ON THE STRUCTURE OF THE CNOT-DIHEDRAL GROUP

SHELLY GARION AND ANDREW W. CROSS

Abstract. In this note we present explicit canonical forms for all the elements in the 2-qubit CNOT-Dihedral group, with minimal numbers of controlled-$S$ ($CS$) and controlled-$X$ ($CX$) gates, using the generating set of quantum gates [$X, T, CX, CS$]. We provide an efficient algorithm, with a sharp bound, to successively construct the n-qubit CNOT-Dihedral group, asserting an optimal number of controlled-$X$ ($CX$) gates. These results are needed to estimate gate errors via non-Clifford randomized benchmarking and may have further applications to circuit optimization over fault-tolerant gate sets.

1. Introduction

Randomized Benchmarking (RB) [20, 21, 22] is a well-known algorithm that provides an efficient and reliable experimental estimation of an average error-rate for a set of quantum gate operations, by running sequences of random gates from the Clifford group that should return the qubits to the initial state. RB techniques are scalable to many qubits since the Clifford group can be efficiently simulated (in polynomial time) using a classical computer [1, 7, 16, 24]. RB can also be used to characterize specific interleaved gate errors [23], coherence errors [25, 29] and leakage errors [30]. RB methods were generalized to certain single qubit non-Clifford gates, like the $T$-gate [11]. In [12] the authors presented a scalable RB procedure to benchmark important non-Clifford gates, such as the controlled-$S$ gate and controlled-controlled-$Z$ gate, which belong to a certain group called the CNOT-Dihedral group.

Certain CNOT-Dihedral groups have two key characteristics in common with the Clifford group. First, these groups have elements with concise representations that can be efficiently manipulated [2, 12]. Second, these groups are the set of transversal (fault-tolerant) gates for certain quantum error-correcting codes [5, 6, 17, 19, 32]. Since the Clifford gates together with the $T$ gate form a universal set of gates, there are many papers aiming to optimize the number of $T$ gates [10, 15, 18, 27, 28]. In addition, as the Clifford gate together with the Controlled-$S$ ($CS$) gate also forms a universal set of gates, an algorithm has recently been introduced to construct a circuit with an optimal number of $CS$ gates given a two-qubit Clifford+$CS$ operator [14]. Additional methods aim to minimize the count of controlled-$X$ gates in universal circuits [31], and in particular, in controlled-$X$-phase circuits [3, 26].

It is therefore important to efficiently present the elements in the CNOT-Dihedral group using a minimal number of physical basic gates, in particular, two-qubit gates like the controlled-$X$ and controlled-$S$ gates.

Recall that $X$ is the Pauli gate defined as

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
Fix an integer $m$ and define
\[ T(m) = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/m} \end{pmatrix} \]

By abuse of notation we will denote $T = T(m)$, although the $T$ gate is usually defined as $T(8) = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/8} \end{pmatrix}$.

The 1-qubit Dihedral group is generated by the $X$ and $T = T(m)$ gates (up to a global phase) and contains $2m$ elements,

\[
\langle X, T \rangle / \langle \lambda I : \lambda \in \mathbb{C} \rangle = \{ X^l T^k : l \in \{0,1\}, k \in \{0, \ldots, m-1\} \}.
\]

More generally, the CNOT-Dihedral group on $n$ qubits $G = G(m)$ is generated by the gates $X$, $T = T(m)$ and controlled-$X$ ($CX$), up to a global phase (see [12] for details),

\[
G = G(m) = \langle X_i, T_i, CX_{i,j} : i, j \in \{0, \ldots, n-1\} \rangle / \langle \lambda I : \lambda \in \mathbb{C} \rangle,
\]

where the controlled-$X$ ($CX$) gate is defined as

\[
CX = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},
\]

When $m$ is not a power of 2, the group $G = G(m)$ has double exponential order as a function of the number of qubits $n$. In the special case when $m$ is a power of two, the group is only exponentially large and we can represent its elements efficiently (see [12]). Elements of $G(m)$ belong to level $\log_2 m$ of the Clifford hierarchy when $m$ is a power of two [17, 19] and this is related to the fact that they are the transversal gates of certain $m$-dimensional quantum codes [5].

Again, by abuse of notation we denote $S = T^2 = T(m)^2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{4\pi i/m} \end{pmatrix}$, although the $S$ gate is usually defined as $T(8)^2 = T(4) = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$. Observe that $S$ has order $m/2$ if $m$ is even, and order $m$ if $m$ is odd, namely, $S$ has order $m/d$ where $d = \gcd(m, 2)$.

