A finite presentation of CNOT-dihedral operators

Matthew Amy
Institute for Quantum Computing and
David R. Cheriton School of Computer Science
University of Waterloo
Waterloo, Canada
matt.e.amy@gmail.com

Jianxin Chen
Institute for Advanced Computer Studies and
Joint Center for Quantum Information and Computer Science
University of Maryland
College Park, USA
chenkenshin@gmail.com

Neil J. Ross
neil.jr.ross@gmail.com

We give a finite presentation by generators and relations of the unitary operators expressible over the $\{\text{CNOT}, T, X\}$ gate set, also known as CNOT-dihedral operators. To this end, we introduce a notion of normal form for CNOT-dihedral circuits and prove that every CNOT-dihedral operator admits a unique normal form. Moreover, we show that in the presence of certain structural rules only finitely many circuit identities are required to reduce an arbitrary CNOT-dihedral circuit to its normal form.

By appropriately restricting our relations, we obtain a finite presentation of unitary operators expressible over the $\{\text{CNOT}, T\}$ gate set as a corollary.

1 Introduction

The *Clifford+T* gate set consists of the CNOT, Hadamard, and T gates [13]. This gate set has been the focus of recent efforts in the study of quantum circuits due to it's close connection to quantum fault tolerance. As a result, the theory of single-qubit Clifford+T circuits is now well-established [9, 12, 15]. In contrast, multi-qubit Clifford+T circuits are not very well understood, despite interesting results [6, 7]. The difficulties associated with multi-qubit circuits shifted emphasis from the full Clifford+T gate set to restricted classes of circuits. In particular, circuits over the $\{\text{CNOT}, T, X\}$ gate set, known as *CNOT-dihedral circuits of order 16*[1], and circuits over the $\{\text{CNOT}, T\}$ gate set, known as *CNOT+T circuits*, received significant attention. This led to a randomized benchmarking procedure for CNOT-dihedral circuits [5] as well as circuit optimizations [1, 2, 3] and improved distillation protocols [8] for CNOT+T circuits.

We give a finite presentation of CNOT-dihedral operators of order 16 in terms of generators and relations, inspired by similar results given for Clifford operators in [17] and certain classes of Boolean operators in [10]. First, we introduce normal forms for CNOT-dihedral circuits. Then, we prove that, in the presence of certain structural rules described in Section 2, a finite set of circuit equalities (the relations) suffices to reduce an arbitrary CNOT-dihedral circuit to its normal form. This shows that normal form representations of CNOT-dihedral operators always exist. Finally, we show that distinct normal forms represent distinct operators, which implies that normal form representations are unique. These results yield a presentation by generators and relations of the collection of CNOT-dihedral operators as a symmetric monoidal groupoid (see Section 2 for more details). By restricting the generators and relations from $\{\text{CNOT}, T, X\}$ to $\{\text{CNOT}, T\}$ and appropriately modifying the normal forms, we obtain an analogous presentation of the symmetric monoidal groupoid of CNOT+T operators.

Our contributions can be seen as the reformulation of prior results in the graphical language of quantum circuits. Indeed, it was shown in [5] that the group of n-qubit CNOT-dihedral operators is

[1] Circuits over the $\{\text{CNOT}, T, X\}$ are known as CNOT-dihedral circuits of order 16 because the group generated by T and X is isomorphic to the dihedral group of order 16 [5]. For brevity, we omit the order of the associated dihedral group and refer to $\{\text{CNOT}, T, X\}$ circuits as CNOT-dihedral circuits.

To appear in EPTCS.

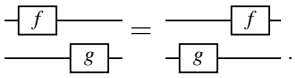
isomorphic to the semidirect product $M \rtimes GA(n,\mathbb{Z}_2)$ where M is some subgroup of $\mathbb{Z}_8^{2^n}$ and $GA(n,\mathbb{Z}_2)$ is the general affine group of order n over the two-element field. Independently, it was shown in [3] that the group of n-qubit CNOT+T operators is isomorphic to the semidirect product $M' \rtimes GL(n,\mathbb{Z}_2)$ where M' is some subgroup of $\mathbb{Z}_8^{2^n-1}$ and $GL(n,\mathbb{Z}_2)$ is the general linear group of order n over the two-element field. Using these characterizations, normal forms for CNOT-dihedral and CNOT+T circuits were discussed in [5] and [8] respectively. In contrast, we give finitely many relations which are sufficient to generate all circuit identities over $\{\text{CNOT}, T, X\}$. Circuit transformations can therefore take place at the circuit level which alleviates the need to translate to and from another formalism. Moreover, a self-contained equational theory of circuits is significantly easier to extend to new gate sets since all equations remain valid in the presence of additional gates.

The paper is organized as follows. In Section 2, we discuss preliminaries. In Section 3, we introduce generators and relations for CNOT-dihedral operators. In Section 4, we define normal forms for CNOT-dihedral circuits. In Section 5, we use the relations to show that every CNOT-dihedral operator admits a normal form. We show that distinct normal forms correspond to distinct operators in Section 6. Finally, we conclude and discuss generalizations and future work in Section 7.

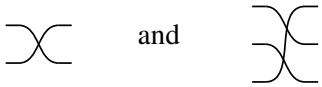
2 Preliminaries

The notion of *presentation* used here is similar to the usual one used in group theory but applied to a more general algebraic structure called a *symmetric monoidal groupoid*. Working with monoidal groupoids allows us to account for the usual horizontal composition of unitaries (matrix multiplication) as well as for their vertical composition (tensor product). In much the same way that a presentation of a group implicitly provides the relations axiomatizing the group operation, a presentation of a symmetric monoidal groupoid implicitly includes relations which account for the horizontal and vertical compositions and their interplay. We state these *structural rules* below in the graphical language of circuits. For further details about symmetric monoidal groupoids, the reader is encouraged to consult [11, 16].

