Logical Methods in Computer Science
Vol. 11(2:10)2015, pp. 1–17
www.lmcs-online.org

Submitted Nov. 9, 2013
Published Jun. 19, 2015

GENERATORS AND RELATIONS FOR n-QUBIT CLIFFORD OPERATORS

PETER SELINGER

Department of Mathematics and Statistics, Dalhousie University
e-mail address: selinger@mathstat.dal.ca

Abstract. We define a normal form for Clifford circuits, and we prove that every Clifford operator has a unique normal form. Moreover, we present a rewrite system by which any Clifford circuit can be reduced to normal form. This yields a presentation of Clifford operators in terms of generators and relations.

1. Introduction

In quantum computation, an important subclass of quantum circuits is the class of *Clifford circuits* or *stabilizer circuits*. It is the smallest class of quantum circuits that includes the gates

$$\omega = e^{i\pi/4}, \quad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad Z_c = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \tag{1.1}$$

identities, and closed under the operations of tensor product and composition. It is well-known that Clifford circuits can be efficiently simulated on a classical computer, and therefore they are not universal for quantum computing [4]. On the other hand, Clifford gates are transversal in many quantum error-correcting codes, and therefore they are particularly easy to implement fault-tolerantly. For this reason, universal gate bases for fault-tolerant quantum computation are often chosen to consist of the Clifford operators and one additional gate, for example the $\pi/8$-gate [2].

For all $n \geqslant 0$, the set of Clifford operators on n qubits forms a group, known as the *Clifford group* on n qubits, which we denote $\mathcal{C}(n)$. It is well-known (and we will prove below) that the Clifford group on n qubits is finite and has

$$|\mathcal{C}(n)| = 8 \cdot \prod_{i=1}^{n} 2(4^i - 1)4^i$$

2012 ACM CCS: [**Theory of computation**]: Models of computation—Quantum computation theory.
Key words and phrases: Stabilizer circuits, Clifford circuits, generators and relations.
Research supported by NSERC.

elements; for example, the sizes for $n = 1$, 2, and 3 are, respectively:

$$|\mathcal{C}(1)| = 192, \quad |\mathcal{C}(2)| = 92160, \quad |\mathcal{C}(3)| = 743178240.$$

In this paper, we define a normal form for Clifford circuits, and we prove that every Clifford operator has a unique normal form. Moreover, we present a rewrite system by which any Clifford circuit can be reduced to normal form. This yields a presentation of Clifford operators in terms of generators and relations, shown in Figure 8.

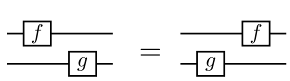
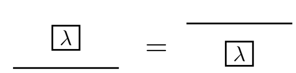
Related work. Van den Nest [9] gave a "normal" form for Clifford circuits, showing that every Clifford circuit can be written as a single layer of Hadamard gates, sandwiched between two circuits consisting only of gates that preserve the computational basis (X, S, controlled-X, and controlled-Z gates). Since it is evident that such circuits can be efficiently simulated on a classical computer, this yields a direct proof of the Gottesman-Knill theorem [4] without relying on the stabilizer formalism. However, Van den Nest's normal forms are not at all unique, and therefore cannot be used to derive an equational presentation of Clifford operators.

Backens [1] showed completeness of the ZX-calculus, a graphical language (given by generators and relations) that generalizes quantum circuits and includes Clifford circuits as a proper subset. While this work is closely related, it does not yield a direct equational presentation of Clifford operators. This is because expressions of the ZX-calculus can denote general linear maps, and not just unitary ones.

2. Generators and relations

Before continuing, it may be worthwhile to clarify what we mean by "generators and relations". We do not mean this in the sense of the usual *word problems* studied in group theory, but in the sense of *two-dimensional word problems* appropriate for quantum circuits. The use of higher-dimensional systems of generators and relations was pioneered by Burroni [3], and was used, for example, by Lafont to axiomatize various classes of boolean circuits [5].

In a nutshell, higher-dimensional word problems are a generalization of word problems where one regards not only composition, but also tensor product as a basic structural operation. We already mentioned that the Clifford operators form a family of groups $\mathcal{C}(0)$, $\mathcal{C}(1)$, $\mathcal{C}(2)$, etc. This family is equipped with the additional structure of a *strict spatial monoidal groupoid* (see [6, 7]). The abstract definition of strict spatial monoidal groupoids is not of great importance here; for our purposes, it simply means the following: the Clifford operators are equipped with an associative tensor product $\otimes : \mathcal{C}(n) \times \mathcal{C}(m) \to \mathcal{C}(n+m)$, such that the identity group element of $\mathcal{C}(0)$ also serves as the left and right unit for tensor, and satisfying the *bifunctorial law* $(f \otimes I_m) \circ (I_n \otimes g) = (I_n \otimes g) \circ (f \otimes I_m)$ and the *spatial law* $\lambda \otimes I_n = I_n \otimes \lambda$, where $f \in \mathcal{C}(n)$, $g \in \mathcal{C}(m)$, $\lambda \in \mathcal{C}(0)$, and I_n, I_m are the identity elements of $\mathcal{C}(n)$ and $\mathcal{C}(m)$, respectively. (From now on, we omit the subscript, writing I for the identity matrix of any size, and in fact for the identity element of any group). In circuit notation:

Bifunctorial law:  ; Spatial law:  .

Thus, the notion of a strict spatial monoidal groupoid already has the notion of the tensor product "built in", along with the fact that operators on disjoint sets of qubits commute with each other, and that scalars commute with everything.

Consequently, when we give generators and relations for Clifford operators *as a strict spatial monoidal groupoid*, the bifunctorial and spatial laws do not need to appear explicitly as part of the axiomatization. Moreover, unlike group theoretic axiomatizations, we only need one generator per basic gate, and not one generator per basic gate per qubit.

As a further illustration of this concept, consider the usual axiomatization of the braid group $\mathcal{B}(n)$ on n strands. If this is axiomatized as a group, one requires $n-1$ generators $\sigma_1, \ldots, \sigma_{n-1}$ (provided that $n \geqslant 2$), as well as $n-2$ instances of the Yang-Baxter equation $\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$ (provided that $n \geqslant 3$), and $(n-2)(n-3)/2$ instances of commutativity $\sigma_i \sigma j = \sigma_j \sigma_i$ where $j \geqslant i+2$ (provided that $n \geqslant 4$). On the other hand, the axiomatization in terms of strict spatial monoidal groupoid requires only one generator $\sigma \in \mathcal{B}(2)$ and one equation $(\sigma \times I)(I \times \sigma)(\sigma \times I) = (I \times \sigma)(\sigma \times I)(I \times \sigma)$, where $I \in \mathcal{B}(1)$ is the group identity.

3. Action of the Clifford group on the Pauli group

Let X, Y, and Z be the usual Pauli operators

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{3.1}$$

The *Pauli group on n qubits* consists of $2^n \times 2^n$-matrices of the form $\lambda P_1 \otimes \ldots \otimes P_n$, where $\lambda \in \{\pm 1, \pm i\}$ and $P_1, \ldots, P_n \in \{I, X, Y, Z\}$. We write $\mathcal{P}(n)$ for the Pauli group on n qubits.

We say that an n-qubit operator U is a *scalar* if it is a scalar multiple of the identity operator, i.e., $U = \lambda I$. In this case, we also write $U = \lambda$ by a mild abuse of notation.

