GENERATORS AND RELATIONS FOR REAL STABILIZERS

by

Justin Makary

Submitted in partial fulfillment of the requirements
for the degree of Master of Science

at

Dalhousie University
Halifax, Nova Scotia
August 2020

I dedicate the work of my dissertation to my father, Joseph Makary,
the loving and hardworking man I aspire to be.

Table of Contents

List of Figures

Abstract

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 Clifford circuit to its normal form. This yields a presentation by generators and relations of the strict spatial monoidal category of real stabilizer operators.

List of Abbreviations and Symbols

$\mathbb{C}$	The field of complex numbers.
$\mathbb{Z}_2^n$	The ring of binary sequences of length n.
$\mathbb{Z}_n$	The ring of integers modulo n.
$\mathbb{R}$	The field of real numbers.
$M_n(\mathbb{R})$	The vector space of $n \times n$ real matrices.
$\mathcal{C}(n, \mathbb{C})$	The complex Clifford Group on n qubits.
$\mathcal{C}(n, \mathbb{R})$ or $\mathcal{C}(n)$	The real Clifford Group on n qubits.
$\mathrm{O}(n)$	The orthogonal group of degree 2^n.
$\mathcal{P}(n, \mathbb{C})$	The complex Pauli Group on n qubits.
$\mathcal{P}(n, \mathbb{R})$ or $\mathcal{P}(n)$	The real Pauli Group on n qubits
$\mathrm{U}(n)$	The unitary group of degree 2^n.
$A \bullet P$	Conjugation of P by A.
$A \otimes B$	The Kronecker product of the matrices A and B.
A^{-1}	The inverse of the matrix A.
$A^{\dagger}$	The conjugate transpose of the matrix A.
A^{T}	The transpose of the matrix A.

H, C_Z, C_{XZ} The Hadamard, controlled-Z, and controlled-XZ gates.

X, Y, Z The Pauli rotation matrices.

Acknowledgements

I would like to express my deepest appreciation to my parents, Joseph and Holly. They have showed me extreme love and kindness, and respectfully had me under their roof over the past seven years of post-secondary study in mathematics. Without them and their support, I would not have had the opportunity to achieve what I have achieved. I love you guys.

I am also extremely grateful to my girlfriend, Emma Fleet. You have supported me emotionally throughout my studies as a mathematician, and been there for me throughout. Thank you for everything love, you are the best.

I am also deeply indebted to my supervisor, Neil J. Ross. You have been a encouraging and kind mentor, and are a role model for me as a professional in academia who positively affects the environment around them. Thank you for everything, I truly would not be here if it was not for your patience, and help.

I wish to further thank my readers Dorette Pronk and Peter Selinger for taking the time to read and give input to my thesis. Having experts such as yourselves help me with my project has been an honour. I especially wish to thank Peter Selinger for making crucial observations and suggesting a path forward when the project had more or less been stalled. Your insights were integral to the final product of this paper.

I would like to thank my two friends Owen Sharpe and Jason d'Eon, for being the brightest, and nicest math nerds I had the pleasure to study with.

Further thanks to Brian Welcher, for being such a kind mentor, and inspiring me to continue my study of mathematics after high school.

Mitja Mastnak, for guiding me through rigorous training in mathematics during my undergrad, and believing in my ability.

Stavros Konstantinidis, for showing me the beauty of the intersection between mathematics and computing, and helping develop my abilities to later do research in this area.

Finally, thanks to Arthur Finbow on captaining the ship of me and the merry

grigs, Jake Babin and Isaac Cain. May we one day defeat the wide-eyed stranger, and receive infinite moony-pies.

Chapter 1

Introduction

Stabilizer operators, which are also known as *Clifford* operators, play a fundamental role in the study of fault-tolerant quantum computation [10].

The Clifford operators are generated, under composition and Kronecker product, by the gates

$$\omega = e^{\frac{i\pi}{4}}, \quad H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, \quad \text{and} \quad C_Z = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix},$$

where ω is a scalar, and H, S, and C_Z are the *Hadamard*, *phase*, and *controlled-Z* gates, respectively. For all $n \geq 0$, the set of Clifford operators on n qubits forms a group, which is known as the *complex Clifford group* and is denoted $\mathcal{C}(n, \mathbb{C})$. This group is a finite subgroup of $\mathrm{U}(2^n)$, the *unitary group* of degree 2^n. If C is a Clifford operator, any representation for C in terms of the generators above is called a *circuit* for C.

Quantum circuits for stabilizer operators have been extensively studied [1, 4, 5, 7, 11, 13, 15]. In particular, in [13], Selinger gave a finite presentation of Clifford operators by introducing a normal form for Clifford circuits together with a finite collection of relations that suffice to rewrite any Clifford circuit to its normal form.

In this thesis, we study *real* Clifford operators which are generated by

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

where Z is the *Pauli Z* gate. The group of n-qubit real Clifford operators $\mathcal{C}(n, \mathbb{R})$ is the intersection of $\mathcal{C}(n, \mathbb{C})$ and the *orthogonal group* $\mathrm{O}(2^n)$ of degree 2^n.

Restrictions such as the one considered here have been previously studied in the context of randomized benchmarking [8], graphical languages [6, 16], and exact synthesis [3].

The contributions of this thesis are the following. We define a normal form for real Clifford circuits and show that every real Clifford operator admits a unique normal form. We then introduce a collection of relations between real Clifford circuits and formulate a rewrite system to transform any real Clifford circuit to its normal form, using a finite number of applications of the relations. Our work largely follows the methods used by Selinger in [13]. In particular, our normal forms, the notions of clean and dirty normal forms, and the normalization procedure described below are adapted from [13]. But the focus on real operators requires additional restrictions on the construction of normal forms. These restrictions are enforced by introducing a notion of *coloured circuit*.

The thesis is organized as follows. In Chapter 2, we examine the structure of the real Pauli and Clifford groups. In Chapter 3 we review the diagrammatic language of circuits and introduce coloured circuits. In Chapter 4 we proceed to define our normal forms and to prove that real Clifford operators admit a unique normal form. We then state our relations in Chapter 5 and propose a system for transforming any real Clifford circuit to its normal form. Lastly, we discuss avenues for future work in Chapter 6.

Chapter 2

The Real Pauli and Clifford Groups

In this chapter, we introduce the matrix groups that will be the focus of this thesis. If A and B are matrices, we write AB for their product and $A \otimes B$ for their Kronecker product. We write I_n for the identity matrix of dimension n, dropping the subscript n when the dimension can be inferred from context. For brevity, if a is a scalar we write a for aI. We denote the transpose of the matrix A by $A^{\intercal}$. A matrix A is symmetric if $A = A^{\intercal}$ and orthogonal if $A^{-1} = A^{\intercal}$. The collection of real $n \times n$ orthogonal matrices forms a group under multiplication known as the *orthogonal group of degree* n and denoted $\mathrm{O}(n)$. Following [13], for $A, B \in \mathrm{O}(n)$, 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 basis. Furthermore, we will refer to our Kronecker product as simply the tensor product, when in reality it is a special case of a tensor product on finite dimensional matrices, such that $(A \otimes B) \otimes C = A \otimes (B \otimes C)$.

2.1 The Real Pauli Group

Definition 2.1.1. The *real Pauli matrices* X and Z are defined as

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

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

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

In what follows, we drop the adjective "real" and simply refer to X and Z as Pauli matrices and to $\mathcal{P}(n, \mathbb{R})$ as the Pauli group. In addition, we write $\mathcal{P}(n)$ for $\mathcal{P}(n, \mathbb{R})$.

Note that $\mathcal{P}(n) \subseteq \mathrm{O}(2^n)$. A set of generators for $\mathcal{P}(n)$ is obtained by taking tensor products of the form $I \otimes \cdots \otimes I \otimes X \otimes I \otimes \cdots \otimes I$ and $I \otimes \cdots \otimes I \otimes Z \otimes I \otimes \cdots \otimes I$, where X and Z appear in all of the possible n components. For example, the following operators generate $\mathcal{P}(3)$:

$$\begin{aligned}
&X \otimes I \otimes I, \\
&I \otimes X \otimes I, \\
&I \otimes I \otimes X, \\
&Z \otimes I \otimes I, \\
&I \otimes Z \otimes I, \text{ and} \\
&I \otimes I \otimes Z.
\end{aligned}$$

Any element P of $\mathcal{P}(n)$ can be written as $P = (-1)^a(X^{b_1}Z^{c_1} \otimes \cdots \otimes X^{b_n}Z^{c_n})$ where $a, b_i, c_i \in \mathbb{Z}_2$. The Pauli matrix P can thus be represented by a triple (a, b, c) where $b = [b_1, b_2, \ldots, b_n]$ and $c = [c_1, c_2, \ldots, c_n]$ are n-dimensional binary vectors. The mapping $P \mapsto (b, c)$, where (a, b, c) is the binary representation of P, defines a homomorphism from $\mathcal{P}(n)$ onto $\mathbb{Z}_2^n \times Z_2^n$.

Proposition 2.1.3. $|\mathcal{P}(n)| = 2^{2n+1}$

Proof. By counting the binary representations of Pauli operators. □

Proposition 2.1.4. *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 $P \in \mathcal{P}(n)$, $P_i^2 = (-1)^d I$ where d is the number of components for which $P_i = XZ$. Thus, $P^2 = I$ if and only if d is even. □

Proposition 2.1.5. *The single-qubit Pauli group $\mathcal{P}(1)$ spans $M_2(\mathbb{R})$, the space of real 2×2 matrices.*

Proof. We notice that

$$\frac{I+Z}{2} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad \frac{X - XZ}{2} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix},$$

$$\frac{X+XZ}{2}=\begin{bmatrix}0 & 0\\ 1 & 0\end{bmatrix}, \quad \text{and} \quad \frac{I-Z}{2}=\begin{bmatrix}0 & 0\\ 0 & 1\end{bmatrix}.$$

It follows that $\mathcal{P}(1)$ spans $M_2(\mathbb{R})$. □

Corollary 2.1.6. *The n-qubit Pauli group $\mathcal{P}(n)$ spans $M_{2^n}(\mathbb{R})$, the space of real $2^n \times 2^n$ matrices.*

Proof. If V is a vector space spanned by some set S, then $S^{\otimes n} = \{s_1 \otimes \cdots \otimes s_n : s_i \in S\}$ spans $V^{\otimes n} = V \otimes \cdots \otimes V$. As a special case of this, since $\mathcal{P}(1)$ spans $M_2(\mathbb{R})$ by Proposition 2.1.5, $\mathcal{P}(n) = \mathcal{P}(1)^{\otimes n}$ spans $M_2(\mathbb{R})^{\otimes n}$. But the latter space is isomorphic to $M_{2^n}(\mathbb{R})$ and the result follows. □