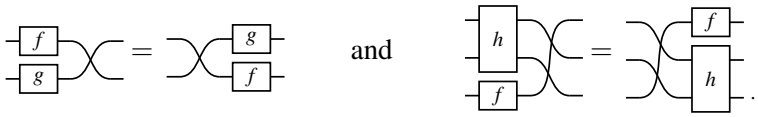
For every pair of operators f and g we have



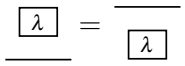
The above equality is known as the *bifunctorial law*. It implies that circuits on disjoint sets of qubits commute and guarantees that the collection of circuits under consideration forms a monoidal groupoid. One obtains a symmetric monoidal groupoid in the presence of a *symmetry* which is a family of self-inverse operators which act as generalized SWAP gates. For example, two instances of the symmetry are



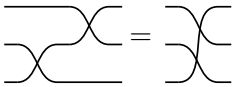
which have the effect of permuting the order of the qubits. Every instance of the symmetry satisfies a *naturality law*, which means that the symmetry has no effect beyond reordering the qubits. For the instances above, the naturality is expressed by the following circuit equalities, where f, g and h are arbitrary,



In particular, the following *spatial law* is a consequence of the naturality of the symmetry, where λ is an arbitrary scalar represented as a gate without input or output wires.



The symmetry also satisfies a property known as *coherence* which asserts that two circuits made of symmetries and implementing the same permutation of wires are equal, e.g.,

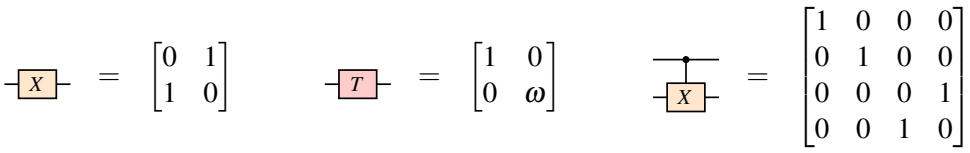


Using symmetric monoidal groupoids allows us to focus on properties that are specific to CNOT-dihedral operators and to abstract away generic properties of quantum circuits. In particular, the bifunctorial law and the existence of a symmetry satisfying naturality and coherence are assumed and needn't be explicitly included in the presentation.

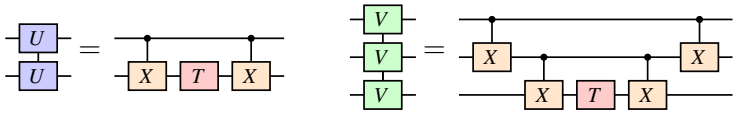
3 Generators and relations

We recall the definition of the standard generators for CNOT-dihedral operators and introduce two derived generators to streamline the presentation.

Definition 3.1. The *generators* are the scalar $\omega = e^{i\pi/4}$ and the gates X, T, and CNOT defined below.



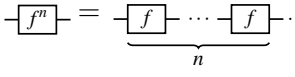
Definition 3.2. The *derived generators* are the gates U and V defined below.



In accordance with Section 2, we assume that all symmetries are given and we refer to any instance of the symmetry as a SWAP gate. Because they act as affine transformations on basis states, we refer to X, CNOT, and SWAP as *affine* gates and by extension to circuits using only affine gates as *affine circuits*. Similarly, we refer to ω, T, U, and V as *diagonal* gates and to circuits using only diagonal gates as *diagonal circuits*. If C is a CNOT-dihedral circuit, we write W_C to denote the operator represented by C. Note that if C is diagonal (resp. affine) circuit, then W_C is diagonal (resp. affine).

Definition 3.3. The *relations* are given in Fig. 1. We refer to relations R_1 through R_6 as *affine relations*, to relations R_7 through R_{10} as *diagonal relations*, and to relations R_{11} through R_{13} as *commutation relations*.

In Fig. 1 and throughout the rest of the paper, we use the following notational conventions. We place global phases (i.e., scalars) in front of circuits as in the right-hand side of R_{11}. Note that this is consistent with the spatial law. Gates labelled f^n for some integer $n \in \mathbb{N}$ denote the n-fold composition of f with itself, i.e.,



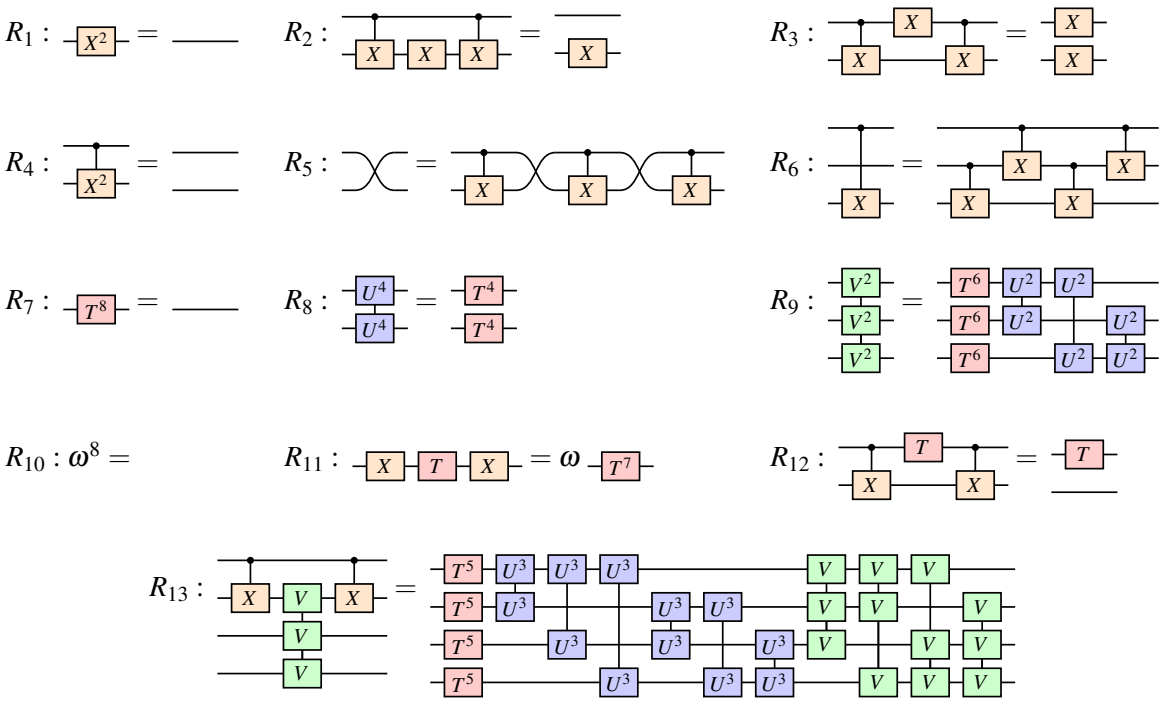
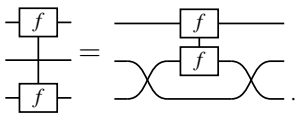