The controlled-$S$ ($CS$) gate belongs to $G$ and can be written as

\[
CS_{i,j} = T_i T_j \cdot CX_{i,j} \cdot I_i T_j^\dagger \cdot CX_{i,j} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{4\pi i/m} \end{pmatrix},
\]

where $T_i T_j$ means the tensor product $T_i \otimes T_j$. In the case where $m = 8$, the $CS$ gate is less expensive to physically implement than one $CX$ gate\footnote{Up to single-qubit rotations, the gate is equivalent to controlled-$\sqrt{X}$ gate, so it can be implemented by evolving for half the duration of a controlled-$X$ gate.} which makes it an alternative to $CX$ for improving circuit decompositions.

We focus on the case where $n = 2$ and provide in the following two Theorems canonical forms for all the elements in the 2-qubit CNOT-Dihedral group, such that the numbers of $CS$ and $CX$ gates are optimal. This is analogous to the description in [13] of the elements in the 2-qubit Clifford group.
Theorem 1. Consider the CS-Dihedral subgroup on 2-qubits, namely the 2-qubit group generated by the gates $X$, $T = T(0)$ and CS (Controlled-S), where $S = T^2$, and denote $d = \gcd(m, 2)$. Then this group has $\frac{4m^3}{d} = \frac{m}{d}(2m)^2$ elements of the following form:

$$U = CS_{0,1}^e \cdot X_0^k X_1^l \cdot T_0^j T_1^{l'}$$

where $k, k' \in \{0, 1\}, l, l' \in \{0, \ldots, m-1\}, e \in \{0, 1, \ldots, m/d-1\} = \{0, \pm 1, \pm 2, \ldots, \pm \lfloor \frac{m-d}{2d} \rfloor\}$.

Theorem 2. Let $G$ be the 2-qubit CNOT-Dihedral group generated by the gates $X$, $T = T(0)$, CX and CS, where $S = T^2$, and denote $d = \gcd(m, 2)$. Then this group has $24 \cdot m^3/d$ elements, divided into the following four classes.

1. The first class is the CS-Dihedral subgroup described in Theorem 1 and has $\frac{4m^3}{d}$ elements, that can be written with no CX gates.

2. The second class, called the CX-like class, consists of $\frac{8m^3}{d} = 2 \cdot \frac{m}{d} \cdot (2m)^2$ elements, and contains all the elements of the following form, which require exactly one CX gate.

$$U = X_0^k X_1^l \cdot T_0^j T_1^{l'} \cdot CX_{i,j} \cdot I_i T_j^e$$

3. The third class, called the Double-CX-like class, consists of $\frac{8m^3}{d} = 2 \cdot \frac{m}{d} \cdot (2m)^2$ elements, and contains all the elements of the following form, which require exactly two CX gates.

$$U = X_0^k X_1^l \cdot T_0^j T_1^{l'} \cdot CX_{i,j} \cdot CX_{i', j} \cdot I_i T_j^{e'}$$

4. The forth class, called the Triple-CX-like class, consists of $\frac{8m^3}{d} = \frac{m}{d} \cdot (2m)^2$ elements, and contains all the elements of the following form, which require exactly three CX gates.

$$U = X_0^k X_1^l \cdot T_0^j T_1^{l'} \cdot CX_{0,1} \cdot CX_{1,0} \cdot I_0 T_1^e \cdot CX_{0,1}$$

where $k, k' \in \{0, 1\}, l, l' \in \{0, \ldots, m\}, e \in \{0, \ldots, m/d-1\}$ and $(i, j) \in \{(0, 1), (1, 0)\}$.

The following key lemma follows [8], and provides an efficient algorithm to generate the $n$-qubit CNOT-Dihedral group. Case (1) of this Lemma shows that one can successively construct the CNOT-Dihedral group asserting an optimal number of CX gates, with a sharp bound on the space to search these group elements (see Remark 4). Moreover, one can also use the “meet in the middle” algorithm of [4] to synthesize gate sequences for the non-Clifford RB.

Lemma 3 (key lemma). Let $G = G(m)$ be the CNOT-Dihedral group on $n$ qubits, and denote $d = \gcd(m, 2)$.

1. Let $F(r)$ be the subset of operators implementable by a circuit with $r$ CX gates (and any number of $X$ and $T$ gates). Suppose $U$ is in $F(r+1)$, then

$$U = I_i T_i^l \cdot CX_{i,j} \cdot U'$$

for some $U' \in F(r)$, $i \neq j$, $i, j \in \{0, \ldots, n-1\}$, $l \in \{0, \ldots, m/d - 1\}$. In particular, $|F(r+1)| \leq \frac{m(n^2 - n)}{d} |F(r)|$.
(2) Let $H(r)$ be the subset of operators implementable by a circuit with $r$ CS or $CS^\dagger$ gates (and any number of $X$ and $T$ gates). Suppose $U$ is in $H(r+1)$, then

$$U = CS_{i,j}^e \cdot U'$$

for some $U' \in H(r)$, $i < j$, $i, j \in \{0, \ldots, n-1\}$, $e \in \{-1, 1\}$. In particular,

$$|H(r+1)| \leq (n^2-n)|H(r)|$$

Remark 4. We note that the bounds in Lemma 3 are sharp. Indeed, assume that $n = 2$. If $H(r)$ is the subset of operators implementable by a circuit with $r$ CS gates, then $H(1) = 2 \cdot H(0)$ (see Theorem 1). If $F(r)$ is the subset of operators implementable by a circuit with $r$ CX gates, then $F(1) = 2^{m_d} \cdot F(0)$ (see Theorem 2).