2.2 The Real Clifford Group

Definition 2.2.1. The *real Clifford group on n qubits* $\mathcal{C}(n,\mathbb{R})$ is the normalizer of $\mathcal{P}(n)$ in $\mathrm{O}(2^n)$. That is,

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

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

Proposition 2.2.2. *Let $C \in \mathcal{C}(n)$. If $C \bullet P = P$ for all $P \in \mathcal{P}(n)$, then $C = \pm 1$.*

Proof. By Corollary 2.1.6, $\mathcal{P}(n)$ spans the space of $2^n \times 2^n$ real matrices. By our assumption, we have that $CPC^{-1} = P$, for all $P \in \mathcal{P}(n)$. 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 2.2.3. *If C and D are two elements of $\mathcal{C}(n)$ that act identically on $\mathcal{P}(n)$, then $C = \pm D$.*

Proof. Since C and D act identically on $\mathcal{P}(n)$, we have

$$(D^{-1}C) \bullet P = D^{-1} \bullet C \bullet P = D^{-1} \bullet D \bullet P = P.$$

Thus, by Proposition 2.2.2, $D^{-1}C = \pm 1$. Hence $C = \pm D$. □

Definition 2.2.4. The *Hadamard matrix* H and the *Controlled-Z matrix* C_Z are defined as

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

We note that $H \in \mathcal{C}(1)$, $C_Z \in \mathcal{C}(2)$, and $\mathcal{P}(n) \subseteq \mathcal{C}(n)$. For future reference, the action of some chosen Clifford operators on elements of the Pauli group are recorded in the proposition below, which is proved by direct calculation.

Proposition 2.2.5. *We have*

$$\begin{aligned} X \bullet X &= X & \qquad X \bullet Z &= -Z \\ Z \bullet X &= -X & \qquad Z \bullet Z &= Z \\ H \bullet X &= Z & \qquad H \bullet Z &= X \end{aligned}$$

$$\begin{aligned} C_Z \bullet (X \otimes I) &= X \otimes Z & \qquad C_Z \bullet (Z \otimes I) &= Z \otimes I \\ C_Z \bullet (I \otimes X) &= Z \otimes X & \qquad C_Z \bullet (I \otimes Z) &= I \otimes Z \end{aligned}$$

2.3 The Complex Pauli and Clifford Groups

We close this chapter with some brief remarks about the complex Pauli and Clifford groups. Recall that a complex matrix V is *unitary* if $V^\dagger = V^{-1}$, where $V^\dagger$ is the *conjugate transpose* of V, and that the group of $n \times n$ unitary matrices forms a group known as the *unitary group of degree* n and denoted $\mathrm{U}(n)$.

The complex Pauli operators are generated by the operators X and Z of Definition 2.1.1 together with the following Pauli Y gate

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}.$$

On a fixed number n of qubits, complex Pauli operators form a group known as the *complex Pauli group on n qubits* and denoted $\mathcal{P}(n, \mathbb{C})$. The *complex Clifford group on* *n qubits* $\mathcal{C}(n,\mathbb{C})$ is the normalizer of $\mathcal{P}(n,\mathbb{C})$ in $\mathrm{U}(2^n)$, the unitary group of degree 2^n. It is known, and was proved, for example, in [13], that the group $\mathcal{C}(n,\mathbb{C})$ has order

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

In contrast, the real Clifford group has order

$$|\mathcal{C}(n,\mathbb{R})| = 2 \cdot \prod_{i=1}^{n} (4^i + 2^i - 2)(2 \cdot 4^{i-1})$$

as was proved in [9]. We will also establish this fact in Chapter 4.

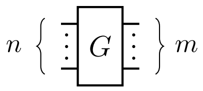
Chapter 3

Circuits

In this chapter, we review the language of quantum circuits, which provides a convenient graphical notation for operators.

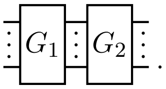
3.1 Quantum Circuits

Quantum circuits are made up of *gates*. Let $m, n \in \mathbb{N}$. A gate with n *inputs* and m *outputs* is represented by a diagram of the following form.

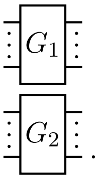


Above, we have n *input* wires on the left, and m *output* wires on the right. We assume the existence of an *identity* gate with 1 input and 1 output. It is represented by a *wire* as below.

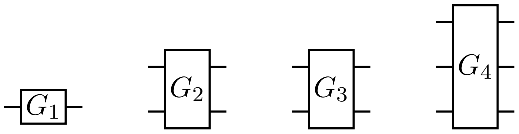
Note that a gate can have 0 inputs and 0 outputs, in which case we call it a *scalar* and often denote it without its bounding box. We can compose gates in two ways: *horizontally* and *vertically*. The horizontal composition of two gates G_1 and G_2 is represented by



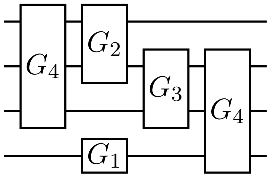
For the horizontal composition of G_1 and G_2 to be defined, G_2 must have as many inputs as G_1 has outputs. The vertical composition of two gates G_1 and G_2 is represented by



If the gate G_1 has n_1 inputs and m_1 outputs, while the gate G_2 has n_2 inputs and m_2 outputs, then their vertical composition will have n_1+n_2 inputs and m_1+m_2 outputs. A *circuit* is a diagram constructed from the horizontal and vertical composition of gates from a base set. For example, consider the base set of gates below.



An example of a circuit constructed from these gates is shown below.

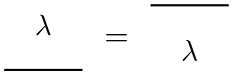


In general, if a circuit C is constructed using gates from $\{G_1, \ldots, G_k\}$, we say that C is *a circuit over the gate set* $\{G_1, \ldots, G_k\}$.

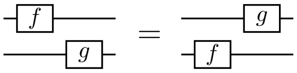
It will sometimes be convenient to refer to gates within a circuit. We say that a gate G is *immediately before* a gate G' if one of the outputs of G connects to one of the inputs of G'. A gate G is simply *before* a gate G' if there is a sequence of gates, each immediately before the next one, starting with G and ending with G'.

We can *interpret* circuits as matrices. This is done by introducing an *interpretation map* $[\![\cdot]\!]$ which assigns a matrix $[\![C]\!]$ to any circuit C. The interpretation is defined by assigning a matrix to each one of the basic gates, and by extending this assignment to arbitrary diagrams as follows: the vertical composition of two diagrams C and D is defined as $[\![C]\!] \otimes [\![D]\!]$ and the horizontal composition of two (composable) diagrams C and D is defined as $[\![D]\!] \cdot [\![C]\!]$. Two circuits are said to be *equivalent* if $[\![C]\!] = [\![D]\!]$. By a slight abuse of notation, we often omit $[\![\cdot]\!]$. Instead, if C is a circuit and M is a matrix such that $[\![C]\!] = M$, we often write $C = M$. Similarly, we often denote the fact that two circuits C and D are equivalent by simply writing $C = D$.

We only consider circuits up to certain topological deformations. In particular, scalars can be freely moved around the diagrams so that we consider the two circuits below to be equal.

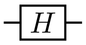


This property is sometimes called the *spatial law.* In addition, gates can be moved along wires, so that, for example, the two circuits below are also considered equal.

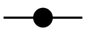


This property is known as the *bifunctorial law.* Finally, wires can be bent or stretched at will, but not cut or crossed. The interpretation of circuits as matrices is robust to these deformations in the sense that if C and D are two circuits that differ only up to, e.g., the placement of scalars, then C and D are in fact equivalent. We note that these implicit identifications endow the collection of circuits with the structure of a spatial monoidal category (see [13], and more formally introduced in [12]), although this fact will not play a large role in what follows.

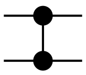
In what follows, we will be interested in circuits for Clifford operators. To this end, we introduce the below gates to be interpreted as the Hadamard, Pauli Z, and controlled-Z matrices respectively.



$$= \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

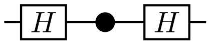


$$= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$



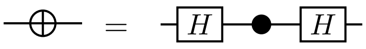
$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

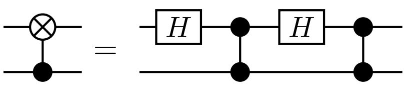
Note that the Pauli X operator can be represented over this gate set since



$$= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

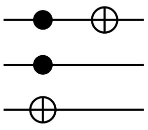
For brevity, we introduce some *derived* gates below, which are shorthand for some Clifford circuits.





The derived gate on the left represents the Pauli X gate. We call the derived gate on the right the C_{XZ} gate, an abbreviation for *controlled-XZ*.

As a final example of an interpreted circuit, it can be verified that the circuit

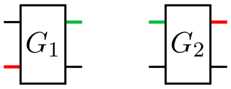


corresponds to the matrix below.

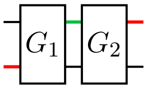
$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

3.2 Coloured Circuits

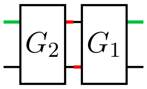
We now introduce *coloured circuits*. The notion of a *coloured gate* coincides with our previous notion of gate, with the difference that some of the wires are coloured, as shown in the two examples below.



The colouring of wires does not affect the vertical composition of gates, but two gates can only be composed horizontally if the colours of the corresponding wires are the same. For example, the gates G_1 and G_2 above can be composed as



but not as

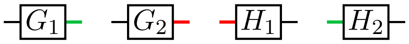


so that the composition in this last diagram is not well-defined.

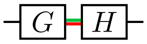
Coloured circuits are then constructed from coloured gates with this restriction. This colouring of gates is meant to act as a form of typing to constrain the construction of circuits.

A coloured 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 a circuit made from preexisting gates. In the second stage, colours are associated to the input and output wires of the gate. Note that any coloured circuit can still be viewed as a non-coloured circuit by simply *forgetting* about the colour of the wires.

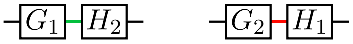
We will sometimes assign more than one colour to the wires of a circuit to concisely specify a family of circuits. As an illustration, consider the coloured gates below.



Then the diagram

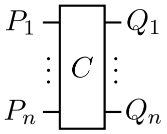


represents the family of circuits in which the gate on the left-hand side is one of G_1 or G_2 and the gate on the right-hand side is one of H_1 or H_2 subject to the condition that the circuit is a well-formed coloured circuit. In fact, there are two circuits in this specific family, namely the two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

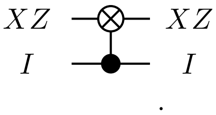


3.3 Annotated Circuits

We close this chapter with a final notational convention: annotations. These annotations allow us to express the action of a Clifford operator on a Pauli operator under conjugation. When $C \in \mathcal{C}(n)$, and $P = P_1 \otimes \cdots \otimes P_n$, $Q = Q_1 \otimes \cdots \otimes Q_n \in \mathcal{P}(n)$, we write



to indicate that $C \bullet P = Q$. For example, we can describe the action of the C_{XZ} gate in this way as follows.