Figure 1: The relations. R_1 through R_6 are affine relations. R_7 through R_{10} are diagonal relations. R_{11} through R_{12} are commutation relations.

We call such a circuit an *f-block of degree n*. By extension, we write $\deg_f(C)$ for the maximum degree of the f-blocks that appear in a circuit C. We also use $\mathscr{T}$ and $\mathscr{X}$ to denote T and X blocks of arbitrary degrees. Gates applied to non-adjacent qubits, as in R_6, R_9, and R_{13}, are defined as adjacent-qubit gates on the top-most wires conjugated by SWAP gates, e.g.,



Because diagonal gates on non-adjacent qubits are diagonal in the computational basis we mildly abuse terminology and refer to circuits such as the right-hand side of R_{13} as diagonal circuits, even if they contain non-diagonal SWAP gates.

The 13 relations of Fig. 1 can be verified by explicit computation. However, it is more illuminating to use the formalism of *phase polynomials* introduced in [2].

Definition 3.4. Let $\oplus$ denote addition in $\mathbb{Z}_2$ and $\bar{x}$ denote the complement of x in $\mathbb{Z}_2$. A *literal* l is either a Boolean variable x or its inverse $\bar{x}$. A *term* over n Boolean variables is an expression of the form $l_1 \oplus \ldots \oplus l_n$ where each l_i is a literal.

Definition 3.5. The T, X, and CNOT gates act on basis states as $T|x\rangle = \omega^x |x\rangle$, $X|x\rangle = |\bar{x}\rangle$, and $\mathrm{CNOT}|x_1x_2\rangle = |x_1(x_1 \oplus x_2)\rangle$. It follows that the action of a CNOT-dihedral circuit C on an arbitrary basis state is given by

$$W_C|x_1x_2\cdots x_n\rangle = \omega^{p_C(x_1,x_2,\ldots,x_n)}|f_C(x_1,x_2,\ldots,x_n)\rangle, \tag{1}$$

where $f_C : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ is an affine reversible operator and $p_C : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is an expression of the form

$$p_C(x_1,\ldots,x_n) = \sum_k^{i=1} a_i \cdot g_i \tag{2}$$

for some $k \in \mathbb{N}$, some $a_i \in \mathbb{Z}_8$, and some terms g_i on no more than n variables. The expression in Eq. (1) is the *phase polynomial representation of C* and the one in Eq. (2) is the *phase polynomial associated with C*.

Note that the phase polynomials of Eq. (2) use mixed arithmetic: the "outside" sum is computed modulo 8 since $\omega^8 = 1$ while the "inside" sums are computed modulo 2. As with usual polynomials, we write 0 for the phase polynomial whose coefficients are all 0.

Phase polynomials are a concise representation of the action of CNOT-dihedral circuits on states and can be used to prove that two distinct circuits represent the same operator.

Proposition 3.6. *The relations of Fig. 1 are sound.*

Proof. We briefly discuss the case of R_{13}. Let C_L and C_R be the circuits on the left-hand side and right-hand side of R_{13} respectively. The phase polynomial representation of C_L is

$$W_{C_L}|x_1x_2x_3x_4\rangle = \omega^{x_1 \oplus x_2 \oplus x_3 \oplus x_4}|x_1x_2x_3x_4\rangle.$$

It can be verified (see, e.g., [3]) that, for any $x_1, x_2, x_3, x_4 \in \mathbb{Z}_2$,

$$x_1 \oplus x_2 \oplus x_3 \oplus x_4 = \sum_i 5x_i + \sum_{i<j} 3(x_i \oplus x_j) + \sum_{i<j<k} x_i \oplus x_j \oplus x_k \mod 8.$$

Hence

$$W_{C_L}|x_1x_2x_3x_4\rangle = \omega^{\sum_i 5x_i + \sum_{i<j} 3(x_i \oplus x_j) + \sum_{i<j<k} x_i \oplus x_j \oplus x_k}|x_1x_2x_3x_4\rangle$$

which is the phase polynomial representation of C_R so that $W_{C_L} = W_{C_R}$. □

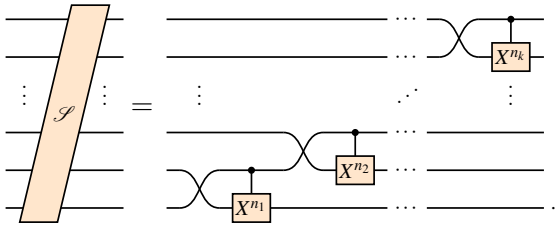
Remark 3.7. By considering only the T, U, V and CNOT gates as generators, and by omitting the relations R_1, R_2, R_3, R_{10}, and R_{11}, one obtains a presentation of the symmetric monoidal groupoid of CNOT+T operators.

Remark 3.8. It can be shown that the relations given in Fig. 1 are *independent*, in that it is not possible to derive one from the others. However, it is not currently known whether the relations are *minimal*, though we believe this to be the case.