Corollary 5. In order to generate all the elements in the $n$-qubit CNOT-Dihedral group $G = G(m)$ having at most $r$ CX gates, the algorithm generates at most

$$(2m)^n \cdot \left(\frac{m}{d}\right)^r \cdot (n^2-n)^r$$

corresponding group elements.

2. Some useful identities and the proof of the key lemma

Consider quantum circuits on a fixed number of qubits $n$ that are products of controlled-$X$ gates $CX$, bit-flip gates $X$, and single-qubit phase gates $T = T(m)$ satisfying $T|u \rangle := e^{i\pi u/m}|u\rangle$. When these gates are applied to each qubit or pairs of qubits, they generate a group $G = G(m)$ of unitary operators that is an example of a CNOT-dihedral group. An element $U \in G$ acts on the standard basis as

$$U|x\rangle = e^{p(x)} f(x)$$

where $p(x) = p(x_1, \ldots, x_n)$ is a polynomial called the phase polynomial and $f(x)$ is an affine reversible function. Since $x_j \in \mathbb{F}_2$, so $x_j^2 = x_j$, the phase polynomial is

$$p(x) = \sum_{\alpha \subseteq \{0,1\}^n} p_\alpha x^\alpha$$

where $x^\alpha = \prod_{j \in \alpha} x_j$. Furthermore, the coefficients can be chosen such that $p_\emptyset = 0$ and $p_\alpha \in (-2)^{|\alpha|-1}\mathbb{Z}_{2m}$ otherwise (see [12]).

Recall the following useful identities in the Dihedral group defined in (1) generated by the $T = T(m)$ and $X$ gates (up to a global phase),

$$T^\dagger = T^{m-1}$$
$$XTX = T^\dagger$$
$$TXT = X$$
$$T^\dagger XT = SX$$

We state here some useful identities in the CNOT-Dihedral group defined in (2) regarding the controlled-$S$ (CS) gate. According to the definition of the CS gate in (3),

$$CS_{i,j} = T_i T_j \cdot CX_{i,j} \cdot I_i T_j^\dagger \cdot CX_{i,j} = CX_{i,j} \cdot I_i T_j^\dagger \cdot CX_{i,j} \cdot T_i T_j$$
We deduce that
\[ CS_{i,j} \cdot CX_{i,j} = T_iT_j \cdot CX_{i,j} \cdot I_i T_j^\dagger, \]
\[ CX_{i,j} \cdot CS_{i,j} = I_i T_j^\dagger \cdot CX_{i,j} \cdot T_i T_j \]
(8)

Similarly,
\[ CS_{i,j}^\dagger = T_i^\dagger T_j^\dagger \cdot CX_{i,j} \cdot I_i T_j \]
\[ CX_{i,j} \cdot CS_{i,j}^\dagger = I_i T_j \cdot CX_{i,j} \cdot T_i^\dagger T_j^\dagger \]
\[ CS_{j,i} = CS_{i,j} \]
\[ CS_{j,i}^\dagger = CS_{i,j}^\dagger \]
(9)

We note that according to their definition, the CS and CS$^\dagger$ gates (as well as their powers) are symmetrical, namely,
\[ T \text{ (and all its powers)} \text{ commutes with the control and target of the CS gate, namely,} \]
\[ I_i T_j \cdot CS_{i,j} = CS_{i,j} \cdot I_i T_j, \]
\[ T_i T_j \cdot CS_{i,j} = CS_{i,j} \cdot T_i T_j \]
(11)

In addition, we have the following relations between the CS and X gates,
\[ X_i I_j \cdot CS_{i,j} \cdot X_i I_j = CS_{i,j}^\dagger \cdot IS = IS \cdot CS_{i,j}^\dagger \]
\[ I_i X_j \cdot CS_{i,j} \cdot I_i X_j = CS_{i,j}^\dagger \cdot SI = SI \cdot CS_{i,j}^\dagger \]
\[ X_i X_j \cdot CS_{i,j} \cdot X_i X_j = CS_{i,j} \cdot S_i^\dagger S_j^\dagger = S_i^\dagger S_j^\dagger \cdot CS_{i,j} \]
\[ CX_{i,j} \cdot X_i I_j \cdot CX_{i,j} = X_i X_j \]
\[ CX_{i,j} \cdot I_i T_j \cdot CX_{i,j} = Z_i Z_j \]
(13)

