Synthesis of CNOT-Dihedral circuits with optimal number of two qubit gates

Shelly Garion[1] and Andrew W. Cross[2]

[1]IBM Quantum, IBM Research Haifa, Haifa University Campus, Mount Carmel, Haifa, 3498825, Israel
[2]IBM Quantum, IBM T.J. Watson Research Center, Yorktown Heights, NY 10598, USA

In this note we present explicit canonical forms for all the elements in the two-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 algorithm 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) [23–25] 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, 10, 20, 27]. RB can also be used to characterize specific interleaved gate errors [26], coherence errors [28, 31] and leakage errors [32]. RB methods were generalized to certain single qubit non-Clifford gates, like the T-gate [12]. In [14] 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 [4, 14]. Second, these groups are the set of transversal (fault-tolerant) gates for certain quantum error-correcting codes [6, 7, 9, 19, 22, 34]. 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 [11, 18, 21, 29, 30]. Additional methods aim to minimize the count of controlled-X (CX) gates in universal circuits [33], and in particular, in controlled-X-phase circuits [3, 15].

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 [17]. Another example is the controlled-controlled-Z gate, which is equivalent to the Toffoli gate (up to single qubit gates), that can be decomposed into 6 CX gates and single qubit gates, but requires only 5 two-qubit gates in its decomposition if the CS and CS^{-1} gates are also available [5].

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 (CX) and controlled-S (CS) 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 $T(8) =$

Shelly Garion: shelly@il.ibm.com
Andrew W. Cross: awcross@us.ibm.com

$\begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/8} \end{pmatrix}$.

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

$$\begin{aligned} &\langle X, T\rangle / \langle \lambda I : \lambda \in \mathbb{C}\rangle = \\ &\{X^l T^k : l \in \{0,1\}, k \in \{0,\ldots,m-1\}\}. \end{aligned} \tag{1}$$

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 [14] for details),

$$\begin{aligned} G = G(m) = &\langle X_i, T_i, CX_{i,j} : \\ &i,j \in \{0,\ldots,n-1\}\rangle / \\ &\langle \lambda I : \lambda \in \mathbb{C}\rangle, \end{aligned} \tag{2}$$

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 [14]). Elements of $G(m)$ belong to level $\log_2 m$ of the Clifford hierarchy when m is a power of two [19, 22] and this is related to the fact that they are the transversal gates of certain m-dimensional quantum codes [7].

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

$$\begin{aligned} CS_{i,j} &= T_i T_j \cdot CX_{i,j} \cdot I_i T_j^\dagger \cdot CX_{i,j} \\ &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{4\pi i/m} \end{pmatrix}, \end{aligned} \tag{3}$$

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[1] which makes it an alternative to CX for improving circuit decompositions.

We focus on the case where $n = 2$. The following two Theorems provide canonical forms for all the elements in the two-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 two-qubit Clifford group.

Theorem 1. *Consider the CS-Dihedral subgroup on two qubits, namely the two-qubit group generated by the gates X, $T = T(m)$ 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:*

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

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

Theorem 2. *Let G be the two-qubit CNOT-Dihedral group generated by the gates X, $T = T(m)$, 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.*

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

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.*

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

[1] 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 [16].

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

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

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

The following Theorem provides an algorithm to successively construct the n-qubit CNOT-Dihedral group. It is analogous to [8] that discusses the generation of the n-qubit Clifford group. Case (1) of this Theorem shows that one can successively construct the CNOT-Dihedral group asserting an optimal number of CX gates, with a bound on the space to search these group elements (see Remark 4). Moreover, one can also use the "meet in the middle" algorithm of [2] to synthesize gate sequences for the non-Clifford RB.

Theorem 3. *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*

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

for some $U' \in F(r)$, $i, j \in \{0, ..., n-1\}$, $i \neq j$, $l \in \{0, \ldots, m/d - 1\}$. *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 $U' \in H(r)$, $i, j \in \{0, ..., n-1\}$, $i < j$, $e \in \{-1, 1\}$. *In particular,*

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

Remark 4. We note that the bounds in Theorem 3 are *sharp* and cannot generally be improved, since there is an equality in certain cases. 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 $F(1) = \frac{2m}{d} \cdot F(0)$ (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*

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

group elements.