4 Normal forms

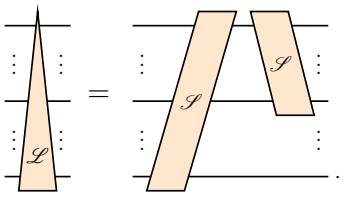
For each CNOT-dihedral operator W we choose a distinguished circuit which we call the *normal form* of W. We define normal forms for affine and diagonal operators independently. For affine operators, we use the normal forms introduced by Lafont in [10] which we recall here for completeness. In both cases, we introduce convenient shorthand prior to introducing normal forms.

Definition 4.1. *Ascending stairs* are circuits of the form



The identity circuit is the only ascending stair on a single qubit. *Descending stairs* are defined similarly.

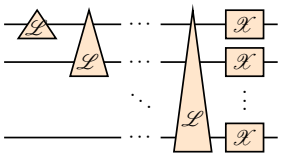
Definition 4.2. *Ladders* are circuits of the form



The identity circuit is the only ladder on a single qubit.

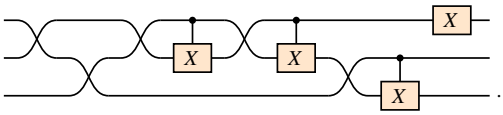
In Definition 4.2, the ascending stair rises from the bottom qubit to the top one. The descending stair, however, may or may not fall all the way to the bottom qubit.

Definition 4.3. An *affine normal form* is a circuit A of the form



such that $\deg_X(A) \in \mathbb{Z}_2$ and $\deg_{\mathrm{CNOT}}(A) \in \mathbb{Z}_2$.

Example 4.4. The affine operator defined by $|x_1x_2x_3\rangle \mapsto |(\overline{x_2 \oplus x_3})x_1(x_1 \oplus x_2)\rangle$, where $\oplus$ is addition in $\mathbb{Z}_2$ and $\bar{x}$ is the additive inverse of x in $\mathbb{Z}_2$, has the following affine normal form

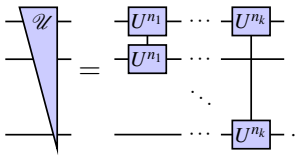


Remark 4.5. There are 2^{n-1} distinct stairs on n qubits and thus 2^n-1 distinct stairs on no more than n qubits. This implies that the number of n-qubit ladders is $2^{n-1}(2^n-1)$ which in turn implies that the number of distinct affine normal forms on n qubits is

$$2^n \cdot \prod_{i=1}^{n} 2^{i-1}(2^i-1) = 2^n \cdot \prod_{i=1}^{n} (2^n - 2^{i-1}). \tag{3}$$

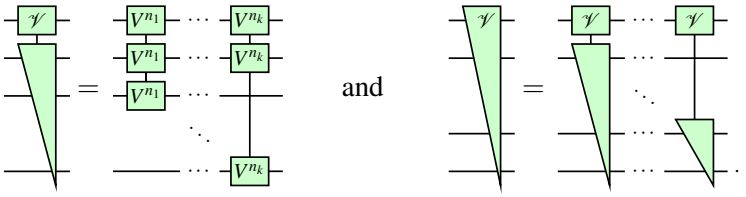
In Eq. (3), the prefactor of 2^n accounts for the layer of X gates which appear at the right of the normal form. Note that the expression in Eq. (3) coincides with the well-known formula for the cardinality of the general affine group of order n.

Definition 4.6. *U-triangles* are circuits of the form



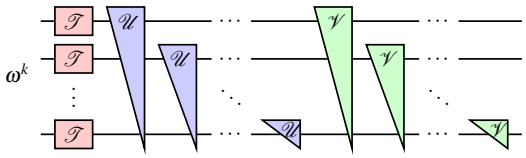
The identity circuit is the only U-triangle on a single qubit.

Definition 4.7. *V-trapezoids* and *V-triangles* are circuits of the form



The identity circuit is the only V-trapezoid or V-triangle on a single qubit. Similarly, the only V-triangle or V-trapezoid on two qubits is the identity circuit.

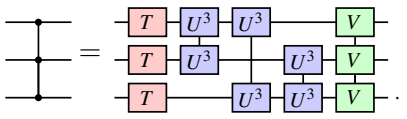
Definition 4.8. A *diagonal normal form* is a circuit D of the form



such that $k \in \mathbb{Z}_8$, $\deg_T(D) \in \mathbb{Z}_8$, $\deg_U(D) \in \mathbb{Z}_4$, and $\deg_V(D) \in \mathbb{Z}_2$.

The normal forms introduced in Definition 4.8 correspond to an ordering of the gates in a diagonal circuit according to which powers of ω appear first, followed by T, U, and V gates. The U gates are positioned in lexicographical order, with respect to the set of qubits they act on. The placement of V gates also follows the lexicographical ordering.

Example 4.9. The doubly-controlled Pauli Z gate, whose matrix is $\mathrm{diag}(1,1,1,1,1,1,1,-1)$, has the following diagonal normal form



Remark 4.10. In analogy with Remark 4.5, we note that there are $8 \cdot 8^{\binom{n}{1}} \cdot 4^{\binom{n}{2}} \cdot 2^{\binom{n}{3}}$ distinct diagonal normal forms.

Definition 4.11. A *normal form* is a circuit of the form DA where D is a diagonal normal form and A is an affine normal form.