Recall that the Z gate is defined as \( Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \). Then we have the following useful relation between the CX gate and the Z gate,
\[ CX_{i,j} \cdot I_i Z_j \cdot CX_{i,j} = Z_i Z_j \]
(15)

Finally, the product \( CX_{i,j} \cdot CX_{j,i} \), which is in the iSWAP-like class of Clifford gates (see [13]), satisfies the following relation,
\[ I_i T_j \cdot CX_{i,j} \cdot CX_{j,i} = CX_{i,j} \cdot CX_{j,i} \cdot T_i I_j \]
(16)

Based on the above identities we can now prove the key lemma.
Proof of Lemma 3. The proof follows [3].

1) There exists a product of single qubit gates $V = V_1 \ldots V_n$, $V_k \in \langle X, T \rangle$ such that $U = V \cdot CX_{i,j} \cdot U'$ for some pair of qubits $i,j$. Absorb $V_k$ for $k \notin \{i,j\}$ into $U'$, namely,

$$U = X_i^k X_j^{k'} \cdot T_i^l T_j^{l'} \cdot CX_{i,j} \cdot U'$$

for some $k,k',l,l'$ and $U' \in F(r)$. Since $T_i^l$ commutes with the control of $CX_{i,j}$ by (13), we can absorb $T_i^l$ in $U'$. Since $X_j^{k'}$ commutes with the target of $CX_{i,j}$ by (13), we can also absorb $X_j^{k'}$ in $U'$. Hence,

$$U = X_i^k T_j^{l'} \cdot CX_{i,j} \cdot U'$$

for some $k,l$ and $U' \in F(r)$.

If $k = 1$ then according to (14), $X_i T_j \cdot CX_{i,j} = CX_{i,j} \cdot X_i X_j$, so we can replace $U$ by

$$I_i T_j^l \cdot CX_{i,j} \cdot X_i X_j \cdot U' = I_i T_j^l \cdot CX_{i,j} \cdot U''$$

where $U'' \in F(r)$. We can therefore assume that $k = 0$. If $m$ is even and $l \geq m/2$ then $T^{m/2} = Z$, so we can rewrite $U$ as

$$U = I_i T_j^l \cdot I_i Z_j \cdot CX_{i,j} \cdot U'$$

for some $l < m/2$. According to (14), $I_i Z_j \cdot CX_{i,j} = CX_{i,j} \cdot Z_i Z_j$, so we can replace $U$ by

$$I_i T_j^l \cdot CX_{i,j} \cdot Z_i Z_j \cdot U' = I_i T_j^l \cdot CX_{i,j} \cdot U''$$

where $U'' \in F(r)$. We can therefore assume that $l < m/2$ as needed.

2) Similarly to (1) we can assume that

$$U = X_i^k X_j^{k'} \cdot T_i^l T_j^{l'} \cdot CS_{i,j}^{e} \cdot U''$$

for some $k,k',l,l', e = \pm 1$ and $U' \in H(r)$. Since $T$ commutes with both control and target of $CS$ by (11), we can absorb $T_i T_j^l$ in $U'$ and so

$$U = X_i^k X_j^{k'} \cdot CS_{i,j}^{e} \cdot U''$$

Now, by (10) we may assume that $i < j$, and by (12) we can absorb $X_i^k X_j^{k'}$ in $U'$ and assume that $U = CS_{i,j}^{e} \cdot U'$ for some $i < j$ and $e = \pm 1$ as needed. \hfill \Box

3. Proof of the theorems and canonical forms

From now on we will now assume that $G$ is the CNOT-Dihedral group on 2-qubits $\{0,1\}$, and describe canonical forms of the elements in $G$. This is analogous to the description in [13] of the elements in the Clifford group on 2-qubits.

Proof of Theorem 1. The proof follows by induction on the number $r$ of $CS$ and $CS^\dagger$ gates. Since $CS$ is of order $m/d$ then necessarily $r < \lfloor m/d \rfloor$.

Let $r = 0$, then any $U \in H(0)$ can be written as

$$U = X_i^k X_j^{k'} \cdot T_0^l T_1^{l'}$$

where $k,k' \in \{0,1\}$, $l,l' \in \{0, \ldots, m - 1\}$, since such an element belongs to the direct product of the two 1-qubit Dihedral groups.
Let $r = 1$, then according to Case (2) of Lemma 3 any $U \in H(1)$ can be written as

$$U = CS_{0,1}^e \cdot X_0^k X_1^{k'} \cdot T_0^o T_1^{l'}$$

where $e \in \{1, -1\}$, $k, k' \in \{0, 1\}$, $l, l' \in \{0, \ldots, m - 1\}$.