It is well-known that the Clifford group acts on the Pauli group by conjugation: whenever $C \in \mathcal{C}(n)$ is a Clifford operator and $P \in \mathcal{P}(n)$ is a Pauli operator, then $C \bullet P := CPC^{-1} \in \mathcal{P}(n)$ is another Pauli operator. Moreover, because $C \bullet (PQ) = (C \bullet P)(C \bullet Q)$, the action of any fixed Clifford operator C on $\mathcal{P}(n)$ is a group automorphism of $\mathcal{P}(n)$. Also, since $C \bullet \lambda = \lambda$, this automorphism fixes scalars. We will show in Proposition 5.5 below that, conversely, any such group automorphism arises from the action of some Clifford operator. We have the following well-known properties:

Proposition 3.1. *Let $C \in \mathcal{C}(n)$. If $C \bullet P = P$ for all $P \in \mathcal{P}(n)$, then C is a scalar.*

Proof. First note that every complex 2×2-matrix can be written in the form $aI + bX + cY + dZ$, for complex scalars a, b, c, d. It follows that the set of Pauli operators spans the set of $2^n \times 2^n$-operators as a vector space. By assumption, $CPC^{-1} = P$ for all Pauli operators P. It follows that $CMC^{-1} = M$, hence $CM = MC$, for all operators M. This implies that C is a scalar. □

Corollary 3.2. *If C, D are two Clifford operators that act identically on the Pauli group, then C, D differ only by a global phase, i.e., $C = \omega^i D$ for some i.*

Proof. By Proposition 3.1, applied to $D^{-1}C$. □

Proposition 3.3. *Let $\varphi : \mathcal{P}(n) \to \mathcal{P}(n)$ be an automorphism of the Pauli group that fixes scalars. Then there exists some Clifford operator $C \in \mathcal{C}(n)$ (necessarily unique up to a phase by Corollary 3.2) such that for all P, $C \bullet P = \varphi(P)$.*

Proposition 3.3 is an immediate consequence of Proposition 5.5, which we will prove below.

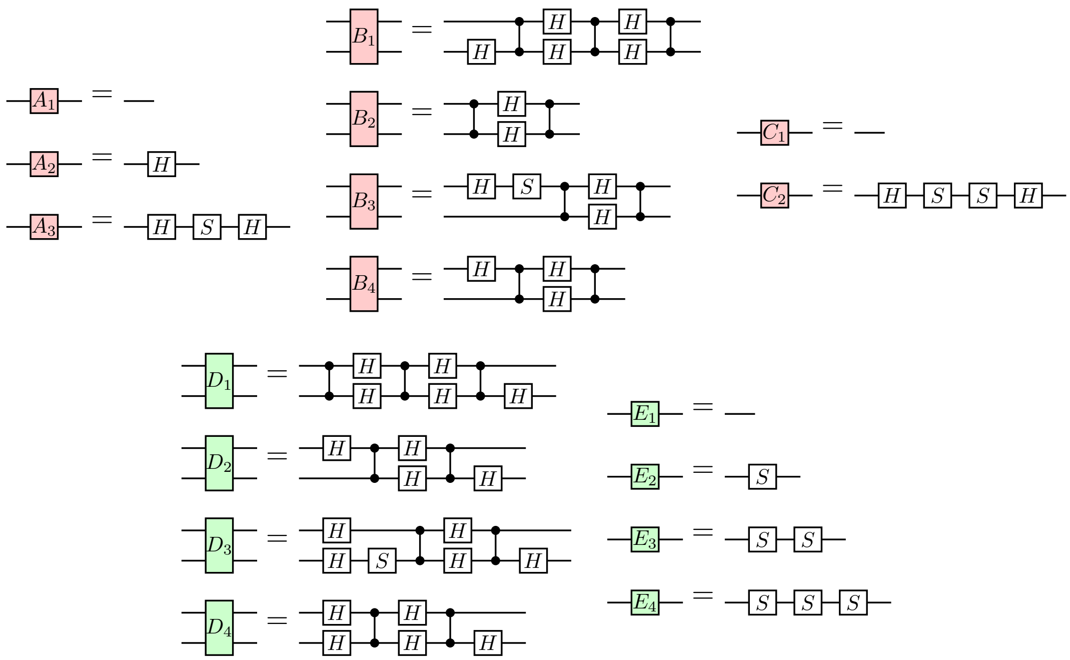
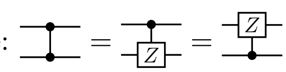


Figure 1: A convenient gate set for Clifford circuits.

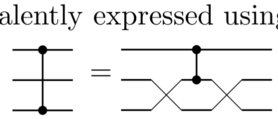
4. Normal forms for Clifford operators

We follow the usual practice of writing quantum circuits from left to right, i.e., in the opposite order of the notation for matrix multiplication. The qubits in a circuit are numbered from top to bottom. The gates ω, H, S, and Z_c were defined in (1.1), and are respectively called the omega-gate, Hadamard gate, S-gate, and controlled-Z gate. We use the usual circuit notations for the Hadamard and S-gates. Because the controlled-Z gate is symmetric in the two qubits it acts upon, we use a symmetric notation for it:

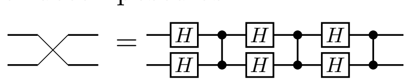
Hadamard gate: $-\boxed{H}-$; S-gate: $-\boxed{S}-$; Controlled Z-gate:  .

The Pauli operators (3.1) are also Clifford operators, and are definable as $X = HSSH$, $Y = HSSHSS\omega^2$, $Z = SS$.

Remark 4.1. In this paper, we assume that controlled-Z gates, and other binary gates, are only applied to *adjacent* qubits. This is without loss of generality, because gates on non-adjacent qubits can be equivalently expressed using swap gates:

 , (4.1)

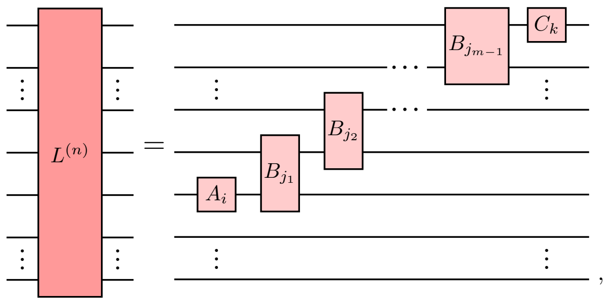
and swap gates can be further decomposed as

 . (4.2)

The restriction of gates to adjacent qubits leads to a much cleaner presentation of normal forms.

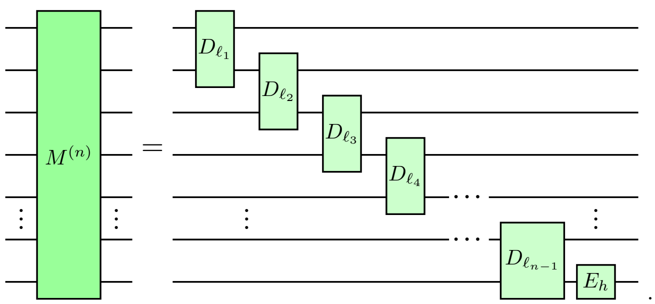
Definition 4.2. We define new basic gates A_i, B_j, C_k, D_ℓ, and E_h, where $i \in \{1,2,3\}$, $j, \ell, h \in \{1,2,3,4\}$, and $k \in \{1,2\}$. The meaning of these gates is given in Figure 1. Note that this gate set is highly redundant; for example, A_1, C_1, and E_1 are three different notations for the single-qubit identity gate. However, these gates will be convenient as building blocks for normal forms. They were chosen for their particular actions on Pauli operators, as will be explained in Section 5 and shown in Figure 2.