Remark 4.12. It follows from Remark 4.5 and Remark 4.10, that the number of normal forms is

$$8 \cdot 8^{\binom{n}{1}} \cdot 4^{\binom{n}{2}} \cdot 2^{\binom{n}{3}} \cdot 2^n \cdot \prod_{i=1}^{n} (2^n - 2^{i-1}) = 2^{3+4\binom{n}{1}+2\binom{n}{2}+\binom{n}{3}} \prod_{i=1}^{n} (2^n - 2^{i-1}).$$

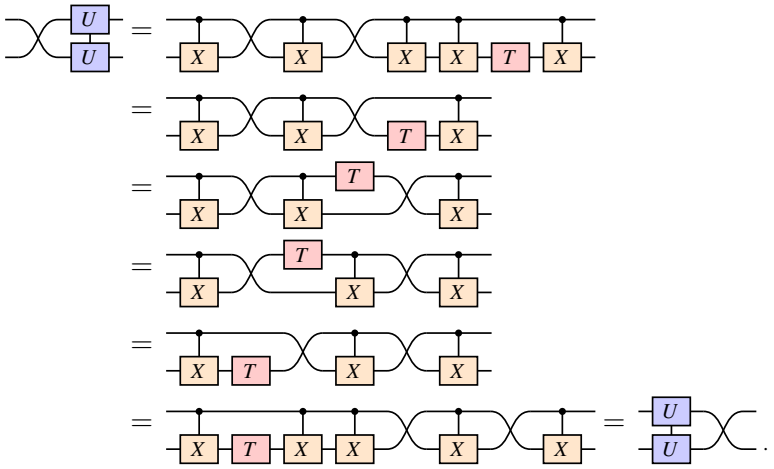
Remark 4.13. In the case of CNOT+T operators, the affine normal forms are replaced with *linear* normal forms which are obtained by removing the final column of X-blocks from the circuits of Definition 4.3. The CNOT+T diagonal normal forms are the scalar-free versions of the circuits of Definition 4.8.

5 Existence

In this section, we use the relations of Fig. 1, together with the structural rules of Section 2, to show that every CNOT-dihedral operator admits a normal form. For this, we first establish that every CNOT-dihedral circuit can be written as a diagonal circuit, followed by an affine one. We then consider the existence of diagonal and affine normal forms independently.

Lemma 5.1. *If C is a* CNOT*-dihedral circuit, then there exists a diagonal circuit D and an affine circuit A such that $C = DA$.*

Proof. It suffices to show that the lemma is true when C consists of a diagonal gate d appearing to the right of an affine gate a. If d and a act on distinct qubits, they can be commuted by the bifunctorial law. Likewise, if d is a power of ω, it can be commuted past a by the spatial law. This leaves the 25 cases listed in Fig. 2. The first six cases show how to commute an X gate past a diagonal gate. The next six cases show how to commute a CNOT gate past a diagonal gate. The last six cases show how to commute a SWAP gate past a diagonal gate. Verifying that each of these equations follows from the relations of Fig. 1 is a tedious but straightforward exercise. We give an example derivation, using the relations R_4, R_5, R_{12} and the bifunctorial law:



Note that in the last six cases of Fig. 2, we only consider the two-qubit SWAP, as opposed to more general SWAP gates. This is because coherence guarantees that an arbitrary SWAP can be expressed as a sequence of two-qubit SWAP gates. □

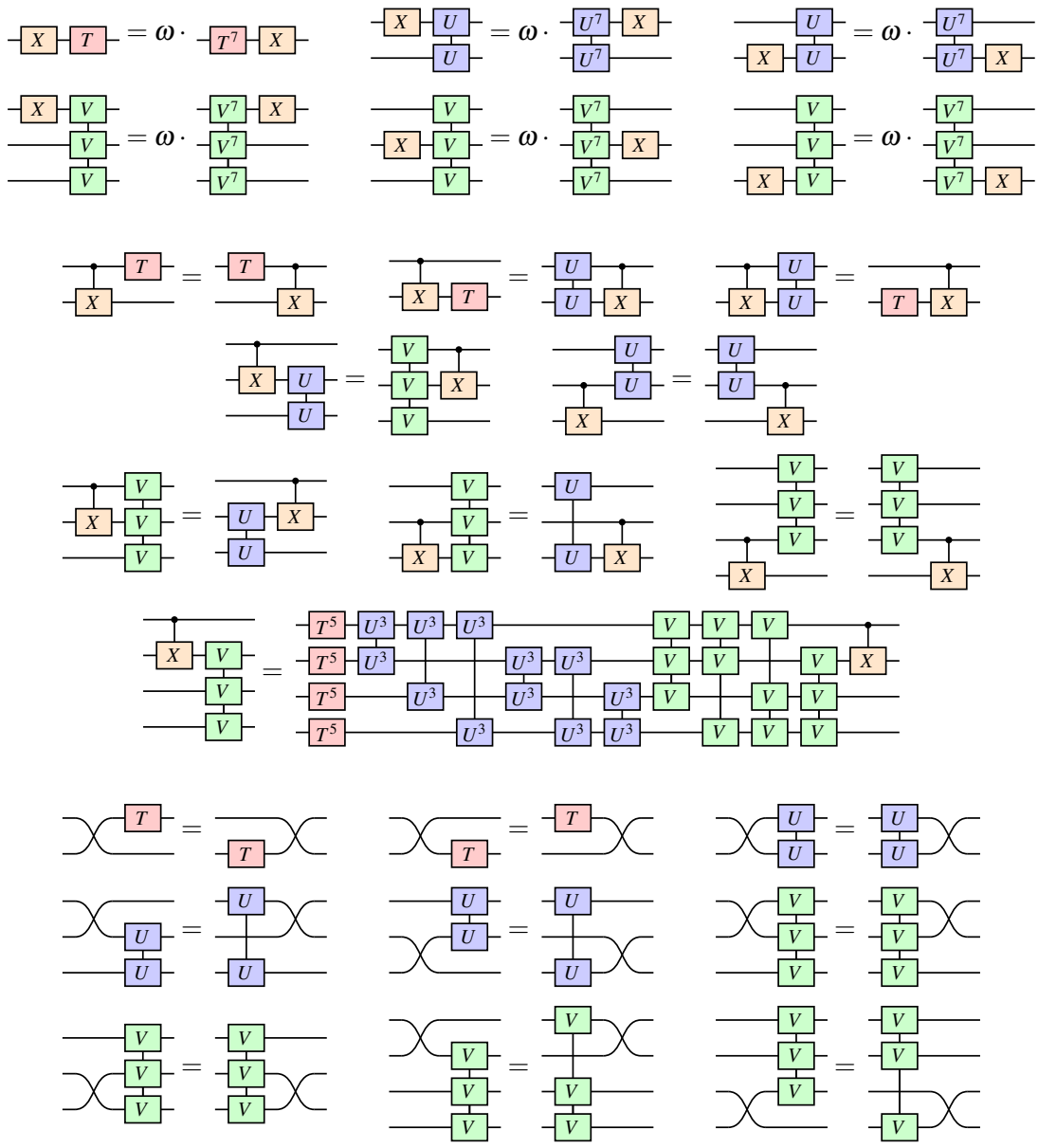
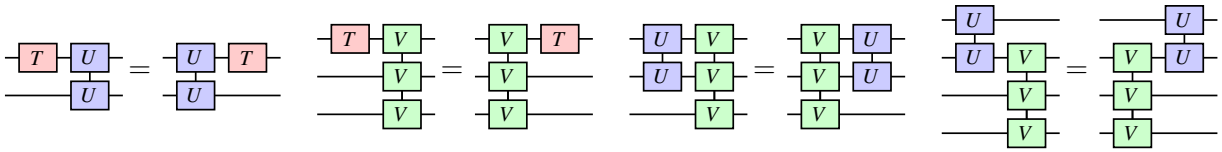