Chapter 4

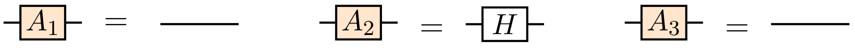
Normal Forms for Real Clifford Circuits

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

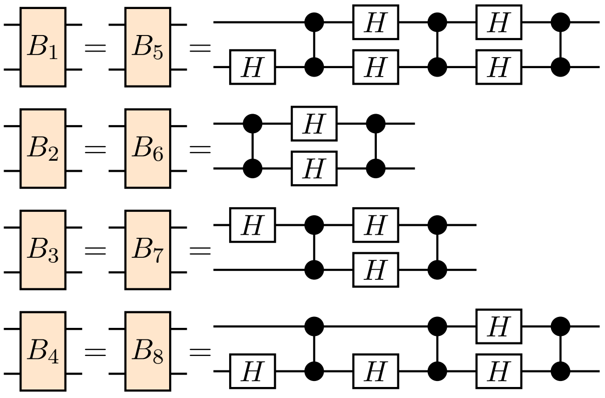
4.1 Derived Generators

We start by introducing *derived generators*, which will serve as the basic building blocks for our normal forms. As discussed in Chapter 3, we introduce these derived generators in two stages: first we define the gates as (uncoloured) circuits and then we specify the colours of their wires. Our derived generators come in five groups which we name A, B, C, D, and E.

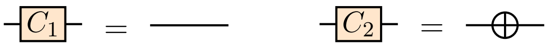
Definition 4.1.1. The A *gates* are defined below.



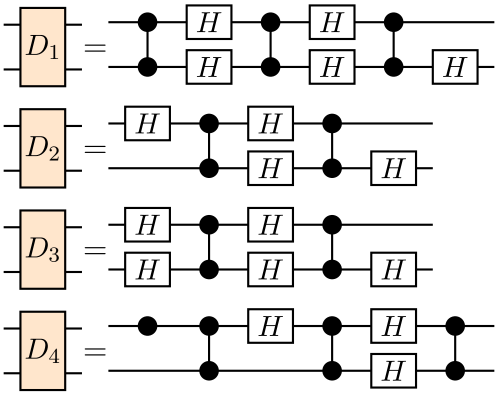
Definition 4.1.2. The B *gates* are defined below.



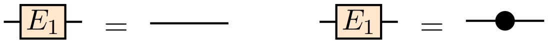
Definition 4.1.3. The C *gates* are defined below.



Definition 4.1.4. The D *gates* are defined below.

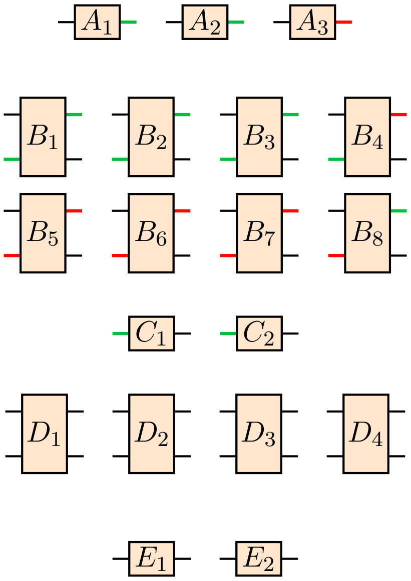


Definition 4.1.5. The E *gates* are defined below.



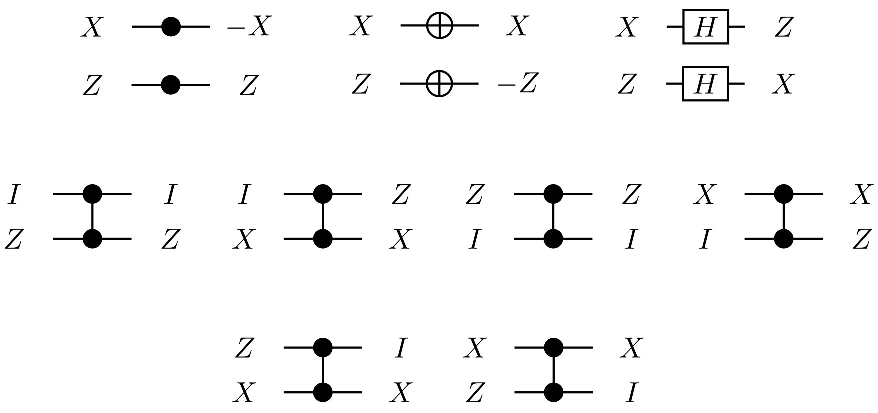
In what follows, we sometimes say that a gate is *of type* A (respectively B, C, D, E) if it is an A (respectively B, C, D, E) gate.

Definition 4.1.6. The coloured gates of type A, B, C, D, and E are defined below.



The following corollary reformulates the actions of Proposition 2.2.5 into annotated circuits. These can be used to compute the actions of larger circuits, such as the defined derived generators.

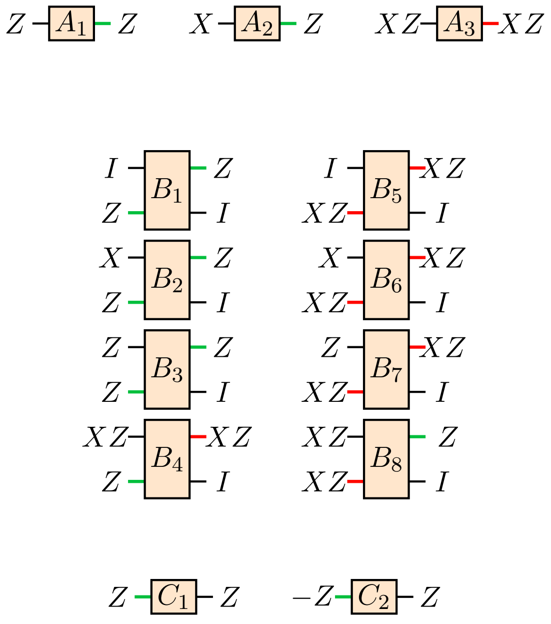
Corollary 4.1.7. *The following annotated circuits record the action of the X, Z, H, and C_Z gates on selected Pauli operators.*

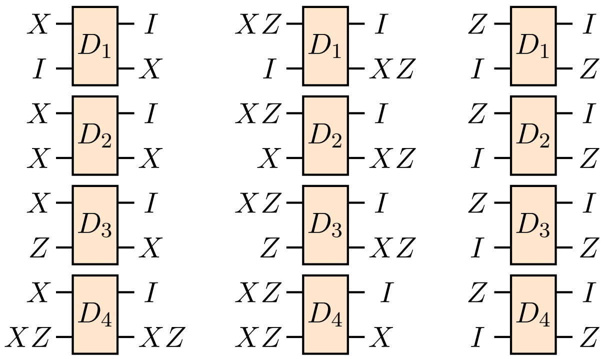


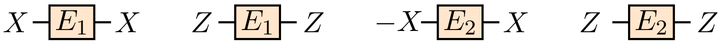
Proof. The first seven annotated circuits follow from the actions in Proposition 2.2.5, while the final two annotated circuits follow from the above seven, and the fact that C_Z is self-inverse. □

The next proposition states the action of the derived generators on well-chosen Pauli operators and will play an important role in the study of normal forms.

Proposition 4.1.8. *The following annotated circuits record the action of the gates of type A, B, C, D, and E on certain Pauli operators.*







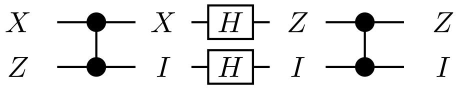
Furthermore, in each action represented above, the specified gate is the unique derived generator of its type and output colours that performs this action.

Proof. By computation. □

The proof of Proposition 4.1.8 requires tedious computation. We note here that one can verify the actions of the derived generators stated above by applying the actions described for each basic generator in Proposition 2.2.5. For example, consider the action of the gate B_2 on the Pauli $X \otimes Z$. Note that since we are only considering the action of the gate, wire colours can be omitted here. Since $B_2 = C_Z \cdot (H \otimes H) \cdot C_Z$, we get

$$\begin{aligned} B_2 \bullet (X \otimes Z) &= C_Z \bullet ((H \otimes H) \bullet (C_Z \bullet (X \otimes Z))) \\ &= C_Z \bullet ((H \otimes H) \bullet (X \otimes I)) \\ &= C_Z \bullet (Z \otimes I) \\ &= Z \otimes I. \end{aligned}$$

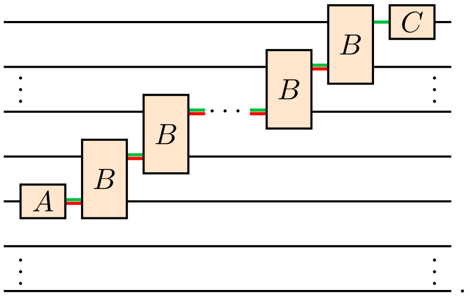
This can also be recognized diagrammatically by considering the annotated circuit of B_2 acting on $X \otimes Z$, and applying a sequence of the actions in Corollary 4.1.7 to receive the right hand side of the annotated circuit. This is shown in the following example.



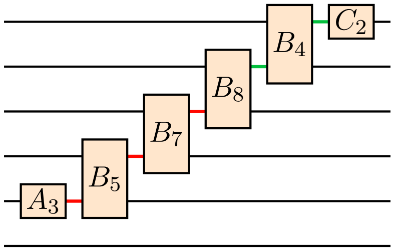
4.2 Normal forms

We now describe our normal forms.

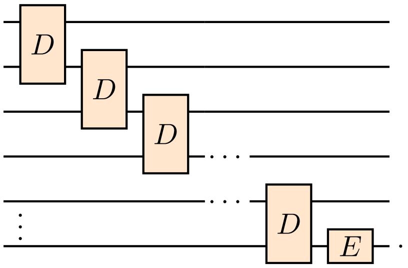
Definition 4.2.1. An n-qubit circuit is a *Z-circuit* if it is of the form



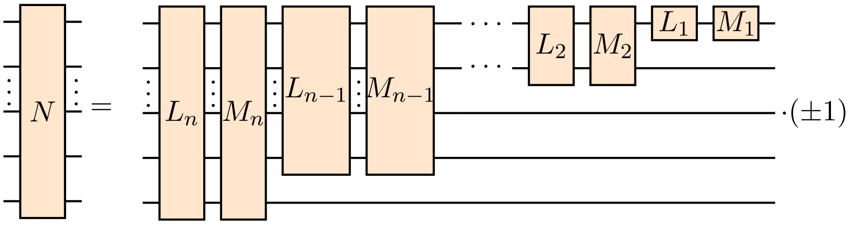
Z-circuits have a ladder structure, and a matching of coloured wires along the way. An example of a Z-circuit is shown below.