Definition 4.3. We say that an n-qubit circuit is Z-*normal* if it is of the form



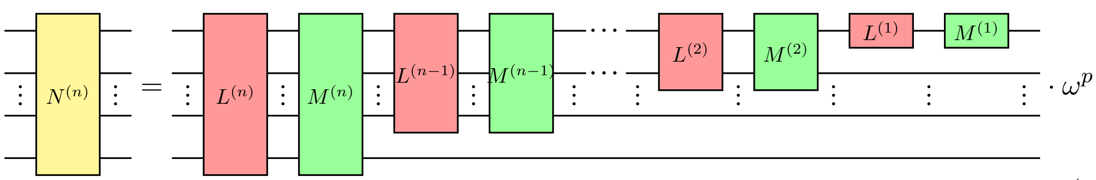
(4.3)

for $1 \leqslant m \leqslant n$. We say that an n-qubit circuit is X-*normal* if it is of the form



(4.4)

Finally, an n-qubit circuit is *normal* if it is of the form

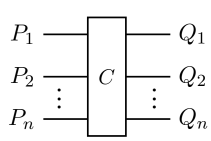


(4.5)

where $p \in \{0, 1, \ldots, 7\}$.

5. Existence and uniqueness of normal forms

When C is a Clifford operator, and $P = P_1 \otimes \ldots \otimes P_n$ and $Q = Q_1 \otimes \ldots \otimes Q_n$ are Pauli operators, we schematically write



to indicate that $C \bullet P = Q$. With that convention, Figure 2 shows the action of the operators A_i, B_j, C_k, D_ℓ, and E_h on selected Pauli operators.

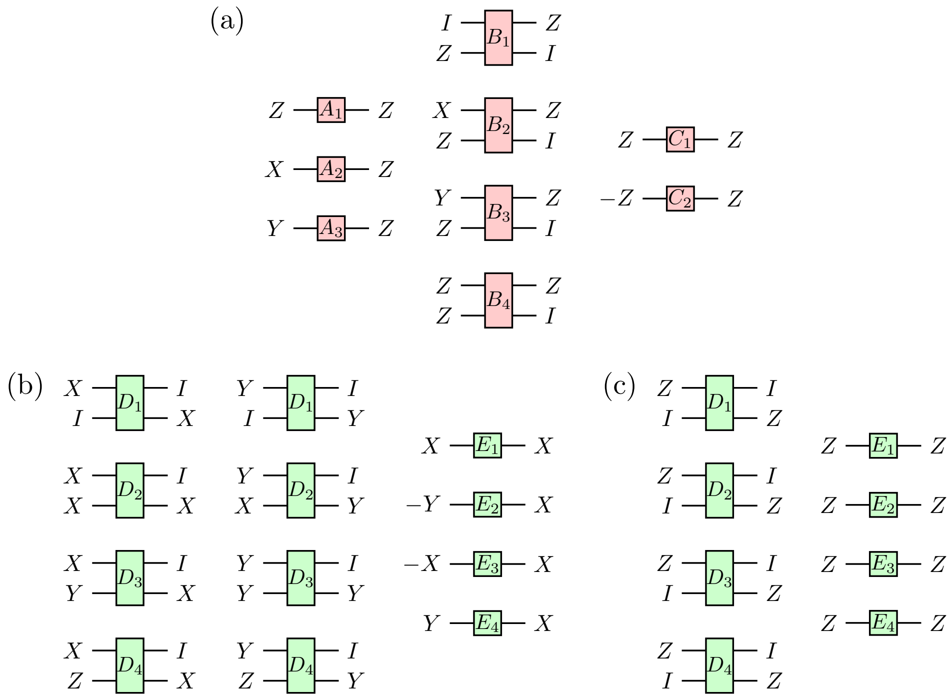
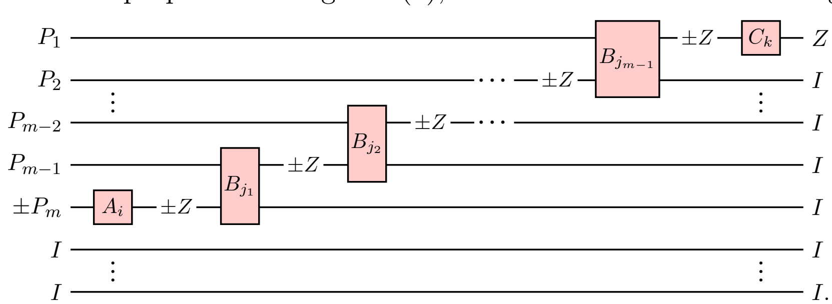


Figure 2: The action of the operators A_i, B_j, C_k, D_ℓ, and E_h on certain Pauli operators.

Lemma 5.1. *Let $n \geqslant 1$, and let P be an n-qubit Pauli operator satisfying $P^2 = I$ and $P \neq \pm I$. Then there exists a unique Z-normal circuit L such that*

$$L \bullet P = Z \otimes I \otimes \ldots \otimes I.$$

Proof. As a Pauli operator, P is of the form $P = \lambda P_1 \otimes P_2 \otimes \ldots \otimes P_n$, where $P_1, \ldots, P_n \in \{I, X, Y, Z\}$. The requirement $P^2 = I$ ensures that λ is ± 1 (and not $\pm i$). Moreover, since $P \neq \pm I$, there must be some m such that $P_m \neq I$; let m be the largest such index. The claim then follows from the properties in Figure 2(a), with reference to the following diagram:

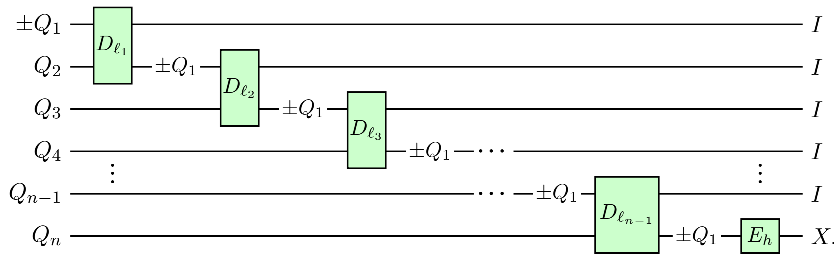


In particular, note that it follows from the properties in Figure 2(a) that there exists a unique A_i sending $\pm P_m$ to $\pm Z$; for each $p = 1, \ldots, m-1$, there exists a unique B_{j_p} sending $P_{m-p} \otimes \pm Z$ to $\pm Z \otimes I$; and there exists a unique C_k sending $\pm Z$ to Z. $\square$

Lemma 5.2. *Let $n \geqslant 1$, and let Q be an n-qubit Pauli operator satisfying $Q^2 = I$ such that Q anticommutes with $Z \otimes I \otimes \ldots \otimes I$. Then there exists a unique X-normal circuit M such* *that*

$$M \bullet Q = I \otimes \ldots \otimes I \otimes X.$$

Proof. As before, since $Q^2 = I$, we know that Q is of the form $Q = \pm Q_1 \otimes Q_2 \otimes \ldots \otimes Q_n$. Moreover, since Q anticommutes with $Z \otimes I \otimes \ldots \otimes I$, we have that $Q_1 \in \{X, Y\}$. The claim then follows from the properties in Figure 2(b), with reference to the following diagram:

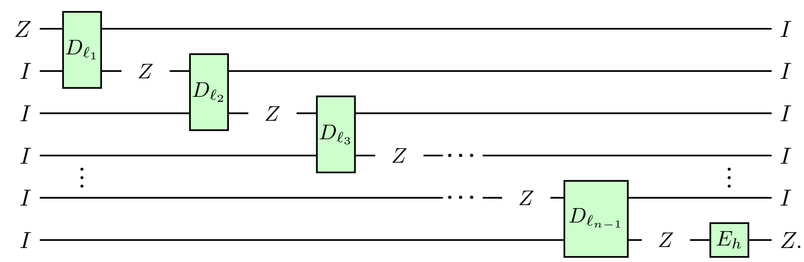


$\square$

Lemma 5.3. *Every X-normal circuit M satisfies*

$$M \bullet (Z \otimes I \otimes \ldots \otimes I) = I \otimes \ldots \otimes I \otimes Z.$$

Proof. By using the properties from Figure 2(c), with reference to the following diagram:



$\square$

Lemma 5.4. *Let $n \geqslant 1$, and let P and Q be n-qubit Pauli operators such that $P^2 = Q^2 = I$, and such that P, Q anticommute. Then there exist unique circuits M and L, where M is X-normal and L is Z-normal, such that*

$$ML \bullet P = I \otimes \ldots \otimes I \otimes Z$$

and

$$ML \bullet Q = I \otimes \ldots \otimes I \otimes X.$$

Proof. By Lemma 5.1, there exists a Z-normal circuit L such that $L \bullet P = Z \otimes I \otimes \ldots \otimes I$. Since P and Q anticommute, so do $L \bullet P$ and $L \bullet Q$. Therefore, by Lemma 5.2, there exists an X-normal circuit M such that $M \bullet (L \bullet Q) = I \otimes \ldots \otimes I \otimes X$, i.e., $ML \bullet Q = I \otimes \ldots \otimes I \otimes X$. By Lemma 5.3, we also have $ML \bullet P = M \bullet (L \bullet P) = M \bullet (Z \otimes I \otimes \ldots \otimes I) = I \otimes \ldots \otimes I \otimes Z$. This proves the existence of M and L. For uniqueness, assume that M' and L' are another pair of operators satisfying the conditions of the lemma. From $M' \bullet (L' \bullet P) = I \otimes \ldots \otimes I \otimes Z$, we have $L' \bullet P = Z \otimes I \otimes \ldots \otimes I$ by Lemma 5.3. Therefore, $L = L'$ by uniqueness of L in Lemma 5.1. But then $M' \bullet (L \bullet Q) = M \bullet (L \bullet Q) = X \otimes I \otimes \ldots \otimes I$, so that $M = M'$ by uniqueness of M in Lemma 5.2. $\square$

Proposition 5.5. *Let $\varphi : \mathcal{P}(n) \to \mathcal{P}(n)$ be an automorphism of the Pauli group such that φ fixes scalars. Then there exists a Clifford circuit C in normal form* (4.5) *such that for all P, $C \bullet P = \varphi(P)$. Moreover, the normal form C is unique up to the scalar ω^p.*

Proof. By induction on n. For $n = 0$, all Pauli operators are scalars, so φ is the identity; we can set $C = 1 = \omega^0$; uniqueness up to a scalar follows because for $n = 0$, all Clifford operators are scalars.

For the induction step, suppose the claim is true for $n-1$. We first prove existence. Let $P = \varphi^{-1}(I \otimes \ldots \otimes I \otimes Z)$ and $Q = \varphi^{-1}(I \otimes \ldots \otimes I \otimes X)$. Note that $I \otimes \ldots \otimes I \otimes Z$ and $I \otimes \ldots \otimes I \otimes X$ each square to the identity and anticommute with each other; since φ is an automorphism, the same is true for P and Q. By Lemma 5.4, there exists a circuit ML, where M is X-normal and L is Z-normal, such that

$$ML \bullet P = I \otimes \ldots \otimes I \otimes Z = \varphi(P) \tag{5.1}$$

and

$$ML \bullet Q = I \otimes \ldots \otimes I \otimes X = \varphi(Q). \tag{5.2}$$

Now define a new automorphism φ' by $\varphi'(U) = \varphi((ML)^{-1} \bullet U)$ for all $U \in \mathcal{P}(n)$. Note that φ' fixes scalars; also, by (5.1) and (5.2), $I \otimes \ldots \otimes I \otimes Z$ and $I \otimes \ldots \otimes I \otimes X$ are fixed points of φ'. Let R be an $n-1$-qubit Pauli operator, and consider $\varphi'(R \otimes I)$. Since $R \otimes I$ commutes with both $I \otimes \ldots \otimes I \otimes Z$ and $I \otimes \ldots \otimes I \otimes X$, the same is true for $\varphi'(R \otimes I)$; therefore, $\varphi'(R \otimes I) = S \otimes I$, for some $S \in \mathcal{P}(n-1)$. It follows that there exists an automorphism $\varphi'' : \mathcal{P}(n-1) \to \mathcal{P}(n-1)$ such that $\varphi'(R \otimes I) = \varphi''(R) \otimes I$, for all $R \in \mathcal{P}(n-1)$. Together with the fact that $I \otimes \ldots \otimes I \otimes Z$ and $I \otimes \ldots \otimes I \otimes X$ are fixed points of φ', this implies that $\varphi' = \varphi'' \otimes I$. By induction hypothesis, there exists a normal $n-1$-qubit Clifford circuit C' such that for all R, $C' \bullet R = \varphi''(R)$. Let $C = (C' \otimes I)ML$. Then for all U, we have

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

This proves the existence of the normal form C.

For uniqueness, suppose that D is another normal form Clifford circuit with $D \bullet U = \varphi(U)$ for all Pauli U. By definition of normal forms, D is of the form $(D' \otimes I)M'L'$, where M' is X-normal, L' is Z-normal, and D' is a normal Clifford circuit of $n-1$ qubits. Then $D \bullet P = \varphi(P) = I \otimes \ldots \otimes I \otimes Z$. It follows that $M'L' \bullet P = (D' \otimes I)^{-1} \bullet (I \otimes \ldots \otimes I \otimes Z) = I \otimes \ldots \otimes I \otimes Z$, and by a similar argument, $M'L' \bullet Q = I \otimes \ldots \otimes I \otimes X$. From the uniqueness of Lemma 5.4, we get $M' = M$ and $L' = L$. Then by uniqueness in the induction hypothesis, D' and C' are equal up to a scalar, and hence the same is true for D and C. □

Proof of Proposition 3.3. Proposition 3.3 is an immediate consequence of Proposition 5.5. □

Corollary 5.6. *The Clifford group on n qubits has exactly*

$$|\mathcal{C}(n)| = 8 \cdot \prod_{i=1}^{n} 2(4^i - 1)4^i$$

elements.