Now assume that the Theorem holds for $H(r)$. According to Case (2) of Lemma 3 and the induction assumption, any element $U \in H(r + 1)$ can be written as

$$U = CS_{0,1}^e \cdot U''$$

where $U'' \in \langle T, X \rangle$.

Note that all the elements obtained in this process are distinct, since an equality $CS_{0,1}^e \cdot U = CS_{0,1}^{e'} \cdot U'$ for some $e, e' \in \{0, \ldots, m/d - 1\}$ and $U, U' \in \langle T, X \rangle$, implies that $CS_{0,1}^{e - e'} \in \langle T, X \rangle$, so necessarily $e = e'$ and $U = U'$.

**Lemma 6.** Let $G$ be the CNOT-Dihedral group on 2 qubits. Then any element in $G$ which has exactly one $CS$ gate and one $CX$ gate can be rewritten as an element with no $CS$ gates and exactly one $CX$ gate.

**Proof.** According to Lemma 3 we may assume w.l.o.g. that such an element $U$ can be written as a product

$$U = (U' \cdot CX_{0,1} \cdot I_0 T_1^{l'}) \cdot (CS_{0,1}^e \cdot U'')$$

where $U', U'' \in \langle T, X \rangle$, $l \in \{0, \ldots, m/d - 1\}$, $e \in \{1, -1\}$.

Since $T$ commutes with the control and target of $CS$ by (11), we may absorb $T_1$ into $U''$, and so $U$ can be rewritten as

$$U = U' \cdot CX_{0,1} \cdot CS_{0,1}^e \cdot U'' = U' \cdot I_0 T_1^{-e} \cdot CX_{0,1} \cdot T_0^o T_1^{l'} \cdot U''$$

for some $U', U''$ by (8). Therefore, $U = U' \cdot CX_{0,1} \cdot U''$ for some $U', U''$, as needed.

**Lemma 7.** Let $G$ be the CNOT-Dihedral group on 2 qubits. Then any element in $G$ which has exactly one $CX$ gate and no $CS$ gates can be written either as:

$$U = X_0^k X_1^{k'} \cdot T_0^o T_1^{l'} \cdot CX_{0,1} \cdot I_0 T_1^{m''}$$

or:

$$U = X_0^k X_1^{k'} \cdot T_0^o T_1^{l'} \cdot CX_{1,0} \cdot T_0^o I_1$$

where $k, k' \in \{0, 1\}$, $l, l' \in \{0, \ldots, m - 1\}$ and $m'' \in \{0, \ldots, m/d - 1\}$. In particular, $G$ has

$$\frac{8m^3}{d} = 2 \cdot \frac{m}{d} \cdot (2m)^2$$

such elements.

**Proof.** The proof follows from Case (1) of Lemma 3.

Note that all the elements obtained in this process are indeed distinct.

First, an equality $U \cdot CX_{0,1} \cdot I_0 T_1^{l'} = U' \cdot CX_{0,1} \cdot I_0 T_1^{m''}$ for some $U, U' \in \langle T, X \rangle$ and $l, l' \in \{0, \ldots, m/d - 1\}$, implies that $CX_{0,1} \cdot I_0 T_1^{m'' - 1} \cdot CX_{0,1} \in \langle T, X \rangle$, hence either $l = l'$ and $U = U'$; or $m$ is even and $l - l' = m/2$, yielding a contradiction since $l, l' < m/2$.

Second, an equality $U \cdot CX_{0,1} \cdot I_0 T_1^{l'} = U' \cdot CX_{1,0} \cdot T_0^o I_1$ for some $U, U' \in \langle T, X \rangle$ and $l, l' \in \{0, \ldots, m/d - 1\}$, implies that $CX_{0,1} \cdot T_0^{-l'} T_1 \cdot CX_{1,0} \in \langle T, X \rangle$, yielding a contradiction.

**Lemma 8.** Let $G$ be the CNOT-Dihedral group on 2 qubits. Then any element in $G$ which has exactly two $CX$ gates and no $CS$ gates can be written either as:

$$U = X_0^k X_1^{k'} \cdot T_0^o T_1^{m''} \cdot CX_{0,1} \cdot CX_{1,0} \cdot I_0 T_1^{l'}$$
or:

\[ U = X_0^k X_1^{k'} \cdot T_0^l T_1^{l'} \cdot CX_{1,0} \cdot CX_{0,1} \cdot T_0^{l''} I_1 \]

where \( k, k' \in \{0, 1\} \), \( l, l', l'' \in \{0, \ldots, m - 1\} \) and \( l'' \in \{0, \ldots, m/d - 1\} \). In particular, \( G \) has \( \frac{m^3}{d^2} = \frac{m^3}{d} \cdot (2m)^2 \) such elements.