Definition 4.2.2. An n-qubit circuit is an *X-circuit* if it is of the form



Definition 4.2.3. An n-qubit circuit is *normal* if it is of the form

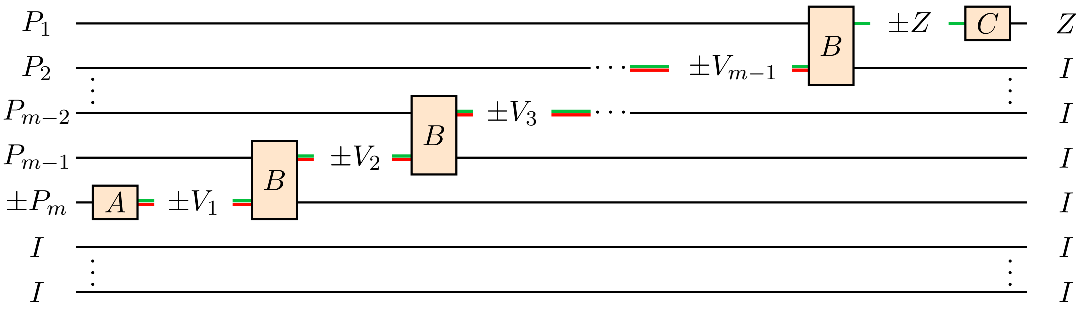


where, for $1 \leq i \leq n$, L_i is a Z-circuit, and M_i is an X-circuit.

The next several propositions culminate in the proof that every Clifford operator is represented by a unique normal circuit.

Proposition 4.2.4. *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.



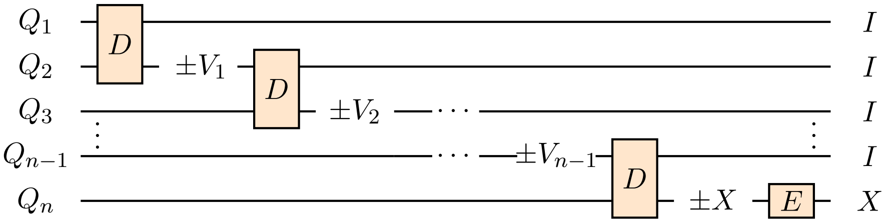
In the above diagram, the V_s are Pauli operators such that $V_s \in \{Z, XZ\}$ and are determined in the following way. By Proposition 4.1.8, if $P_m = \pm X, \pm Z$, there is a unique A gate A_g with green output such that $A_g \bullet P_m = \pm Z$. If $P_m = \pm XZ$, there is a unique A gate A_r with red output 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 red wire or $V_1 = \pm Z$ on a green wire. We will further use the actions described in Proposition 4.1.8 to move these Z or XZ Pauli operators up.

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 green, and if $V_2 = XZ$, the output wire is red. 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 green. Since we are constructing a normal circuit C such that $C \bullet P = Z \otimes I \otimes \ldots \otimes I$, which squares to the identity, we must have that the final B-gate is such that $B \bullet (P_1 \otimes \pm V_{m-1}) = Z \otimes I$, and hence ends on a green wire. Another reasoning for such is that since $P^2 = I$, there are evenly many indices i such that $P_i = XZ$, which are in effect canceled out by an application of B_8, switching back to Z along a green wire. 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.

Finally, note that every choice of gate is unique with respect to type and colour. If our normal form was constructed the same way with the absence of colours, uniqueness with respect to type would be sufficient for a unique Z-circuit, as typing and placement would be the only restrictions on circuit construction. Here with uniqueness with respect to type and colour, we must prove that no two Z-circuits describing an action as above can have different colour schemes, as with respect to colour each choice of gate is unique, making the overall Z-circuit unique. Thus we consider two Z-circuits C and D that correspond to the diagram above, such that $C \bullet P = D \bullet P = Z \otimes I \otimes \ldots \otimes I$, and prove they have the same colour 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 colour, 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 colour 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. These B_4 and B_8 gate represent the gate and actions, but with different colours of inputs and outputs. 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 colour. Note that if the input colour 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 green, and B_5, B_6, B_7, B_8 in the case of red. Since our output colour of A is given, and we must satisfy all needed equations of $B \bullet P_{m-j} \otimes V_j = V_{j+1} \otimes I$, 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 colouring scheme, ending in green, 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 colouring scheme. Since the colouring schemes must be the same, every local action must be the same unique gates chosen with respect to type. Hence these two Z-circuits are equal. This concludes uniqueness. □

Proposition 4.2.5. *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 $M \bullet Q = I \otimes \cdots \otimes I \otimes X$.*

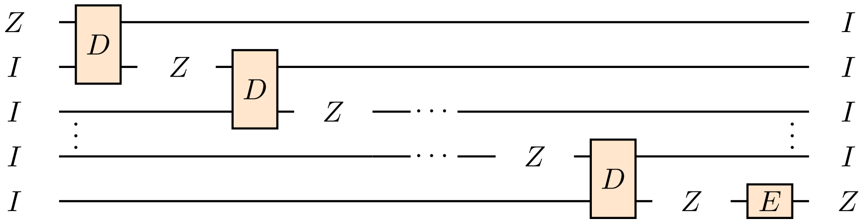
Proof. Since Q anticommutes with $Z \otimes I \otimes \cdots \otimes I$, we have $Q_1 = \pm XZ$ or $Q_1 = \pm X$. With this, we consider the diagram



where the V_s are Pauli operators such that $V_s \in \{X, XZ\}$, and are determined by the Q_i as in Proposition 4.2.4. By Proposition 4.1.8, the D gates push X and XZ gates down the qubits. This is again 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, and will leave us with $V_1 = X, XZ$. We continue the same process down to the bottom qubit. Again since $Q^2 = I$, by Proposition 2.1.4, 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 4.1.8, 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 type, the circuit is uniquely determined. □

Proposition 4.2.6. *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 4.1.8 with respect to the diagram below.



□

Proposition 4.2.7. *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 4.2.4, 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 4.2.5, 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 4.2.6, $ML \bullet P = M \bullet (L \bullet P) = M \bullet (Z \otimes I \otimes \cdots \otimes I) = I \otimes I \otimes \cdots \otimes Z$. 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 4.2.4, 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 4.2.5. □

Proposition 4.2.8. *Let $\phi : \mathcal{P}(n) \to \mathcal{P}(n)$ 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. For $n = 0$, we observe that 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 $n = 0$, all 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 $PQ = \phi^{-1}(I \otimes \ldots \otimes I \otimes ZX)$. Now note that since $I \otimes \ldots \otimes I \otimes Z$ and $I \otimes \ldots \otimes I \otimes X$ anticommute, so do P and Q. By Proposition 4.2.7, there exists a unique X-circuit M and a unique Z-circuit L such that

$$ML \bullet P = I \otimes \ldots \otimes I \otimes Z = \phi(P),$$

$$ML \bullet Q = I \otimes \ldots \otimes I \otimes X = \phi(Q), \text{ and}$$

$$ML \bullet PQ = (ML \bullet P)(ML \bullet Q) = I \otimes \cdots \otimes I \otimes ZX = \phi(PQ).$$

We now define a new automorphism $\phi' : \mathcal{P}(n) \to \mathcal{P}(n)$ 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

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

Let R be an $(n-1)$-qubit Pauli operator. We consider $\phi'(R \otimes I)$. Since $R \otimes I$ commutes with $I \otimes \cdots \otimes I \otimes Z, I \otimes \cdots \otimes I \otimes X$, and $I \otimes \cdots \otimes I \otimes ZX$, the same is true of $\phi'(R \otimes I)$. Hence $\phi'(R \otimes I) = V \otimes I$, where $V \in \mathcal{P}(n-1)$. It follows that there exists an automorphism $\phi'' : \mathcal{P}(n-1) \to \mathcal{P}(n-1)$ such that for every $R \in \mathcal{P}(n-1)$

$$\phi'(R \otimes I) = \phi''(R) \otimes I.$$

Since $I \otimes \cdots \otimes I \otimes Z, I \otimes \cdots \otimes I \otimes X$, and $I \otimes \cdots \otimes I \otimes ZX$ are all fixed points of ϕ', we then have $\phi' = \phi'' \otimes I$.

Now by our induction hypothesis, there exists a normal $n-1$ qubit Clifford circuit C' such that for all $R \in \mathcal{P}(n-1)$, $C' \bullet R = \phi''(R)$. Let $C = (C' \otimes I)ML$. Now 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.

Now, to prove uniqueness, suppose that D is another Clifford circuit in normal form such that $D \bullet U = \phi(U)$ for all $U \in \mathcal{P}(n)$. Then by our 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 4.2.7, $M' = M$ and $L' = L$. Then by the uniqueness of our 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. □

By the existence part of Proposition 4.2.8, every automorphism of the Pauli group can be represented as a circuit over H, Z, and C_Z. Thus all of these automorphisms are Clifford operators. Conversely, as remarked in Chapter 2, every Clifford operator is an automorphism of the Pauli group. Hence, Proposition 4.2.8 indeed establishes that every Clifford operator admits a unique normal form. We also note that this proves that the Clifford operators are indeed generated by $-1, Z, H$, and C_Z, a property that in prior was taken on faith. We can therefore count these normal forms in order to count Clifford operators.

Corollary 4.2.9. *The Clifford group on n qubits has exactly*

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

elements.

Proof. First note that by Definition 4.2.1, the A gate on the left of a normal form will determine the input colour of the first possible B gate. Then the choice of each B gate is dependent of the output colour of the previous gate.

There are four gates with a green input, B_1, B_2, B_3, and B_4, and four gates with a red input, 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 colour of the top wire matching that of the input colour of the bottom wire. The gates B_4 and B_8 on the other hand, swap between red and green. Thus, if the last chosen gate had a green output wire, 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 red output wire.

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 colour-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 red wire and we must choose oddly many colour-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 4.2.2, there are exactly $2 \cdot 4^{n-1}$ X-circuits on n qubits. Since there are exactly 2 scalars, by Definition 4.2.3, there are exactly

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

normal circuits. By Proposition 4.2.8, these are in bijection with the elements of the n-qubit Clifford group. □

Chapter 5

Relations for Real Clifford Circuits

In this chapter, we 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 our initial circuit into the normal form on its right.

5.1 Relations

Definition 5.1.1. The relations are given in Figures 5.1 to 5.9.

The relations are meant to cover all the cases where a gate appears to the left of a normal form. Because our 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 appear in Figures 5.1 to 5.9.