Proof. From the definition of Z-normal circuits, there are exactly

$$\sum_{m=1}^{n} 3 \cdot 4^{m-1} \cdot 2 = 2(4^n - 1)$$

circuits of the form $L^{(n)}$. Moreover, there are 4^n circuits of the form $M^{(n)}$, hence $2(4^n-1)4^n$ circuits of the form $M^{(n)}L^{(n)}$. Because there are exactly 8 scalars, it follows that there are

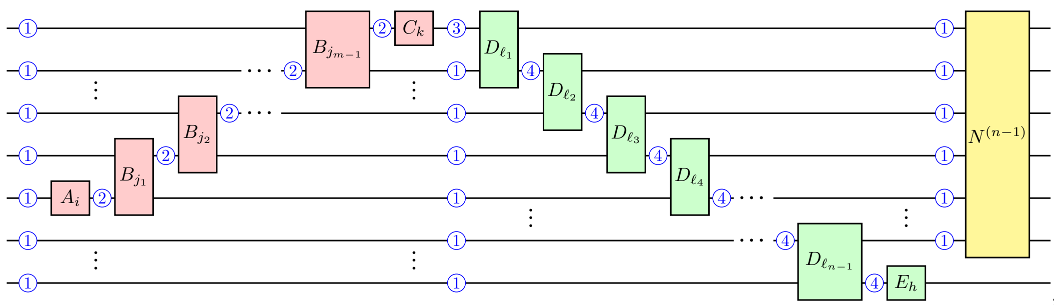
$$8 \cdot \prod_{i=1}^{n} 2(4^i-1)4^i$$

circuits of the form $N^{(n)}$ shown in (4.5). By Proposition 5.5, these are in one-to-one correspondence with the elements of the n-qubit Clifford group. □

6. Normalization via rewrite rules

In this section, we will describe an explicit procedure for converting any given Clifford circuit to normal form by using only a finite number of equations. This yields a presentation of the Clifford group by generators and relations.

Definition 6.1. Consider an n-qubit Clifford circuit in normal form:



(6.1)

We say that a circuit is in *dirty normal form* if it is of the form (6.1), except that the circuit may contain some additional gates, subject to the following rules:

- H-gates may be added to any wire labelled 1;
- S-gates may be added to any wire labelled 1, 2, 3, or 4;
- X-gates may be added to any wire labelled 2;
- Controlled Z-gates may be added to any pair of adjacent wires, provided that the top wire is labelled 1, 2, or 3, and the bottom wire is labelled 1;

We recursively assume that $N^{(n-1)}$ is in dirty normal form as well.

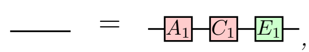
Lemma 6.2. *Any dirty normal form can be converted to an equivalent normal form by using the equations in Figures 3–7, in the left-to-right direction, a finite number of times.*

Proof. By inspection. Let us call the gates of type A–E *"clean"*, and the gates H, S, X, and Z_c *"dirty"*. Given two gate occurrences F and G in a circuit, we say that F is *immediately before* G if one of the outputs of F is connected to one of the inputs of G. We say that F is *before* G if there exists a sequence of gates, starting with F and ending with G, such that each is immediately before the next one.

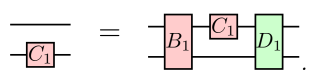
By the definition of dirty normal forms, every dirty gate occurs before some clean gate. Therefore, as long as there is at least one dirty gate in the circuit, some dirty gate (for example, the rightmost one) must occur *immediately* before a clean gate. The left-hand sides of the equations in Figures 3–7 cover all possible cases of a dirty gate occurring immediately before a clean gate. So as long as there are dirty gates left, one of the equations can always be applied. Moreover, a straightforward but tedious inspection of the equations in Figures 3–7 shows that the left-to-right application of each equation to a dirty normal form yields another dirty normal form.

It remains to be shown that this procedure terminates. To this end, we associate to each dirty normal form a sequence $\vec{v}$ of natural numbers as follows. Suppose the dirty normal form has r clean gates, which have been numbered $1, \ldots, r$ from left to right in the order in which they appear in (6.1). Then let $\vec{v} = (v_1, \ldots, v_r)$, where v_i is the number of dirty gates before the ith clean gate. It is easy to see that, with the exception of the equation $\omega^8 = 1$, each left-to-right application of an equation from Figures 3–7 decreases the sequence $\vec{v}$ in the lexicographic ordering. Although the length r of $\vec{v}$ is not constant, it is bounded by n^2, and since the set of all such sequences is well-ordered, it follows that the procedure terminates in a finite number of steps. □

Proposition 6.3. *Consider a Clifford circuit expressed in terms of the generators H, S, and controlled-Z gates on adjacent qubits. Any such circuit can be converted to its equivalent normal form by finitely many uses of the equations in Figures 3–7, together with the equations*

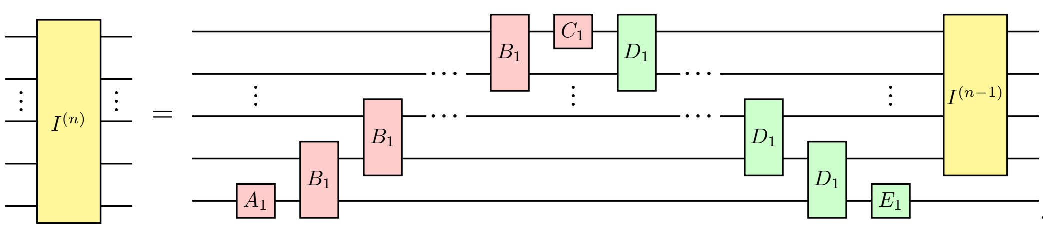


(6.2)



(6.3)

Proof. First, note that the normal form of the identity operator on n qubit is



(6.4)

The identity circuit can be converted to this normal form by a finite number of applications of the equations (6.2) and (6.3). By appending the normal form of the identity operator (6.4) to the given Clifford circuit, we obtain a dirty normal form, which can then be converted to a normal form by Lemma 6.2. □

7. An equational presentation of the Clifford groupoid

As an immediate consequence of Proposition 6.3, we know that the equations in Figures 3–7, together with the equations (6.2) and (6.3), and the defining equations in Figure 1, form a presentation of the Clifford groupoid by generators and relations. However, this formulation uses a large number of generators (namely all the gates of type A–E, as well as ω, S, H, X, and Z_c), and also a very large number of equations. Naturally, it would be desirable to find a much smaller set of generators and relations. This is done in the following proposition.

Proposition 7.1. *The Clifford groupoid is presented, as a strict spatial monoidal groupoid, by the generators shown in* (1.1) *and the relations shown in Figure 8.*

Proof. First, we can use the defining equations of Figure 1 to eliminate the generators of type A–E from (6.2), (6.3), and from the equations in Figures 3–7; we can also use the equation $X = HSSH$ to eliminate the gate X. This leaves only the generators ω, S, H, and Z_c. It is then a tedious, but finite exercise to verify that (6.2), (6.3), and each of the equations in Figures 3–7 is a consequence of the equations from Figure 8. A full, mostly machine-generated proof is available as a supplement to this paper [8]. □

It is not currently known to the author whether the equations in Figure 8 are independent.

Remark 7.2. Proving an equation about 2-qubit circuits never requires any of the 3-qubit axioms to be used; therefore, the equations of Figure 8(a)–(c) are sufficient to present the 2-qubit Clifford operators in terms of generators and relations. Similarly, the equations of Figure 8(a)–(b) are sufficient to present the 1-qubit Clifford operators, and, trivially, the relation of Figure 8(a) is sufficient to present the 0-qubit Clifford operators. It is also interesting to note that there are no special axioms involving 4 or more qubits; all equational properties of n-qubit Clifford circuits follow from axioms involving at most 3 qubits.