Proof. According to Case (1) of Lemma 3 and Lemma 7 we may assume w.l.o.g. that such an element \( U \) can be written as

\[ U = I_0 T_1^l \cdot CX_{0,1} \cdot I_0 T_1^{l'} \cdot CX_{0,1} \cdot U' \]

where \( U' \in \langle T, X \rangle \), \( i, j \in \{0, 1\} \), \( l, l' \in \{0, \ldots, m/d - 1\} \). Hence, there are two options, either \((i, j) = (0, 1)\) or \((1, 0)\).

1) First, assume that \((i, j) = (0, 1)\), then

\[ U = I_0 T_1^l \cdot CX_{0,1} \cdot I_0 T_1^{l'} \cdot CX_{0,1} \cdot U' \]

If \( l' = 0 \) then \( U \in \langle X, T \rangle \) and we are done.

Otherwise, according to (11), \( CX_{0,1} \cdot I_0 T_1 \cdot CX_{0,1} = CS_{0,1}^1 \cdot T_0 T_1 \), implying that

\[ CX_{0,1} \cdot I_0 T_1^l \cdot CX_{0,1} = (CX_{0,1} \cdot I_0 T_1 \cdot CX_{0,1})^{l'} = (CS_{0,1}^1 \cdot T_0 T_1)^{l'} = CS_{0,1}^{l'} \cdot T_0^{l'} T_1^{l''} \]

by (11). Thus we can write \( U \) as an element in the subgroup generated by \( CS, X \) and \( T \).

Then we are done by Theorem 1.

2) Now, assume that \((i, j) = (1, 0)\), then we can write \( U \) as

\[ U = T_0^l I_1 \cdot CX_{1,0} \cdot I_0 T_1^{l'} \cdot CX_{0,1} \cdot U' \]

By (13), \( T_1 \) commutes with \( CX_{1,0} \), so we may write \( U \) as

\[ U = T_0^l I_1 \cdot CX_{1,0} \cdot CX_{0,1} \cdot U' \]

According to (11), \( T_0 I_1 \cdot CX_{1,0} \cdot CX_{0,1} = CX_{1,0} \cdot CX_{0,1} \cdot I_0 T_1 \), so we can absorb \( T_0 \) in \( U' \).

Therefore,

\[ U = I_0 T_1^{l'} \cdot CX_{1,0} \cdot CX_{0,1} \cdot U' \]

for some \( U' \in \langle X, T \rangle \) and \( l' \in \{0, \ldots, m/d - 1\} \) as needed.

Similar argument as in the proof of Lemma 7 shows that all the elements obtained in this process are indeed distinct.

First, an equality \( U \cdot CX_{0,1} \cdot CX_{1,0} \cdot I_0 T_1^l = U' \cdot CX_{0,1} \cdot CX_{1,0} \cdot I_0 T_1^{l'} \) for some \( U, U' \in \langle T, X \rangle \) and \( l, l' \in \{0, \ldots, m/d - 1\} \), implies that \( CX_{0,1} \cdot CX_{1,0} \cdot I_0 T_1^{l'-l} \cdot CX_{1,0} \cdot CX_{0,1} = \langle T, X \rangle \), implying that \( l = l' \) and \( U = U' \).

Second, an equality \( U \cdot CX_{0,1} \cdot CX_{1,0} \cdot I_0 T_1^l = U' \cdot CX_{0,1} \cdot CX_{1,0} \cdot T_0^{l''} \cdot I_1 \) for some \( U, U' \in \langle T, X \rangle \) and \( l, l' \in \{0, \ldots, m/d - 1\} \), implies that \( CX_{0,1} \cdot CX_{1,0} \cdot T_0^{-l''} T_1^l \cdot CX_{0,1} \cdot CX_{1,0} = \langle T, X \rangle \), yielding a contradiction. \( \square \)

Lemma 9. Let \( G \) be the CNOT-Dihedral group on 2 qubits. Then any element in \( G \) which has exactly three \( CX \) gates and no \( CS \) gates can be written as:

\[ U = X_0^k X_1^{k'} \cdot T_0^l T_1^{l'} \cdot CX_{0,1} \cdot CX_{1,0} \cdot I_0 T_1^{l''} \cdot CX_{0,1} \]

where \( k, k' \in \{0, 1\} \), \( l, l', l'' \in \{0, \ldots, m - 1\} \) and \( l'' \in \{0, \ldots, m/d - 1\} \). In particular, \( G \) has \( \frac{m^3}{d^2} = \frac{m^3}{d} \cdot (2m)^2 \) such elements.
Proof. According to Case (1) of Lemma 3 and Lemma 8 we may assume w.l.o.g. that such an element $U$ can be written as

$$U = I_i T_j^l \cdot CX_{i,j} \cdot I_0 T_{10}^{l'} \cdot CX_{1,0} \cdot U'$$

where $U' \in \langle T, X \rangle$, $i, j \in \{0, 1\}$, $l, l' \in \{0, \ldots, m/d - 1\}$. Hence, there are two options, either $(i, j) = (0, 1)$ or $(1, 0)$.