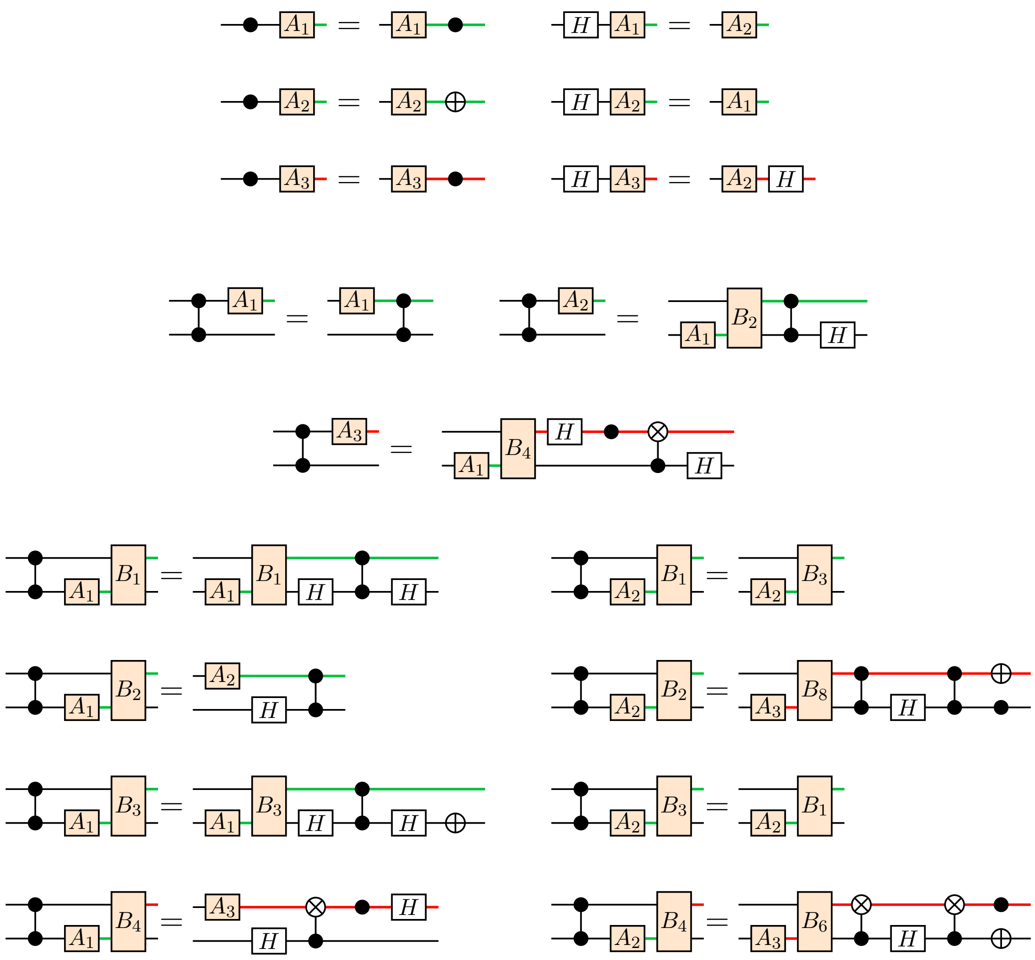

A_1 = A_1
H A_1 = A_2
A_2 = A_2
H A_2 = A_1
A_3 = A_3
H A_3 = A_2 H
A_1 = A_1
A_2 = A_1 B_2 H
A_3 = A_1 B_4 H H
A_1 B_1 = A_1 B_1 H H
A_2 B_1 = A_2 B_3
A_1 B_2 = A_2 H
A_2 B_2 = A_3 B_8 H
A_1 B_3 = A_1 B_3 H H
A_2 B_3 = A_2 B_1
A_1 B_4 = A_3 H H
A_2 B_4 = A_3 B_6 H

Figure 5.1: Rewrite rules for normal forms, part I.

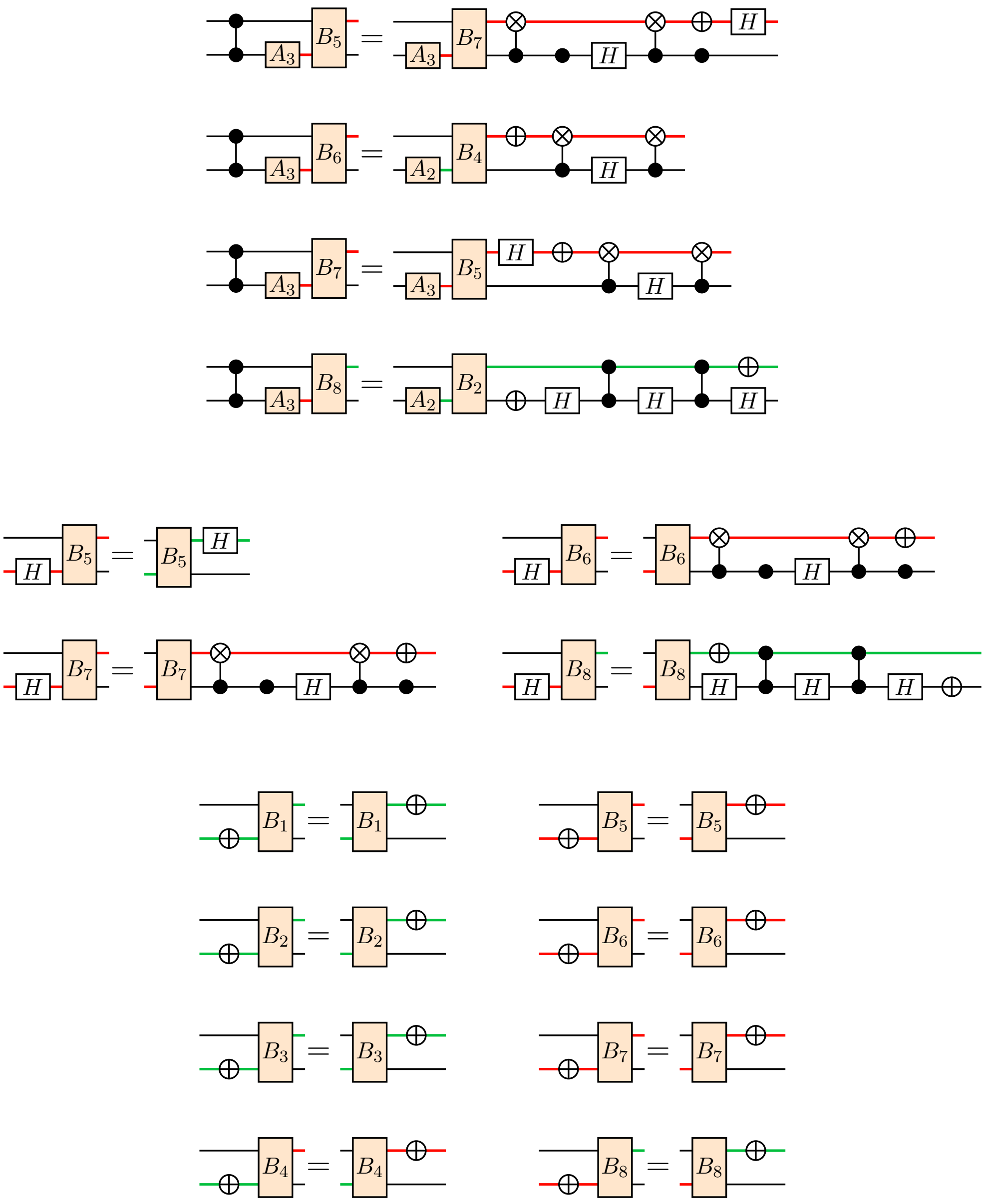


Figure 5.2: Rewrite rules for normal forms, part II.

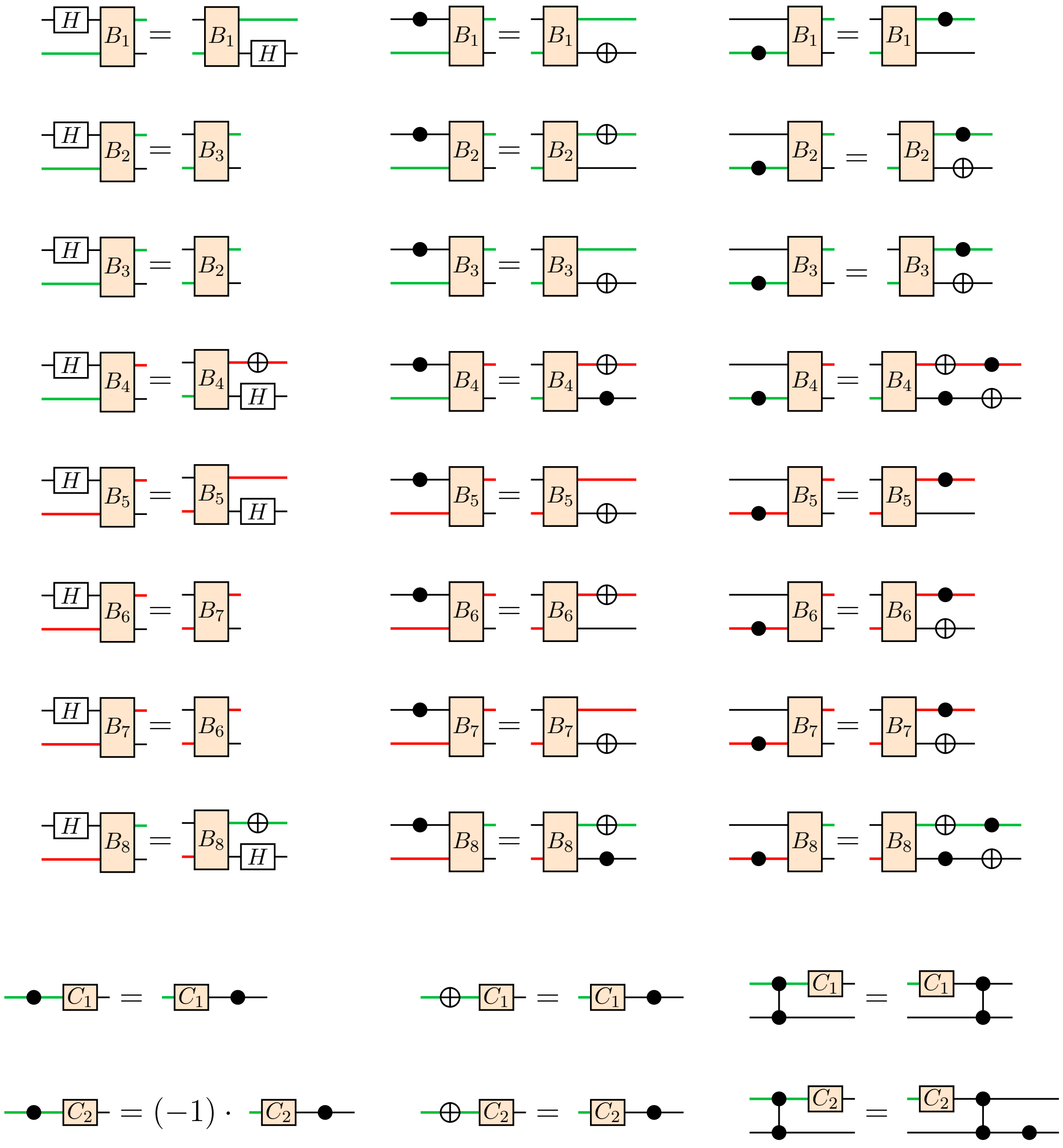


Figure 5.3: Rewrite rules for normal forms, part III.