Figure 2: Derivable commutation rules.

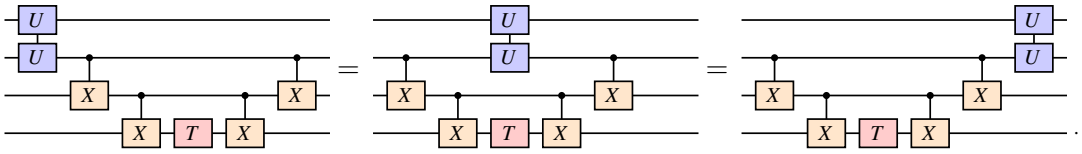
In order to prove that diagonal circuits admit a normal form, we start by showing that commutation rules between diagonal gates can be derived from the relations of Fig. 1.

Lemma 5.2. *Diagonal gates commute.*

Proof. As in the proof of Lemma 5.1, we only need to consider the cases where two diagonal gates act on at least one common qubit. Moreover, since U and V are symmetric with respect to the qubits they act on – i.e., they commute with SWAP gates as shown in Fig. 2 – we can further reduce the number of cases to consider to the following four.



Verifying that the above equations follow from the relations in Fig. 1 is another straightforward exercise. As an example, we derive the fourth equation below, using the definition of V as well as the fact that U commutes with the top wire of the CNOT gate, which is one of the derivable rules of Fig. 2.



□

Lemma 5.3. *Every diagonal circuit admits a normal form.*

Proof. Let C be an n-qubit diagonal circuit. By Lemma 5.2 the gates of C may be reordered into the form of Definition 4.8. It therefore suffices to bound the degree of T, U and V blocks by $7, 3$ and 1, respectively. We first reduce the degree of all V blocks modulo 2 by applying relation R_9. Note that the right hand side of R_9 contains no V gates and hence does not increase the degree of any V block. Once all V blocks have been reduced and gates have been reordered and combined appropriately, the U blocks may likewise be reduced modulo 4 via R_8. Again, the right hand side of R_8 contains only T gates and hence cannot increase the degree of any U or V blocks. Finally R_7 may be used to reduce the remaining T blocks to degree at most 7. □

Lemma 5.3 establishes that diagonal circuits admit normal forms. To prove that arbitrary CNOT-dihedral circuits can be normalized, we need an analogous result for affine circuits, which was proved by Lafont.

Lemma 5.4 (Lafont [10])**.** *Every affine circuit admits a unique normal form.*

Proposition 5.5. *Every* CNOT*-dihedral circuit admits a normal form.*

Proof. Let C be a CNOT-dihedral circuit. By Lemma 5.1, C can be written as a product DA where D is a diagonal circuit and and A is an affine circuit. By Lemma 5.3 and Lemma 5.4, D has a diagonal normal form D' and A has an affine normal form A'. The CNOT-dihedral circuit C therefore has normal form $C = D'A'$. □

Remark 5.6. The existence of CNOT+T normal forms can be established by reasoning as in Proposition 5.5.

6 Uniqueness

In this section, we show that normal forms are unique: distinct normal forms represent distinct operators. To this end, we use the formalism of phase polynomials introduced in Section 3.

The action of powers of the diagonal gates of definitions 3.1 and 3.2 on basis states are $\omega^k |x_1\rangle = \omega^k |x_1\rangle$, $T^k |x_1\rangle = \omega^{kx_1} |x_1\rangle$, $U^k |x_1x_2\rangle = \omega^{k(x_1 \oplus x_2)} |x_1x_2\rangle$, and $V^k |x_1x_2x_3\rangle = \omega^{k(x_1 \oplus x_2 \oplus x_3)} |x_1x_2x_3\rangle$. As a result, if D is a diagonal normal form on n qubits and $|x\rangle = |x_1 \ldots x_n\rangle$ is a basis state then $D|x\rangle = \omega^{p_D(x)} |x\rangle$, where $p_D(x)$ is an expression of the form

$$p_D(x) = a_0 + \sum_i a_i \cdot x_i + \sum_{i<j} b_{i,j} \cdot (x_i \oplus x_j) + \sum_{i<j<k} c_{i,j,k}(x_i \oplus x_j \oplus x_k) \tag{4}$$

with $a_i \in \mathbb{Z}_8$ for $i \in \{0, \ldots, n\}$, and $b_{i,j} \in \mathbb{Z}_4$, $c_{i,j,k} \in \mathbb{Z}_2$, for $i, j, k \in \{1, \ldots, n\}$. Further, every diagonal normal form corresponds to a unique expression of the form Eq. (4), as distinct powers of the T, U, and V gates contribute to distinct terms in the expression $p_D(x)$.