References

[1] M. Backens. The ZX-calculus is complete for stabilizer quantum mechanics. *New Journal of Physics*, 16:093021 (30 pages), 2014. Also available from `arXiv:1307.7025`.

[2] H. Buhrman, R. Cleve, M. Laurent, N. Linden, A. Schrijver, and F. Unger. New limits on fault-tolerant quantum computation. In *Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2006)*, pages 411–419, 2006.

[3] A. Burroni. Higher-dimensional word problems with applications to equational logic. *Theoretical Computer Science*, 115(1):43–62, 1993.

[4] D. Gottesman. The Heisenberg representation of quantum computers. In S. P. Corney, R. Delbourgo, and P. D. Jarvis, editors, *Group 22: Proceedings of the 12th International Colloquium on Group Theoretical Methods in Physics*, pages 32–43. International Press, 1999. Also available from `arXiv:quant-ph/9807006`.

[5] Y. Lafont. Towards an algebraic theory of Boolean circuits. *Journal of Pure and Applied Algebra*, 184:257–310, 2003.

[6] S. Mac Lane. *Categories for the Working Mathematician*. Graduate Texts in Mathematics 5. Springer, 1971.

[7] P. Selinger. A survey of graphical languages for monoidal categories. In B. Coecke, editor, *New Structures for Physics*, volume 813 of *Lecture Notes in Physics*, pages 289–355. Springer, 2011. Also available from `arXiv:0908.3347`.

[8] P. Selinger. Supplement to: Generators and relations for n-qubit Clifford operators. 105 pages. Available as ancillary material at `arXiv:1310.6813`, Oct. 2013.

[9] M. Van den Nest. Classical simulation of quantum computation, the Gottesman-Knill theorem, and slightly beyond. *Quantum Information and Computation*, 10(3–4):258–271, 2010. Also available from `arXiv:0811.0898`.