2 Useful identities and the proof of Theorem 3

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

$$U|x\rangle = e^{p(x)}|f(x)\rangle \tag{4}$$

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

$$p(x) = \sum_{\alpha \subseteq \{0,1\}^n} p_\alpha x^\alpha \tag{5}$$

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 [14]).

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),

$$\begin{aligned} T^\dagger &= T^{m-1} \\ XTX &= T^\dagger \\ TXT &= X \\ TXT^\dagger &= SX \end{aligned} \tag{6}$$

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),

$$\begin{aligned} CS_{i,j} &= T_iT_j \cdot CX_{i,j} \cdot I_iT_j^\dagger \cdot CX_{i,j} \\ &= CX_{i,j} \cdot I_iT_j^\dagger \cdot CX_{i,j} \cdot T_iT_j \end{aligned} \tag{7}$$

We deduce that

$$\begin{aligned} CS_{i,j} \cdot CX_{i,j} &= T_iT_j \cdot CX_{i,j} \cdot I_iT_j^\dagger, \\ CX_{i,j} \cdot CS_{i,j} &= I_iT_j^\dagger \cdot CX_{i,j} \cdot T_iT_j \end{aligned} \tag{8}$$

Similarly,

$$\begin{aligned} CS_{i,j}^\dagger &= T_i^\dagger T_j^\dagger \cdot CX_{i,j} \cdot I_iT_j \cdot CX_{i,j} \\ &= CX_{i,j} \cdot I_iT_j \cdot CX_{i,j} \cdot T_i^\dagger T_j^\dagger \end{aligned} \tag{9}$$

We note that according to their definition, the CS and $CS^\dagger$ gates (as well as their powers) are symmetrical, namely,

$$\begin{aligned} CS_{j,i} &= CS_{i,j} \\ CS_{j,i}^\dagger &= CS_{i,j}^\dagger \end{aligned} \tag{10}$$

T (and all its powers) commutes with the control and target of the CS gate, namely,

$$\begin{aligned} I_iT_j \cdot CS_{i,j} &= CS_{i,j} \cdot I_iT_j, \\ T_iI_j \cdot CS_{i,j} &= CS_{i,j} \cdot T_iI_j, \\ T_iT_j \cdot CS_{i,j} &= CS_{i,j} \cdot T_iT_j \end{aligned} \tag{11}$$

In addition, we have the following relations between the CS and X gates,

$$\begin{aligned} X_iI_j \cdot CS_{i,j} \cdot X_iI_j &= CS_{i,j}^\dagger \cdot I_iS_j = I_iS_j \cdot CS_{i,j}^\dagger \\ I_iX_j \cdot CS_{i,j} \cdot I_iX_j &= CS_{i,j}^\dagger \cdot S_iI_j = S_iI_j \cdot CS_{i,j}^\dagger \\ X_iX_j \cdot CS_{i,j} \cdot X_iX_j &= CS_{i,j} \cdot S_i^\dagger S_j^\dagger = S_i^\dagger S_j^\dagger \cdot CS_{i,j} \end{aligned} \tag{12}$$

We shall moreover use the following identities of the CX gate. T (and all its powers) commutes with the control of CX, and X (and all its powers) commutes with the target of CX, namely,

$$\begin{aligned} I_iX_j \cdot CX_{i,j} &= CX_{i,j} \cdot I_iX_j, \\ T_iI_j \cdot CX_{i,j} &= CX_{i,j} \cdot T_iI_j \end{aligned} \tag{13}$$

In addition, we have the following relation between the control of CX and the X gate,

$$CX_{i,j} \cdot X_iI_j \cdot CX_{i,j} = X_iX_j \tag{14}$$

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,

$$CX_{i,j} \cdot I_iZ_j \cdot CX_{i,j} = Z_iZ_j \tag{15}$$

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,

$$I_iT_j \cdot CX_{i,j} \cdot CX_{j,i} = CX_{i,j} \cdot CX_{j,i} \cdot T_iI_j \tag{16}$$

Based on the above identities we can now prove Theorem 3.