To prove that every diagonal normal form represents a distinct operator, it is helpful to express the mixed arithmetic polynomial of Eq. (4) as a *multilinear polynomial over* $\mathbb{Z}_8$, i.e., as a polynomial over $\mathbb{Z}_8$ that is linear in each of its variables [14].

Lemma 6.1. *If $p(x)$ and $p'(x)$ are phase polynomials as in Eq.* (4) *then there exists a multilinear polynomial $q(x)$ such that $p(y) - p'(y) = q(y)$ for all $y \in \mathbb{Z}_2^n$. Moreover, if $p(x) - p'(x) \neq 0$ then $q(x) \neq 0$.*

Proof. It can be verified by computation that the following equalities hold for $x_i, x_j, x_k \in \mathbb{Z}_2$

$$\begin{aligned} x_i \oplus x_j &= x_i + x_j - 2x_ix_j \\ x_i \oplus x_j \oplus x_k &= x_i + x_j + x_k - 2x_ix_j - 2x_ix_k - 2x_jx_k + 4x_ix_jx_k \end{aligned}$$

where $\oplus$ is addition in $\mathbb{Z}_2$ but all other arithmetic operations are performed in $\mathbb{Z}_8$. The first claim follows by applying the above equalities to $p(x) - p'(x)$. For the second claim, note that if $p(x) - p'(x) \neq 0$, we must have $a_i - a'_i \neq 0$ modulo 8, $b_{ij} - b'_{ij} \neq 0$ modulo 4, or $c_{ijk} - c'_{ijk} \neq 0$ modulo 2. If there exists i, j, k such that $c_{ijk} - c'_{ijk} \neq 0$ modulo 2, then $4(c_{ijk} - c'_{ijk}) \neq 0$ modulo 8. This implies that $q(x) \neq 0$, since $4(c_{ijk} - c'_{ijk})$ is the unique coefficient associated with the monomial $x_ix_jx_k$. If no such i, j, k exists, we can reason analogously with a coefficient of the form $b_{ij} - b'_{ij}$ or $a_i - a'_i$. □

Lemma 6.2. *Distinct diagonal normal forms represent distinct operators.*

Proof. Let D and D' be distinct diagonal normal forms with phase polynomials $p_D(x)$ and $p_{D'}(x)$ respectively. Since D and D' are normal, $p_D(x)$ and $p_{D'}(x)$ are of the form given in Eq. (4). And since D and D' are distinct, $p_D(x)$ and $p_{D'}(x)$ are likewise distinct, hence $p_D(x) - p_{D'}(x) \neq 0$. Lemma 6.1 therefore implies that there exists a nonzero multilinear polynomial $q(x)$ such that $p(y) - p'(y) = q(y)$ for all $y \in \mathbb{Z}_2^n$. Now let $d \cdot x_{i_1} \ldots x_{i_j}$ be a non-zero term in $q(x)$ of lowest degree and let $y \in \mathbb{Z}_2^n$ be the vector with 1's in the $i_1 \cdots i_j$ positions and 0's elsewhere. Then $q(y) = d \neq 0$, which implies that $p_D(y) - p_{D'}(y) \neq 0$ and therefore that $D|y\rangle \neq D'|y\rangle$. □

Lemma 6.2 establishes that diagonal normal forms are unique. To obtain the uniqueness of normal forms, we need a similar result for affine normal forms, which was proved by Lafont.

Lemma 6.3 (Lafont [10])**.** *Distinct affine normal forms represent distinct operators.*

Proposition 6.4. *Distinct normal forms represent distinct operators.*

Proof. Let C and C' be two normal forms. By definition, $C = DA$ and $C' = D'A'$ for some diagonal normal forms D, D' and some affine normal forms A, A'. Suppose that C and C' represent the same operator, i.e., that $W_C = W_{C'}$. Then $W_A W_D = W_{A'} W_{D'}$ and therefore $W_D = W_A^\dagger W_{A'} W_{D'}$. Since W_D and $W_{D'}$ are diagonal, $W_A^\dagger W_{A'}$ is a diagonal affine operator and thus $W_A^\dagger W_{A'} = 1$, or $W_A = W_{A'}$. This implies that $W_D = W_{D'}$. The result then follows from Lemma 6.2 and Lemma 6.3. □

By Proposition 6.4 and Proposition 5.5, there is a bijection between normal forms and CNOT-dihedral operators so that the number of n-qubit CNOT-dihedral operators is equal to the number of normal forms on n qubits that was computed in Remark 4.12.

Corollary 6.5. *The order of the group of* CNOT*-dihedral operators on n qubits is*

$$2^{3+4\binom{n}{1}+2\binom{n}{2}+\binom{n}{3}} \prod_{i=1}^{n} (2^n - 2^{i-1}).$$

Remark 6.6. The results of this section can be adapted to show that distinct CNOT+T normal forms represent distinct operators which then implies that the number of CNOT+T operators is

$$2^{3\binom{n}{1}+2\binom{n}{2}+\binom{n}{3}} \prod_{i=1}^{n} (2^n - 2^{i-1}).$$

Remark 6.7. The CNOT-dihedral operators are not universal for quantum computation. One obtains the universal Clifford+T gate set by adding the following Hadamard gate to the generators

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

Since the Hadamard gate is not diagonal, one may wonder to what extent it contributes to diagonal Clifford+T operators. We can use Corollary 6.5 to quantify this contribution. Indeed, there are

$$2^{3+4\binom{n}{1}+2\binom{n}{2}+\binom{n}{3}} = O(2^{n^3})$$

diagonal CNOT-dihedral operators on n qubits. In comparison, it is known from [6] that for $n \geq 4$, the number of ancilla-free diagonal Clifford+T operators on n qubits is $8^{2^n-1} = O(2^{2^n})$. The Hadamard gate therefore contributes to the vast majority of diagonal Clifford+T operators.

7 Conclusion

We gave a finite presentation of the symmetric monoidal groupoid of CNOT-dihedral operators of order 16. To this end, we introduced a notion of normal form for CNOT-dihedral circuits and showed that every CNOT-dihedral operator admits a unique normal form. As a corollary, we obtained a finite presentation of the symmetric monoidal groupoid of CNOT+T operators.

