubit Clifford group. □