Proof of Theorem 3. 1) There exists a product of single qubit gates $V = V_1 \dots V_n$, $V_k \in \langle X, T \rangle$ 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), $X_iI_j \cdot CX_{i,j} = CX_{i,j} \cdot X_iX_j$, so we can replace U by

$$I_iT_j^l \cdot CX_{i,j} \cdot X_iX_j \cdot U' = I_iT_j^l \cdot CX_{i,j} \cdot U''$$

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

$$U = I_iT_j^l \cdot I_iZ_j \cdot CX_{i,j} \cdot U'$$

for some $l < m/2$. According to (15), $I_iZ_j \cdot CX_{i,j} = CX_{i,j} \cdot Z_iZ_j$, so we can replace U by

$$I_iT_j^l \cdot CX_{i,j} \cdot Z_iZ_j \cdot U' = I_iT_j^l \cdot CX_{i,j} \cdot U''$$

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 $T_i^l T_j^{l'}$ 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. □

3 The canonical forms and proofs of Theorems 1 and 2

From now on we will now assume that G is the CNOT-Dihedral group on two 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 two 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 $r < \lceil \frac{m-d}{2d} \rceil$.

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

$$U = X_0^k X_1^{k'} \cdot T_0^l T_1^{l'}$$

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 single-qubit Dihedral groups.

Let $r = 1$, then according to Case (2) of Theorem 3, any $U \in H(1)$ can be written as

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

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 Theorem 3 and the induction assumption, any element $U \in H(r+1)$ can be written as

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

where $U' \in \langle T, X \rangle$, $e = \pm 1$ and $e' = \pm r$, as needed.

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 two 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 Theorem 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

$$\begin{aligned} U &= U' \cdot CX_{0,1} \cdot CS_{0,1}^e \cdot U'' \\ &= U' \cdot I_0 T_1^{-e} \cdot CX_{0,1} \cdot T_0^e T_1^e \cdot U'' \end{aligned}$$

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 two qubits. Then any element in G which has exactly one CX gate and no CS gates can be written either as:*

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

or:

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

where $k, k' \in \{0, 1\}$, $l, l' \in \{0, \ldots, m-1\}$ and $l'' \in \{0, \ldots, m/d - 1\}$. 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 Theorem 3.

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

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

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

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

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 $k, k' \in \{0,1\}$, $l, l' \in \{0, \dots, m-1\}$ and $l'' \in \{0, \dots, m/d-1\}$. In particular, G has $\frac{8m^3}{d} = 2 \cdot \frac{m}{d} \cdot (2m)^2$ such elements.

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

$$U = I_i T_j^l \cdot CX_{i,j} \cdot I_0 T_1^{l'} \cdot CX_{0,1} \cdot U'$$

where $U' \in \langle T, X \rangle$, $i, j \in \{0,1\}$, $l, l' \in \{0, ..., m/d-1\}$. 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 (9), $CX_{0,1} \cdot I_0 T_1 \cdot CX_{0,1} = CS_{0,1}^\dagger \cdot T_0 T_1$, implying that

$$\begin{aligned} CX_{0,1} \cdot I_0 T_1^{l'} \cdot CX_{0,1} &= (CX_{0,1} \cdot I_0 T_1 \cdot CX_{0,1})^{l'} \\ &= (CS_{0,1}^\dagger \cdot T_0 T_1)^{l'} \\ &= CS_{0,1}^{-l'} \cdot T_0^{l'} T_1^{l'} \end{aligned}$$

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

$$U = T_0^l T_1^{l'} \cdot CX_{1,0} \cdot CX_{0,1} \cdot U'$$

According to (16), $T_0 I_1 \cdot CX_{1,0} \cdot CX_{0,1} = CX_{1,0} \cdot CX_{0,1} \cdot I_0 T_1$, 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 $l' \in \{0, ..., m/d-1\}$ 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 $l, l' \in \{0, \dots, m/d-1\}$, implies that $CX_{0,1} \cdot CX_{1,0} \cdot I_0 T_1^{l'-l} \cdot CX_{1,0} \cdot CX_{0,1} \in \langle T, X \rangle$, implying that $l = l$ and $U = U'$.