1) First, assume that $(i, j) = (1, 0)$, then

$$U = T_0^l I_1 \cdot CX_{1,0} \cdot I_0 T_{1l}^{l'} \cdot CX_{1,0} \cdot CX_{0,1} \cdot U'$$

By (3), $T_1$ commutes with $CX_{1,0}$, so we can write $U$ as

$$U = T_0^l I_1 \cdot CX_{1,0} \cdot I_0 T_{1l}^{l'} \cdot CX_{1,0} \cdot CX_{0,1} \cdot U'$$

Then we actually have only one $CX$ gate and we are done by Lemma 7.

2) Now assume that $(i, j) = (0, 1)$, then we can write $U$ as

$$U = I_0 T_{1l}^l \cdot CX_{0,1} \cdot I_0 T_{1l}^{l'} \cdot CX_{1,0} \cdot CX_{0,1} \cdot U'$$

for some $U', U''$, $l, l'$.

By (3), $T_1$ commutes with $CX_{1,0}$, so we can rewrite $U$ as

$$U = I_0 T_{1l}^l \cdot CX_{0,1} \cdot CX_{1,0} \cdot I_0 T_{1l}^{l'} \cdot CX_{0,1} \cdot U'$$

According to (6), $I_0 T_{1l} \cdot CX_{0,1} \cdot CX_{1,0} = CX_{0,1} \cdot CX_{1,0} \cdot I_0 T_{1l}$, therefore,

$$U = CX_{0,1} \cdot CX_{1,0} \cdot I_0 T_{1l}^{l'} \cdot CX_{0,1} \cdot U'$$

for some $l, l' \in \{0, \ldots, m/d - 1\}$.

Now, by (3), $T_0$ commutes with $CX_{0,1}$ and so we can absorb $T_0$ in $U'$, thus

$$U = CX_{0,1} \cdot CX_{1,0} \cdot I_0 T_{1l}^{l'} \cdot CX_{0,1} \cdot U' = CX_{0,1} \cdot I_0 T_{1l}^{l'} \cdot CX_{1,0} \cdot CX_{0,1} \cdot U'$$

by using (13) again.

The same argument as in the proof of Lemma 3 shows that all the elements obtained in this process are indeed distinct. \[\square\]

**Proof of Theorem 2.** According to Corollary 1 in [12], the CNOT-Dihedral group $G = G(m)$ on 2-qubits has exactly 24 · $m^3/d$ elements.

By Lemma 3 there are no elements with both $CX$ and $CS$ gates. The cases where there are only $CS$ gates were handled in Theorem 1. The remaining cases where there are only $CX$ gates were proved in Lemmas 7 and 9. \[\square\]

**References**

[1] Scott Aaaronson and Daniel Gottesman, *Improved Simulation of Stabilizer Circuits*, Phys. Rev. A 70(052328), 2004. https://arxiv.org/abs/quant-ph/0406196
[2] Matthew Amy, Jianxin Chen, Neil J. Ross, *A Finite Presentation of CNOT-Dihedral Operators*, EPTCS 266, 2018, pp. 84-97. https://arxiv.org/abs/1701.00140
[3] Matthew Amy, Parsiad Azimzadeh, Michele Mosca, *On the CNOT-Complexity of CNOT-Phase Circuits*, Quantum Science and Technology 4.1 (2018): 015002, https://arxiv.org/abs/1712.01859
[4] M. Amy, D. Maslov, M. Mosca, and M. Roetteler, *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, Volume 32, Issue 6, 2013. https://arxiv.org/abs/1206.0758
[5] Héctor Bombín, *Gauge Color Codes: Optimal Transversal Gates and Gauge Fixing in Topological Stabilizer Codes*, New J. Phys. 17(083002), 2015. https://arxiv.org/abs/1311.0879

[6] H. Bombin and M. A. Martin-Delgado, *Topological Computation without Braiding*, Phys. Rev. Lett. 98(160502), 2007. https://arxiv.org/abs/quant-ph/0610024

[7] Sergey Bravyi and D. Maslov, *Hadamard-free circuits expose the structure of the Clifford group*, https://arxiv.org/abs/2003.09412

[8] Sergey Bravyi, *Compiling Clifford operators*, internal note.