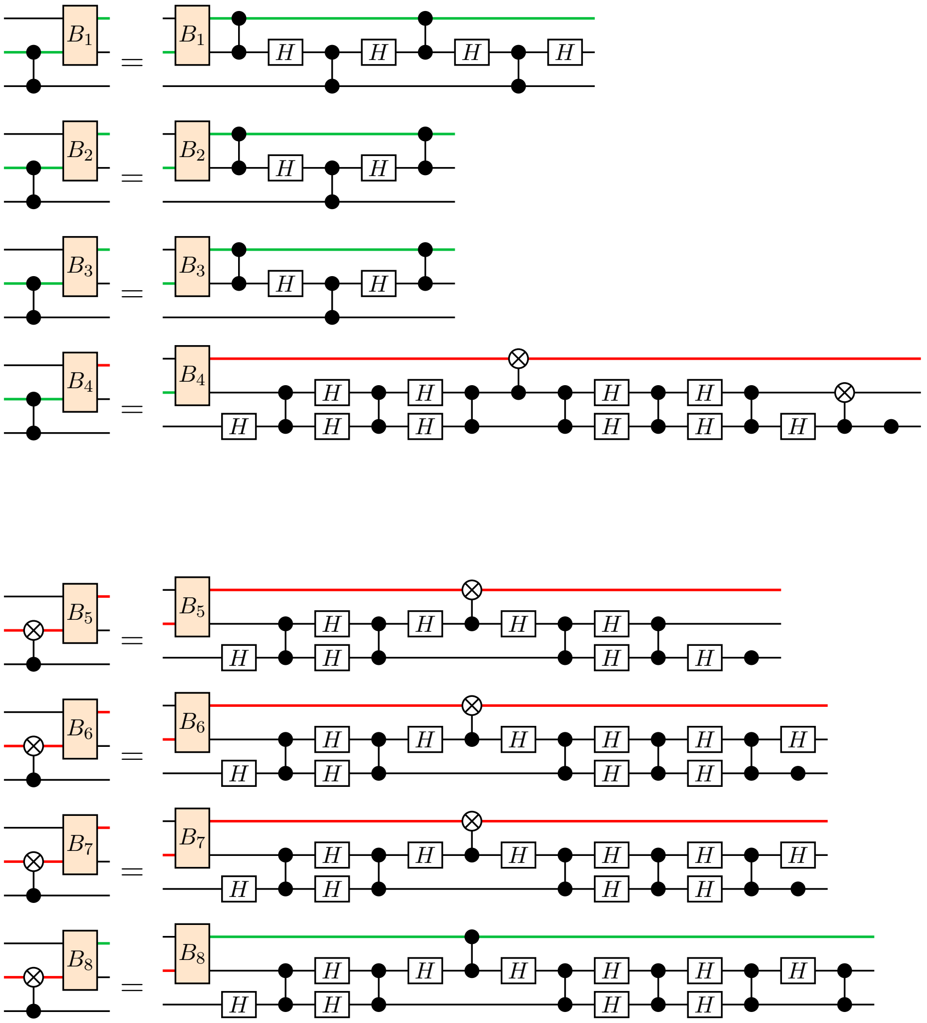

B1 = B1 H H H H
B2 = B2 H H
B3 = B3 H H
B4 = B4 H H H H H H H H H H
B5 = B5 H H H H H H H H
B6 = B6 H H H H H H H H H H
B7 = B7 H H H H H H H H H H
B8 = B8 H H H H H H H H H H

Figure 5.4: Rewrite rules for normal forms, part IV.

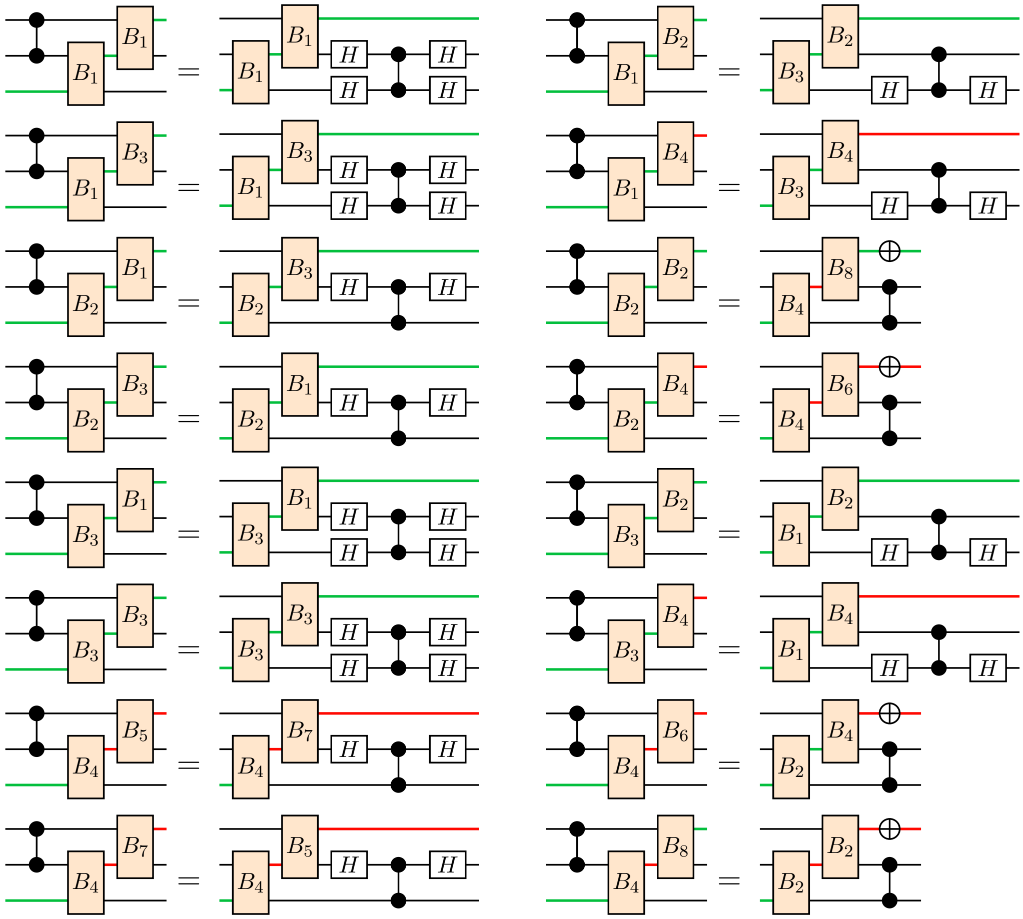

B_1 B_1 = B_1 B_1 H H H H
B_1 B_2 = B_3 B_2 H H
B_1 B_3 = B_1 B_3 H H H H
B_1 B_4 = B_3 B_4 H H
B_2 B_1 = B_2 B_3 H H
B_2 B_2 = B_4 B_8
B_2 B_3 = B_2 B_1 H H
B_2 B_4 = B_4 B_6
B_3 B_1 = B_3 B_1 H H H H
B_3 B_2 = B_1 B_2 H H
B_3 B_3 = B_3 B_3 H H H H
B_3 B_4 = B_1 B_4 H H
B_4 B_5 = B_4 B_7 H H
B_4 B_6 = B_2 B_4
B_4 B_7 = B_4 B_5 H H
B_4 B_8 = B_2 B_2

Figure 5.5: Rewrite rules for normal forms, part V.