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

Lemma 9. *Let G be the CNOT-Dihedral group on two 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 $k, k' \in \{0,1\}$, $l, l' \in \{0, \dots, m-1\}$ and $l'' \in \{0, \dots, m/d-1\}$. In particular, G has $\frac{4m^3}{d} = \frac{m}{d} \cdot (2m)^2$ such elements.

Proof. According to Case (1) of Theorem 3 and Lemma 8 we may assume w.l.o.g. that such an element U can be written as

$$U = I_i T_j^l \cdot CX_{i,j} \cdot I_0 T_1^{l'} \cdot CX_{1,0} \cdot CX_{0,1} \cdot U'$$

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

Hence, there are two options, either $(i,j) = (0,1)$ or $(1,0)$.

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

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

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

$$\begin{aligned} U &= T_0^l I_1 \cdot I_0 T_1^{l'} \cdot CX_{1,0} \cdot CX_{1,0} \cdot CX_{0,1} \cdot U' \\ &= T_0^l T_1^{l'} \cdot CX_{0,1} \cdot U' \end{aligned}$$

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

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

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

By (13), T_1 commutes with $CX_{1,0}$, so we can rewrite U as

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

According to (16), $I_0 T_1 \cdot CX_{0,1} \cdot CX_{1,0} = CX_{0,1} \cdot CX_{1,0} \cdot T_0 I_1$, therefore,

$$U = CX_{0,1} \cdot CX_{1,0} \cdot T_0^l T_1^{l'} \cdot CX_{0,1} \cdot U'$$

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

Now, by (13), T_0 commutes with $CX_{0,1}$ and so we can absorb T_0 in U', thus

$$\begin{aligned} U &= CX_{0,1} \cdot CX_{1,0} \cdot I_0 T_1^{l'} \cdot CX_{0,1} \cdot U' \\ &= CX_{0,1} \cdot I_0 T_1^{l'} \cdot CX_{1,0} \cdot CX_{0,1} \cdot U' \end{aligned}$$

by using (13) again.

The same argument as in the proof of Lemma 8 shows that all the elements obtained in this process are indeed distinct. □

Proof of Theorem 2. According to Corollary 1 in [14], the CNOT-Dihedral group $G = G(m)$ on two qubits has exactly $24 \cdot m^3/d$ elements.

By Lemma 6, 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, 8 and 9. □

References

[1] Scott Aaronson and Daniel Gottesman. Improved simulation of stabilizer circuits. *Phys. Rev. A*, 70:052328, Nov 2004. DOI: 10.1103/PhysRevA.70.052328. URL https://link.aps.org/doi/10.1103/PhysRevA.70.052328.

[2] 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*, 32(6):818–830, 2013. DOI: 10.1109/TCAD.2013.2244643.

[3] Matthew Amy, Parsiad Azimzadeh, and Michele Mosca. On the controlled-NOT complexity of controlled-NOT–phase circuits. *Quantum Science and Technology*, 4 (1):015002, sep 2018. DOI: 10.1088/2058-9565/aad8ca. URL https://doi.org/10.1088%2F2058-9565%2Faad8ca.

[4] Matthew Amy, Jianxin Chen, and Neil J. Ross. A finite presentation of cnot-dihedral operators. *Electronic Proceedings in Theoretical Computer Science*, 266:84–97, 2018. DOI: 10.4204/eptcs.266.5. URL https://app.dimensions.ai/details/publication/pub.1101260386andhttps://arxiv.org/pdf/1701.00140.

[5] Adriano Barenco, Charles H. Bennett, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A. Smolin, and Harald Weinfurter. Elementary gates for quantum computation. *Phys. Rev. A*, 52:3457–3467, Nov 1995. DOI: 10.1103/PhysRevA.52.3457. URL https://link.aps.org/doi/10.1103/PhysRevA.52.3457.

[6] H. Bombin and M. A. Martin-Delgado. Topological computation without braiding. *Phys. Rev. Lett.*, 98:160502, Apr 2007. DOI: 10.1103/PhysRevLett.98.160502. URL https://link.aps.org/doi/10.1103/PhysRevLett.98.160502.