$$\omega^8 = 1$$

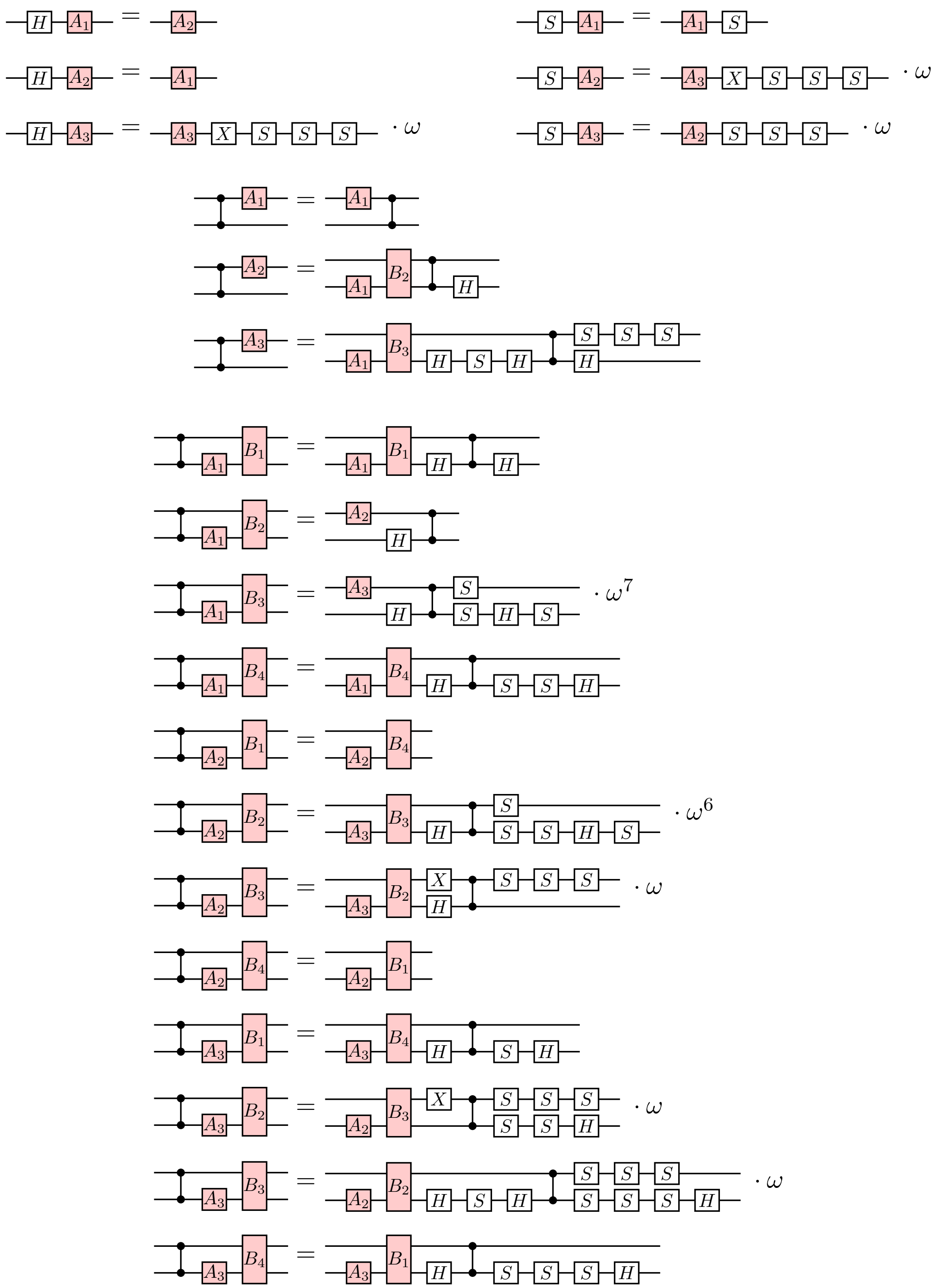


Figure 3: Rewrite rules for normal forms, part I

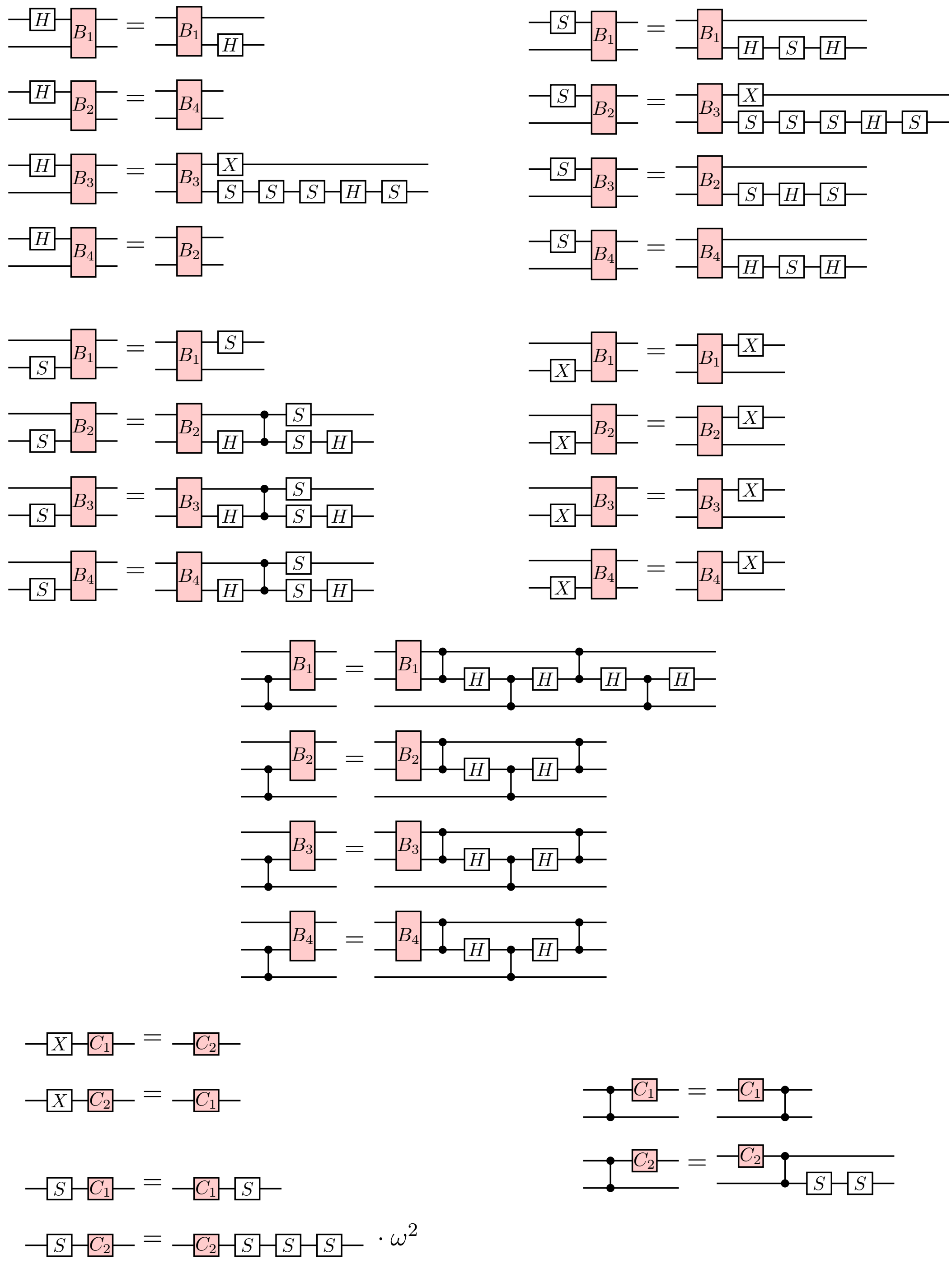


Figure 4: Rewrite rules for normal forms, part II

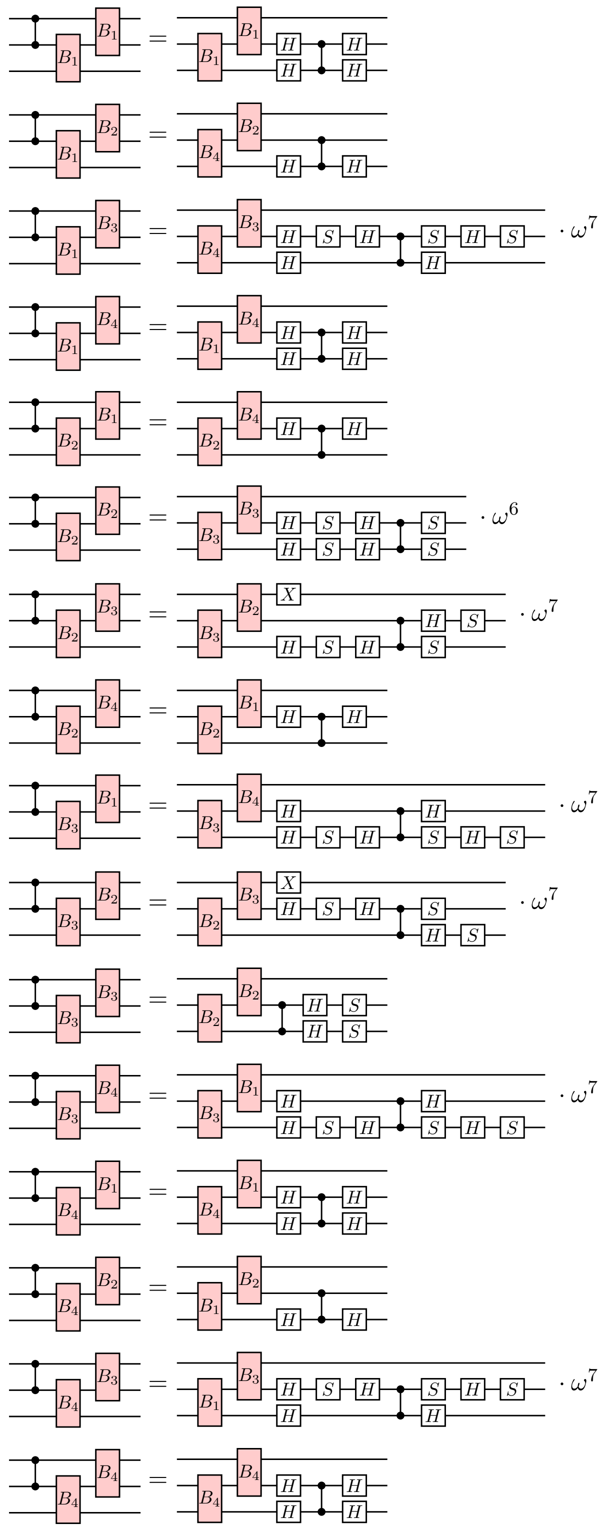


Figure 5: Rewrite rules for normal forms, part III

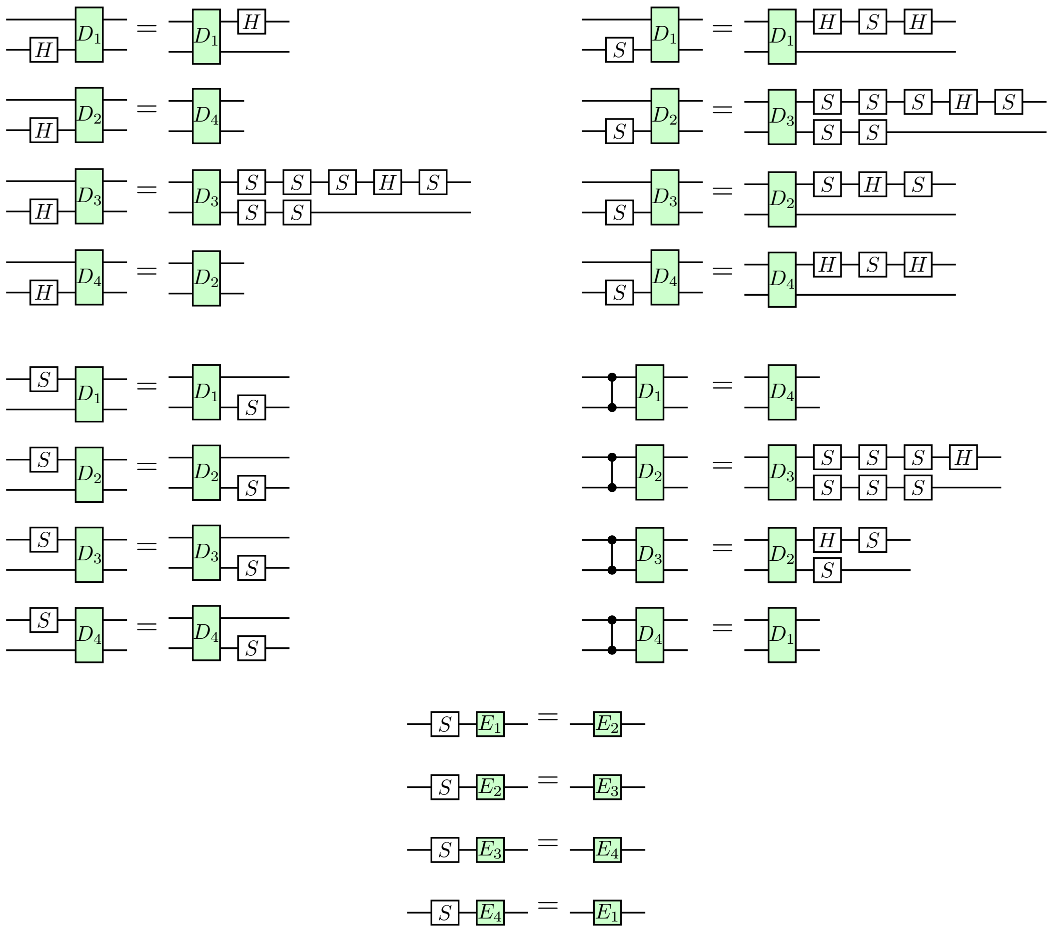


Figure 6: Rewrite rules for normal forms, part IV

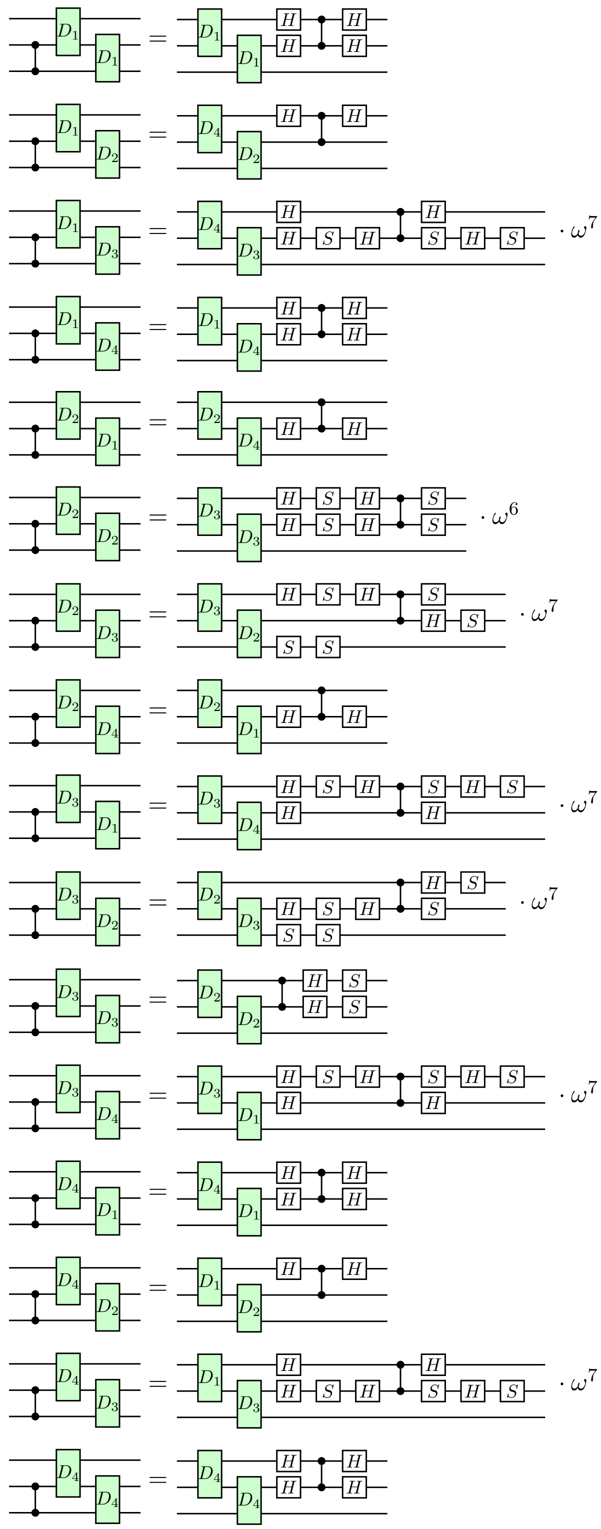


Figure 7: Rewrite rules for normal forms, part V

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