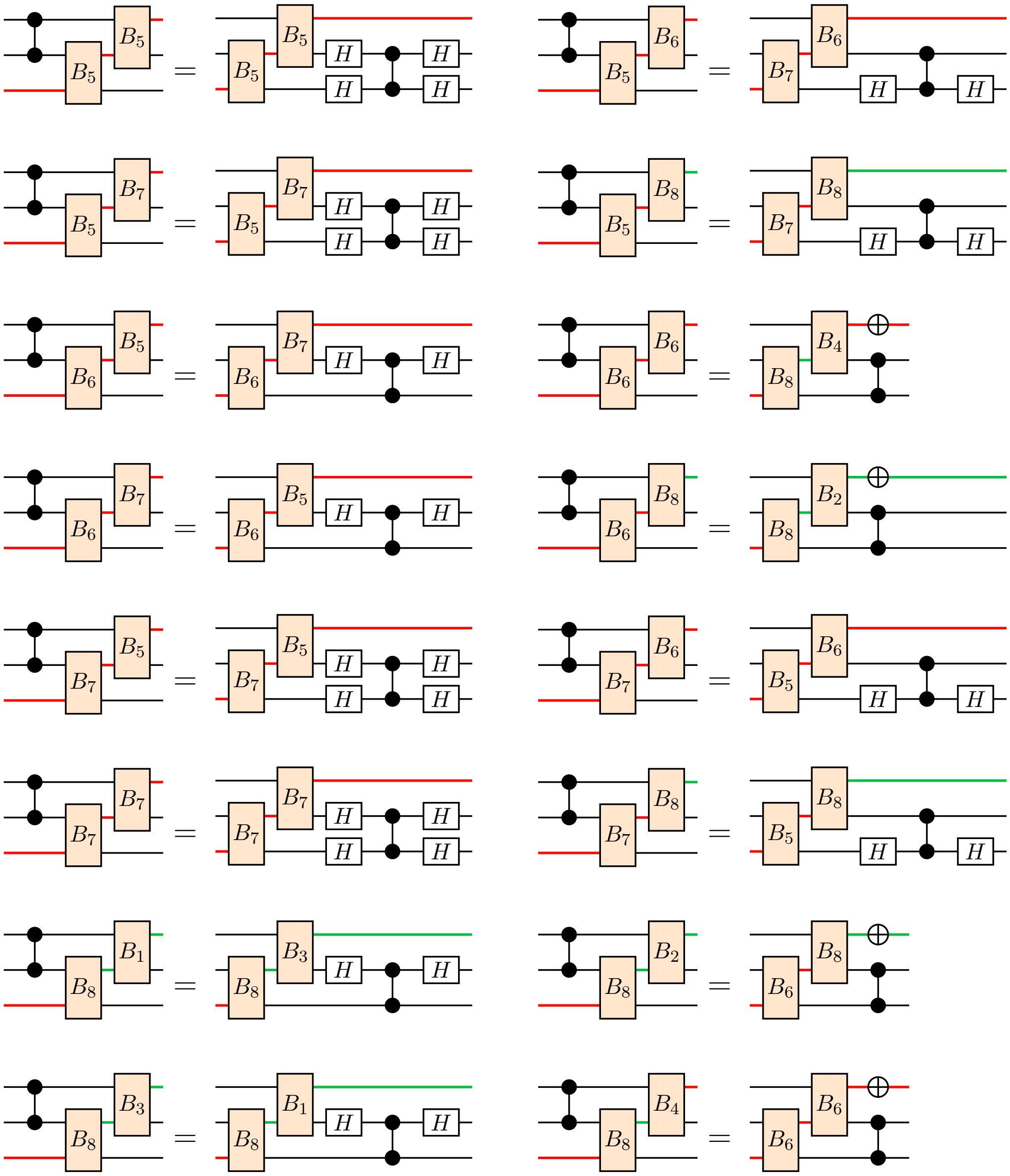

B_5 B_5 = B_5 B_5 H H H H
B_5 B_6 = B_7 B_6 H H
B_5 B_7 = B_5 B_7 H H H H
B_5 B_8 = B_7 B_8 H H
B_6 B_5 = B_6 B_7 H H
B_6 B_6 = B_8 B_4 ⊕
B_6 B_7 = B_6 B_5 H H
B_6 B_8 = B_8 B_2 ⊕
B_7 B_5 = B_7 B_5 H H H H
B_7 B_6 = B_5 B_6 H H
B_7 B_7 = B_7 B_7 H H H H
B_7 B_8 = B_5 B_8 H H
B_8 B_1 = B_8 B_3 H H
B_8 B_2 = B_6 B_8 ⊕
B_8 B_3 = B_8 B_1 H H
B_8 B_4 = B_6 B_6 ⊕

Figure 5.6: Rewrite rules for normal forms, part VI.

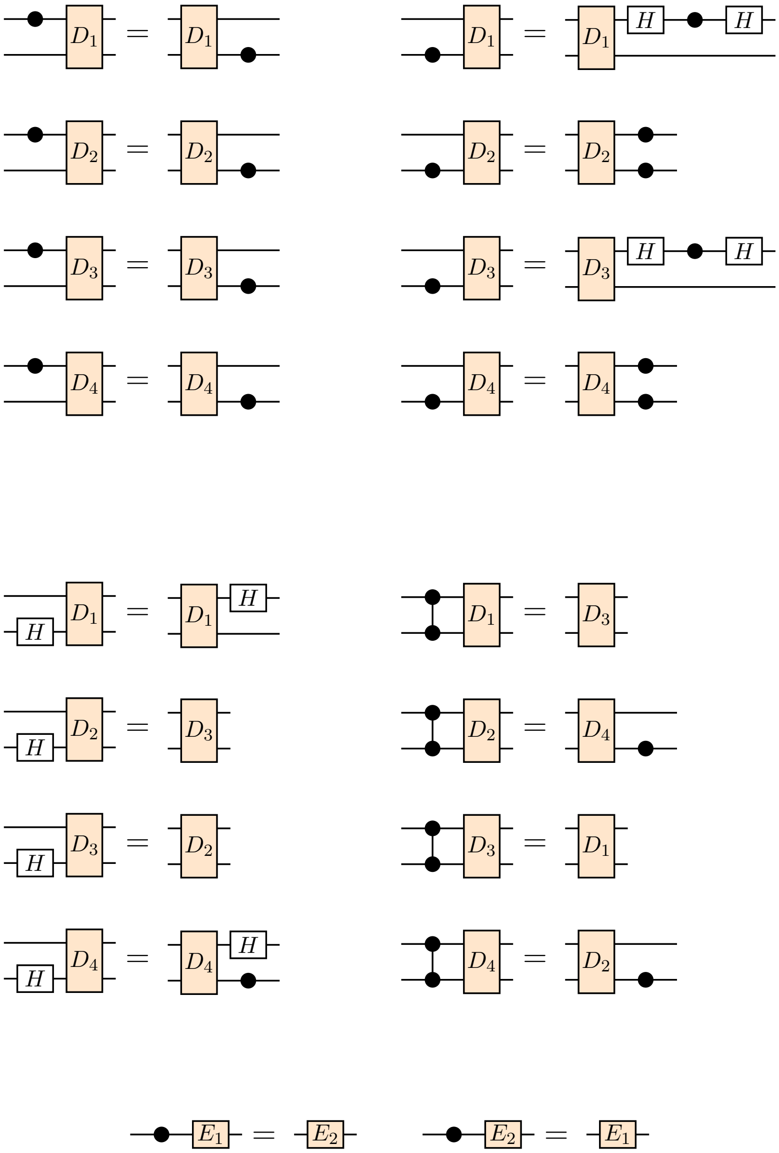


Figure 5.7: Rewrite rules for normal forms, part VII.

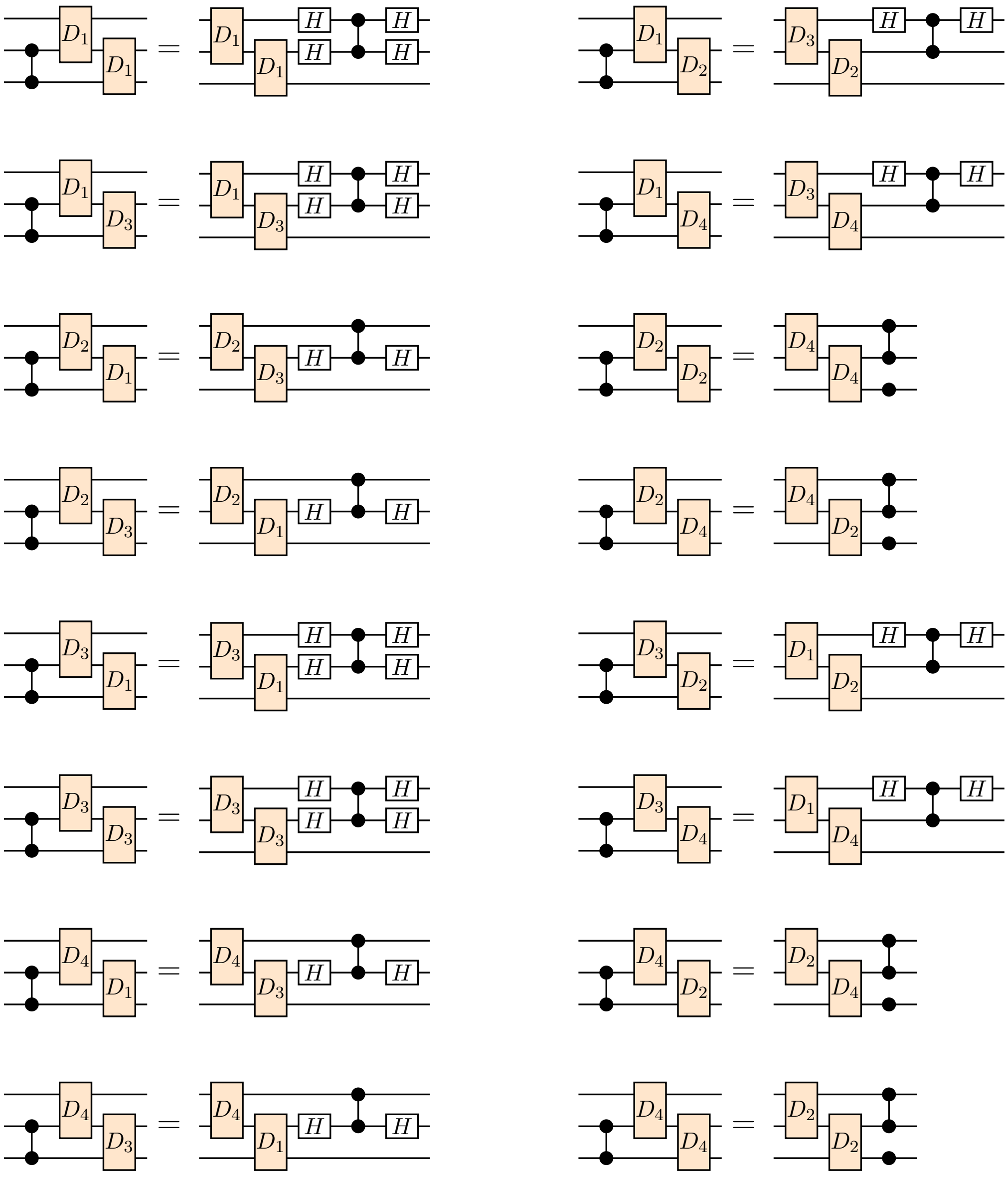

D_1 D_1 = D_1 D_1 H H H H
D_1 D_2 = D_3 D_2 H H
D_1 D_3 = D_1 D_3 H H H H
D_1 D_4 = D_3 D_4 H H
D_2 D_1 = D_2 D_3 H H
D_2 D_2 = D_4 D_4
D_2 D_3 = D_2 D_1 H H
D_2 D_4 = D_4 D_2
D_3 D_1 = D_3 D_1 H H H H
D_3 D_2 = D_1 D_2 H H
D_3 D_3 = D_3 D_3 H H H H
D_3 D_4 = D_1 D_4 H H
D_4 D_1 = D_4 D_3 H H
D_4 D_2 = D_2 D_4
D_4 D_3 = D_4 D_1 H H
D_4 D_4 = D_2 D_2

Figure 5.8: Rewrite rules for normal forms, part VIII.

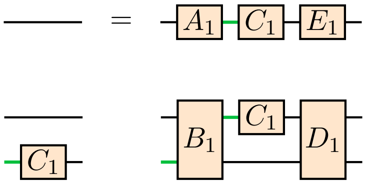
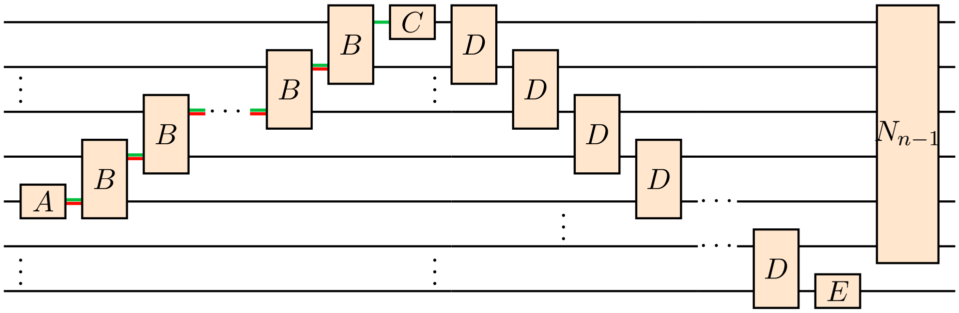


Figure 5.9: Rewrite rules for normal forms, part VIIII.