[7] Héctor Bombín. Gauge color codes: optimal transversal gates and gauge fixing in topological stabilizer codes. *New Journal of Physics*, 17(8):083002, aug 2015. DOI: 10.1088/1367-2630/17/8/083002. URL https://doi.org/10.1088%2F1367-2630%2F17%2F8%2F083002.

[8] Sergey Bravyi. Compiling clifford operators.

[9] Sergey Bravyi and Robert König. Classification of topologically protected gates for local stabilizer codes. *Phys. Rev. Lett.*, 110:170503, Apr 2013. DOI: 10.1103/PhysRevLett.110.170503. URL https://link.aps.org/doi/10.1103/PhysRevLett.110.170503.

[10] Sergey Bravyi and Dmitri Maslov. Hadamard-free circuits expose the structure of the clifford group, 2020. URL https://arxiv.org/abs/2003.09412.

[11] Earl T. Campbell and Mark Howard. Unifying gate synthesis and magic state distillation. *Phys. Rev. Lett.*, 118:060501, Feb 2017. DOI: 10.1103/PhysRevLett.118.060501. URL https://link.aps.org/doi/10.1103/PhysRevLett.118.060501.

[12] Arnaud Carignan-Dugas, Joel J. Wallman, and Joseph Emerson. Characterizing universal gate sets via dihe-

dral benchmarking. *Phys. Rev. A*, 92: 060302, Dec 2015. DOI: 10.1103/PhysRevA.92.060302. URL https://link.aps.org/doi/10.1103/PhysRevA.92.060302.

[13] A. D. Córcoles, Jay M. Gambetta, Jerry M. Chow, John A. Smolin, Matthew Ware, Joel Strand, B. L. T. Plourde, and M. Steffen. Process verification of two-qubit quantum gates by randomized benchmarking. *Phys. Rev. A*, 87: 030301, Mar 2013. DOI: 10.1103/PhysRevA.87.030301. URL https://link.aps.org/doi/10.1103/PhysRevA.87.030301.

[14] Andrew W Cross, Easwar Magesan, Lev S Bishop, John A Smolin, and Jay M Gambetta. Scalable randomised benchmarking of non-clifford gates. *npj Quantum Information*, 2(1), 2016. DOI: 10.1038/npjqi.2016.12. URL https://doi.org/10.1038/npjqi.2016.12.

[15] Meuli G., Soeken M., and De Micheli G. Sat-based {CNOT, T} quantum circuit synthesis. *Kari J., Ulidowski I. (eds) Reversible Computation. RC 2018. Lecture Notes in Computer Science*, 11106, 2018. DOI: 10.1007/978-3-319-99498-7˙12.

[16] Shelly Garion, Naoki Kanazawa, Haggai Landa, David C. McKay, Sarah Sheldon, Andrew W. Cross, and Christopher J. Wood. Experimental implementation of non-clifford interleaved randomized benchmarking with a controlled-s gate, 2020. URL https://arxiv.org/abs/2007.08532.

[17] Andrew N. Glaudell, Neil J. Ross, and Jacob M. Taylor. Optimal two-qubit circuits for universal fault-tolerant quantum computation, 2020. URL https://arxiv.org/abs/2001.05997.

[18] David Gosset, Vadym Kliuchnikov, Michele Mosca, and Vincent Russo. An algorithm for the t-count. *Quantum Info. Comput.*, 14(15–16):1261–1276, November 2014. ISSN 1533-7146. URL https://dl.acm.org/doi/10.5555/2685179.2685180.

[19] Daniel Gottesman and Isaac L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402: 390–393, 1999. ISSN 1476-4687. DOI: 10.1038/46503. URL https://doi.org/10.1038/46503.

[20] Daniel Eric Gottesman. Stabilizer codes and quantum error correction, 1997. URL https://resolver.caltech.edu/CaltechETD:etd-07162004-113028.

[21] Luke E Heyfron and Earl T Campbell. An efficient quantum compiler that reduces t count. *Quantum Science and Technology*, 4 (1):015004, sep 2018. DOI: 10.1088/2058-9565/aad604. URL https://doi.org/10.1088%2F2058-9565%2Faad604.