Although we have shied from doing so in this paper, our methods can be extended to CNOT-dihedral operators of higher order. For CNOT-dihedral operators of order $2n$, the generators ω and T are replaced with the scalar $\zeta_n = e^{2\pi i/n}$ and the phase gate

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

A presentation may then be obtained by modifying the diagonal relations appropriately. The results of [3] can be used to show that it is sufficient to include the relevant order relations (akin to R_7 and R_{10}) as well as relations reducing the order of multi-qubit phase gates (akin to R_8, R_9, and R_{13}). In the latter case, it suffices to introduce, for each 2^k dividing n, a relation between a $k+1$ qubit phase gate of order 2^k and a circuit using phase gates of smaller arity.

An avenue for future research is to find a rewrite system for CNOT-dihedral circuits. Indeed, Proposition 5.5 establishes that every CNOT-dihedral operator admits a normal form but it does not contain an algorithm to normalize an arbitrary CNOT-dihedral circuit via rewriting. This is because the proof of Proposition 5.5 appeals non-constructively to properties of the ambient symmetric monoidal structure. Recent results in rewriting theory address this problem [4] and might be used in order to obtain an effective presentation of CNOT-dihedral operators.

8 Acknowledgements

MA and NJR wish to thank the Banff International Research Station (BIRS) where the ideas presented here were first discussed. NJR wishes to thank Dmitri Maslov for sparking his interest in restricted Clifford+T circuits and to thank David Gosset and Yves Guiraud for stimulating discussions. MA, JC, and NJR thank Miriam Backens and anonymous referees for helpful comments on an earlier version of this paper.

MA is partially funded by Canada's NSERC. JC and NJR are funded by the Department of Defense.

References

[1] Matthew Amy, Dmitri Maslov & Michele Mosca (2014): *Polynomial-time T-depth Optimization of Clifford+T circuits via Matroid Partitioning*. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 33(10), pp. 1476–1489. Available at `http://arxiv.org/abs/1303.2042v2`.

[2] Matthew Amy, Dmitri Maslov, Michele Mosca & Martin Roetteler (2013): *A Meet-in-the-Middle Algorithm for Fast Synthesis of Depth-Optimal Quantum Circuits*. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 32(6), pp. 818–830. Available at `http://arxiv.org/abs/1206.0758`.

[3] Matthew Amy & Michele Mosca (2016): *T-count optimization and Reed-Muller codes*. Available at `http://arxiv.org/abs/1601.07363`.

[4] Filippo Bonchi, Fabio Gadducci, Aleks Kissinger, PawełSobociński & Fabio Zanasi (2016): *Rewriting Modulo Symmetric Monoidal Structure*. In: *Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS '16, ACM, New York, NY, USA, pp. 710–719, doi:`http://dx.doi.org/10.1145/2933575.2935316`. Available at `http://arxiv.org/abs/1602.06771`.

[5] Andrew W Cross, Easwar Magesan, Lev S Bishop, John A Smolin & Jay M Gambetta (2016): *Scalable randomised benchmarking of non-Clifford gates*. *npj Quantum Information* 2. Available at `http://arxiv.org/abs/1510.02720`.

[6] Brett Giles & Peter Selinger (2013): *Exact synthesis of multiqubit Clifford+T circuits*. *Physical Review A* 87, p. 032332. Available at `http://arxiv.org/abs/1212.0506`.

[7] David Gosset, Vadym Kliuchnikov, Michele Mosca & Vincent Russo (2014): *An Algorithm for the T-count*. *Quantum Information & Computation* 14(15-16), pp. 1261–1276. Available at `http://arxiv.org/abs/1308.4134`.

[8] Mark Howard & Earl T. Campbell (2016): *A unified framework for magic state distillation and multi-qubit gate-synthesis with reduced resource cost*. Available at `http://arxiv.org/abs/1606.01904`.

[9] Vadym Kliuchnikov, Dmitri Maslov & Michele Mosca (2013): *Fast and efficient exact synthesis of single qubit unitaries generated by Clifford and T gates*. Quantum Information & Computation 13(7–8), pp. 607–630. Available at http://arxiv.org/abs/1206.5236v4.

[10] Yves Lafont (2003): *Towards an Algebraic Theory of Boolean Circuits*. Journal of Pure and Applied Algebra 184(2-3), pp. 257–310. Available at http://iml.univ-mrs.fr/~lafont/pub/circuits.pdf.

[11] S.M. Lane (1998): *Categories for the Working Mathematician*. Graduate Texts in Mathematics, Springer, New York, NY, USA.

[12] Ken Matsumoto & Kazuyuki Amano (2008): *Representation of Quantum Circuits with Clifford and $\pi/8$ Gates*. Available at http://arxiv.org/abs/0806.3834.

[13] Michael A. Nielsen & Isaac L. Chuang (2002): *Quantum Computation and Quantum Information*. Cambridge University Press, New York, NY, USA.

[14] Ryan O'Donnell (2014): *Analysis of Boolean Functions*. Cambridge University Press, New York, NY, USA.

[15] Neil J. Ross & Peter Selinger (2016): *Optimal ancilla-free Clifford+T approximation of* z*-rotations*. Quantum Information & Computation 16(11&12), pp. 901–953. Available at http://arxiv.org/abs/1403.2975.

[16] Peter Selinger (2011): *A Survey of Graphical Languages for Monoidal Categories*. In Bob Coecke, editor: New Structures for Physics, Lecture Notes in Physics 813, Springer, pp. 289–355, doi:http://dx.doi.org/10.1007/978-3-642-12821-9_4. Available at http://arxiv.org/abs/0908.3347.

[17] Peter Selinger (2015): *Generators and Relations for n-Qubit Clifford Operators*. Logical Methods in Computer Science 11(10), pp. 1–17. Available at http://arxiv.org/abs/1310.6813v3.