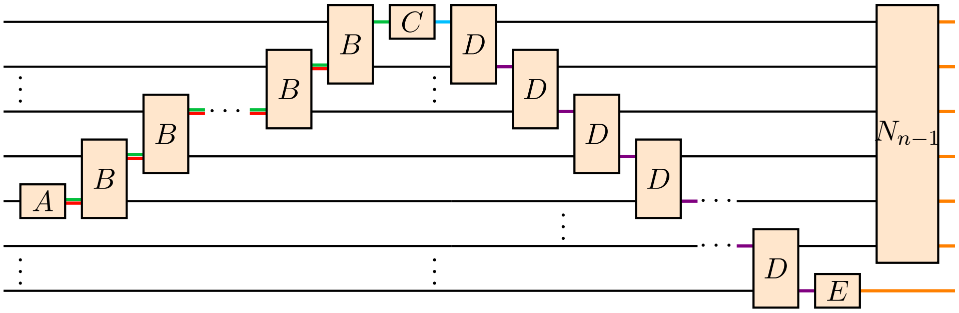
5.2 Normalization

We start by imposing additional colourings on normal circuits, which is convenient to describe our rewrite system. This further colouring is not used to restrict horizontal composition, but simply to aid in referring to specific parts of the circuit and will be used as a labelling to discuss the rewrite rules.

Definition 5.2.1. Consider an n-qubit normal circuit



where $N_{(n-1)}$ is recursively assumed to be an $(n-1)$-qubit normal form. We apply colours to specific wires to produce the following *coloured normal form*



where $N_{(n-1)}$ is recursively coloured in the same manner. Explicitly, the output wire of a C gate is blue, the top input wire of the first D gate is blue, the top input wire of all other D gates is purple, the bottom output wire of a D gate is purple, and the output wire of an E gate is orange.

Definition 5.2.2. *Dirty normal forms* are obtained from coloured normal forms by adding gates according to the following scheme.

- An H gate can be placed on a black or red wire.
- A Z gate can be placed on a black, green, red, blue, or purple wire.

- An X gate can be placed on a black, green, or red wire.
- A C_Z gate can be placed on adjacent wires, provided that the bottom wire is black, and the top wire is black, green, or blue.
- A C_{XZ} gate can be placed on adjacent wires, provided that the bottom wire is black, and the top wire is red.
- No gate can be placed on an orange wire.

When discussing dirty normal forms, we call H, Z, X, C_Z, and C_{XZ} gates *dirty*, while gates of type A, B, C, D, and E are called *clean*.

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

Lemma 5.2.3. *Any dirty normal form can be converted to its normal form by applying the relations of Figures 5.1 to 5.8 a finite number of times.*

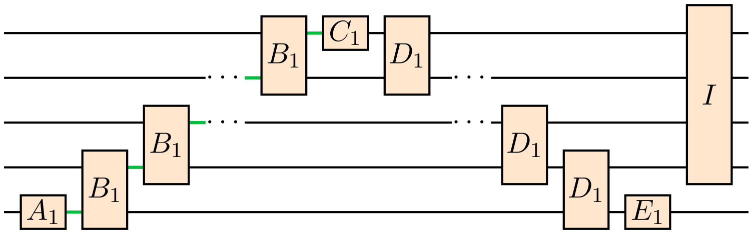
Proof. By inspection of Definition 5.2.2, it can be observed that every dirty gate occurs before a clean gate. Therefore, as long as there is still at least one dirty gate in the circuit, there must be a dirty gate that occurs immediately before a clean gate. The left-hand side of the relations in Figures 5.1 to 5.8 contain every possible case of a dirty gate occurring immediately before a clean gate. Thus as long as dirty gates are left, a rule can be applied. In fact, a tedious inspection of the figures shows that each rule takes a dirty normal form to another dirty normal form. It now remains to show that this procedure terminates in a finite number of steps. To this end we can associate a sequence of natural numbers to each dirty normal form in the following way. Suppose a dirty normal form has t clean gates, which can be indexed $1, \ldots, t$ as they appear from left to right. Then we can define a sequence $s = (s_1, s_2, \ldots, s_t)$ where s_i is the number of dirty gates that occur before the i-th clean gate. Now note that a left-to-right application of the rules decreases the sequence s in the lexicographic order. It is also clear from the rules that the length of this sequence might not be constant, but this is in fact bounded by the maximum possible number of clean gates in a circuit. In an n-qubit normal form, one can notice that this is represented by the sum

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

Because the set of all such sequences is well-ordered, this process terminates in a finite number of steps. □

Proposition 5.2.4. *Any Clifford circuit can be rewritten into its normal form using the relations in Figures 5.1 to 5.9.*

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

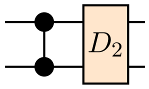


where I denotes the normal form for the identity on $n-1$ wires. Note that by applying the relation in Figure 5.9, we can rewrite the empty circuit on n wires into its normal form. Now consider a Clifford circuit C. By expanding the wires on the right of C into the normal form for the identity, we obtain a dirty normal form. We can then convert this dirty normal form into a normal form using Lemma 5.2.3, which completes the proof. □

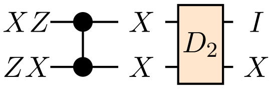
As an remark, this yields a presentation for the Clifford operators, with the only additional condition that we include the definition of our coloured gates in terms of its generators without colour, as relations in the system. Without doing this, we would, for example, be unable to prove that $A_1 A_1$ is equal to A_1. Another approach is to include the derived generators as their definition in terms of basic gates, and include all relations with the derived generators replaced as their definition in terms of basic gates. This set of relations will be complete, but complex, untidy, still redundant, and less magnifying to the structure of the Clifford group in its current state.

As another concluding remark, the reader may wonder how one would come to find such rewrite rules. We can consider this with the use of annotated circuits using the following example.

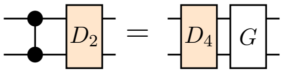
Imagine we wish to find the right hand side of the following rewrite rule.



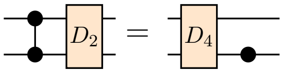
Recall that the intended action of the D_2 gate is $D_2 \bullet \pm X \otimes X = I \otimes \pm X$. We can place this on the right hand side of the annotated circuit, and back track it to the left by applying reverse conjugation of every gate. This shows us how the additional C_Z gate perturbs the local action.



We now receive $XZ \otimes ZX$ on the left hand side of the annotated circuit, which is also equal to $-(XZ \otimes XZ)$. This is the Pauli operator that this circuit takes to $I \otimes X$ under conjugation. We can notice that D_4 also describes this same action, that $D_4 \bullet (XZ \otimes Z) = I \otimes \pm X$. This gives us the D gate that we wish to have as the left gate in the right hand side of the equation, along with possibly some dirty gates to the right. As in we wish to complete the following rewrite rule.



Where G is a possible circuit to the right of D_4. We can solve for G by computing $D_2 \cdot C_Z \cdot D_4^\dagger$, and finding a circuit over the basic gates representing this operator. In this case we receive that $D_2 \cdot C_Z \cdot D_4^\dagger = I \otimes Z$, and hence we arrive at the following rewrite rule.



Chapter 6

Conclusion

In this thesis, we defined a normal form for real Clifford operators. We then introduced a rewrite system to transform any real Clifford circuit to its associated normal form, applying only a finite number of rules.

The most natural extension of this work is to find a more compact presentation. Indeed, our derived generators are highly redundant, especially once colours are forgotten. For example, the gates A_1 and A_3 represent the same operator: the identity. It would be preferable to re-express the relations solely in terms of the basic generators H, Z, and C_Z.

Further afield, it would be interesting to study universal extensions of the real Clifford gate set. One such extension is obtained by adding the Toffoli gate to the generators. The resulting gate set is universal for quantum computing [2, 14]. As a consequence, the group of n-qubit operators expressible as a circuit over this gate set is infinite (for $n \geq 3$) and the problem of finding relations for these circuits is presumably much harder.

Bibliography

[1] Scott Aaronson and Daniel Gottesman. Improved simulation of stabilizer circuits. *Physical Review A*, 70:052328, Nov 2004. Also available from `arXiv:quant-ph/0406196`.

[2] Dorit Aharonov. A simple proof that Toffoli and Hadamard are quantum universal. Available from `arXiv:quant-ph/0301040`, January 2003.

[3] Matthew Amy, Andrew N. Glaudell, and Neil J. Ross. Number-theoretic characterizations of some restricted Clifford+T circuits. *Quantum*, 4:252, April 2020. Also available from `arXiv:1908.06076`.

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

[5] Sergey Bravyi and Dmitri Maslov. Hadamard-free circuits expose the structure of the Clifford group. Available from `arXiv:2003.09412`, March 2020.

[6] Cole Comfort. Circuit Relations for Real Stabilizers: Towards TOF+H. Available from `arXiv:1904.10614`, Apr 2019.

[7] Daniel Gottesman. The Heisenberg representation of quantum computers. Available from `arXiv:quant-ph/9807006`, Jul 1998.

[8] A. K. Hashagen, S. T. Flammia, D. Gross, and J. J. Wallman. Real randomized benchmarking. *Quantum*, 2:85, 2018. Also available from `arXiv:1801.06121`.

[9] G. Nebe, E. M. Rains, and N. J. A. Sloane. Invariants of the Clifford Groups. *Designs, Codes and Cryptography*, 24, 2001. Also available from `arXiv:0001038`.

[10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge Series on Information and the Natural Sciences. Cambridge University Press, 2000.

[11] Narayanan Rengaswamy, Robert Calderbank, Swanand Kadhe, and Henry D. Pfister. Logical Clifford Synthesis for Stabilizer Codes. Available from `arXiv:1907.00310`, June 2019.

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

[13] Peter Selinger. Generators and relations for n-qubit Clifford operators. *Logical Methods in Computer Science*, 11(10):1–17, 2015. Also available from `arXiv:1310.6813`.

[14] Yaoyun Shi. Both Toffoli and controlled-NOT need little help to do universal quantum computing. *Quantum Information & Computation*, 3(1):84–92, 2003. Also available from `arXiv:quant-ph/0205115`.

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

[16] Renaud Vilmart. 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 '18, pages 313–344, 2018. Also available from `arXiv:1804.03084`.