[22] Tomas Jochym-O'Connor, Aleksander Kubica, and Theodore J. Yoder. Disjointness of stabilizer codes and limitations on fault-tolerant logical gates. *Phys. Rev. X*, 8:021047, May 2018. DOI: 10.1103/PhysRevX.8.021047. URL https://link.aps.org/doi/10.1103/PhysRevX.8.021047.

[23] 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, Jan 2008. DOI: 10.1103/PhysRevA.77.012307. URL https://link.aps.org/doi/10.1103/PhysRevA.77.012307.

[24] Easwar Magesan, J. M. Gambetta, and Joseph Emerson. Scalable and robust randomized benchmarking of quantum processes. *Phys. Rev. Lett.*, 106:180504, May 2011. DOI: 10.1103/PhysRevLett.106.180504. URL https://link.aps.org/doi/10.1103/PhysRevLett.106.180504.

[25] Easwar Magesan, Jay M. Gambetta, and Joseph Emerson. Characterizing quantum gates via randomized benchmarking. *Phys. Rev. A*, 85:042311, Apr 2012. DOI: 10.1103/PhysRevA.85.042311. URL https://link.aps.org/doi/10.1103/PhysRevA.85.042311.

[26] Easwar Magesan, Jay M. Gambetta, B. R. Johnson, Colm A. Ryan, Jerry M. Chow, Seth T. Merkel, Marcus P. da Silva, George A. Keefe, 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, Aug 2012. DOI: 10.1103/PhysRevLett.109.080505. URL

https://link.aps.org/doi/10.1103/PhysRevLett.109.080505.

[27] D. Maslov and M. Roetteler. Shorter stabilizer circuits via bruhat decomposition and quantum circuit transformations. *IEEE Transactions on Information Theory*, 64(7):4729–4738, 2018. DOI: 10.1109/TIT.2018.2825602.

[28] David C. McKay, Stefan Filipp, Antonio Mezzacapo, Easwar Magesan, Jerry M. Chow, and Jay M. Gambetta. Universal gate for fixed-frequency qubits via a tunable bus. *Phys. Rev. Applied*, 6:064007, Dec 2016. DOI: 10.1103/PhysRevApplied.6.064007. URL https://link.aps.org/doi/10.1103/PhysRevApplied.6.064007.

[29] Yunseong Nam, Neil J. Ross, Yuan Su, Andrew M. Childs, and Dmitri Maslov. Automated optimization of large quantum circuits with continuous parameters. 4:23, 2018. ISSN 2056-6387. DOI: 10.1038/s41534-018-0072-4. URL https://doi.org/10.1038/s41534-018-0072-4.

[30] Neil J. Ross and Peter Selinger. Optimal ancilla-free clifford + t approximation of z-rotations. *Quantum Info. Comput.*, 16(11–12):901–953, September 2016. ISSN 1533-7146. URL https://dl.acm.org/doi/abs/10.5555/3179330.3179331.

[31] Joel Wallman, Chris Granade, Robin Harper, and Steven T Flammia. Estimating the coherence of noise. *New Journal of Physics*, 17(11):113020, nov 2015. DOI: 10.1088/1367-2630/17/11/113020. URL https://doi.org/10.1088%2F1367-2630%2F17%2F11%2F113020.

[32] Christopher J. Wood and Jay M. Gambetta. Quantification and characterization of leakage errors. *Phys. Rev. A*, 97:032306, Mar 2018. DOI: 10.1103/PhysRevA.97.032306. URL https://link.aps.org/doi/10.1103/PhysRevA.97.032306.

[33] Ed Younis, Koushik Sen, Katherine Yelick, and Costin Iancu. Qfast: Quantum synthesis using a hierarchical continuous circuit space, 2020. URL https://arxiv.org/abs/2003.04462.

[34] B. Zeng, A. Cross, and I. L. Chuang. Transversality versus universality for additive quantum codes. *IEEE Transactions on Information Theory*, 57(9):6272–6284, 2011. DOI: 10.1109/TIT.2011.2161917.