$$\omega^8 = 1 \tag{C1}$$

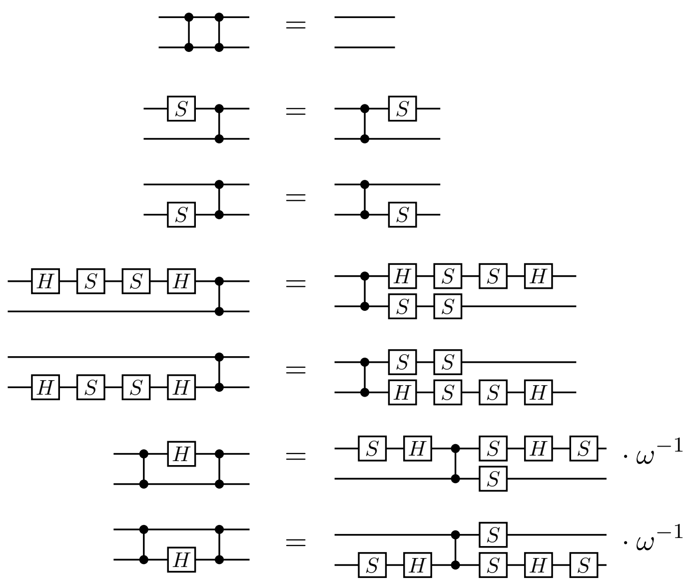
(b) Equations for $n \geqslant 1$:

$$H^2 = 1 \tag{C2}$$

$$S^4 = 1 \tag{C3}$$

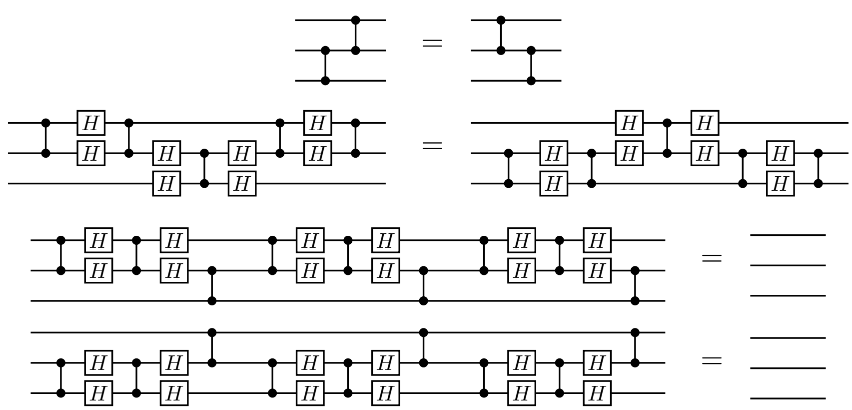
$$SHSHSH = \omega \tag{C4}$$

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



(C5)
(C6)
(C7)
(C8)
(C9)
(C10)
(C11)

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



(C12)
(C13)
(C14)
(C15)

Figure 8: A presentation of the (strict spatial monoidal) Clifford groupoid by generators and relations