[9] Sergey Bravyi, Robert Koenig, *Classification of topologically protected gates for local stabilizer codes*, Phys. Rev. Lett. 110(170503), 2013. https://arxiv.org/abs/1206.1609

[10] Earl T. Campbell, Mark Howard, *Unifying gate-synthesis and magic state distillation*, Phys. Rev. Lett. 118(060501), 2017. https://arxiv.org/abs/1606.01906

[11] Arnaud Carignan-Dugas, Joel Wallman, and Joseph Emerson, *Characterizing Universal Gate Sets via Dihedral Benchmarking*, Phys. Rev. A 92(6), 2015. https://arxiv.org/abs/1508.06312

[12] Andrew W. Cross, Easwar Magesan, Lev S. Bishop, John A. Smolin and Jay M. Gambetta, *Scalable randomised benchmarking of non-Clifford gates*, npj Quantum Inf 2, 16012 (2016). https://arxiv.org/abs/1510.02720.

[13] A. D. Córcoles, Jay M. Gambetta, Jerry M. Chow, John A. Smolin, Matthew Ware, J. D. Strand, B. L. T. Plourde, and M. Steffen, *Supplementary material for “Process verification of two-qubit quantum gates by randomized benchmarking”*, Phys. Rev. A 87(030301(R)), 2013. https://arxiv.org/abs/1210.7011.

[14] Daniel Gottesman, *Stabilizer codes and quantum error correction*. PhD dissertation, Caltech, 1997.

[15] Easwar Magesan, Jay M. Gambetta, and Joseph Emerson, *Robust randomized benchmarking of quantum processes*, Phys. Rev. Lett. 106(180504), 2011. https://arxiv.org/pdf/1009.3639.

[16] Easwar Magesan, Jay M. Gambetta, and Joseph Emerson, *Characterizing Quantum Gates via Randomized Benchmarking*, Phys. Rev. A 85(042311), 2012. https://arxiv.org/pdf/1109.6887.

[17] Easwar Magesan, Jay M. Gambetta, B. R. Johnson, Colm A. Ryan, Jerry M. Chow, Seth T. Merkel, Marcus P. da Silva, George A. Keele, Mary B. Rothwell, Thomas A. Ohki, Mark B. Ketchen, and M. Steffen, *Efficient measurement of quantum gate error by interleaved randomized benchmarking*, Phys. Rev. Lett. 109(080505), 2012. https://arxiv.org/abs/1203.4550.

[18] D. Maslov and Martin Roetteler, *Shorter stabilizer circuits via Bruhat decomposition and quantum circuit transformations*, IEEE Transactions on Information Theory 64(7):4729-4738, 2018. https://arxiv.org/abs/1705.09176

[19] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland, *Randomized benchmarking of quantum gates*, Phys. Rev. A 77(012307), 2008. https://arxiv.org/abs/0707.0963.

[20] Giulia Meuli, Mathias Soeken, and Giovanni De Micheli, *SAT-Based {CNOT, T} Quantum Circuit Synthesis*, International Conference on Reversible Computation, Springer, 2018, 13 pages.
[27] Yunseong Nam, Neil J. Ross, Yuan Su, Andrew M. Childs, and Dmitri Maslov, *Automated optimization of large quantum circuits with continuous parameters*, npj Quantum Information 4(23), 2018. https://arxiv.org/abs/1710.07345.

[28] Neil J. Ross and Peter Selinger, *Optimal ancilla-free Clifford+T approximation of z-rotations*, Quantum Information and Computation 16(11-12):901-953, 2016. https://arxiv.org/abs/1403.2975.

[29] Joel Wallman, Chris Granade, Robin Harper, and Steven T. Flammia, *Estimating the Coherence of Noise*, New J. Phys. 17(113020), 2015. https://arxiv.org/abs/1503.07865.

[30] Christopher J. Wood, Jay Gambetta, *Quantification and Characterization of Leakage Errors*, Phys. Rev. A 97(032306), 2018. https://arxiv.org/abs/1704.03081.

[31] Ed Younis, Koushik Sen, Katherine Yelick, and Costin Iancu, *QFAST: Quantum Synthesis Using a Hierarchical Continuous Circuit Space*, arXiv:2003.04462v1, 2020.

[32] Bei Zeng, Andrew Cross, Isaac L. Chuang, *Transversality versus Universality for Additive Quantum Codes*, IEEE Transactions on Information Theory 57(9), 6272–6284, 2011. https://arxiv.org/abs/0706.1382.

1. IBM Quantum, IBM Research Haifa, Haifa University Campus, Mount Carmel, Haifa, 3498825, Israel
   *E-mail address: shelley@il.ibm.com*

2. IBM Quantum, IBM T.J. Watson Research Center, Yorktown Heights, NY 10598, USA
   *E-mail address: awcross@us.ibm.com*