Multi-qubit controlled gate with optimal T-count

Soichiro Yamazaki
The University of Tokyo
Tokyo, Japan
soichiro.yamazaki@phys.s.u-tokyo.ac.jp

Seiseki Akibue
Communication Science Laboratories, NTT, Inc.,
NTT Research Center for Theoretical Quantum Information,
NTT Institute for Fundamental Mathematics,
3–1 Morinosato Wakamiya, Atsugi, Kanagawa, Japan
seiseki.akibue@ntt.com

Controlled gates are key components in various quantum algorithms. Improving on the prior work of Gosset et al., we show that, for an allowed error ε, $3\log_2(1/\varepsilon)+o(\log(1/\varepsilon))$ T gates are sufficient to approximate most multi-qubit controlled SU(2)s. We also show that this T-count matches the lower bound among approximating circuits that preserve the block-diagonal form. As an application, general controlled gate synthesis and efficient SU(4) gate synthesis are given.

1 Introduction

The Gottesman-Knill theorem reveals that circuits composed of Clifford gates can be efficiently simulated classically and do not possess quantum computational advantage. Adding just one non-Clifford gate to Clifford gates achieves quantum universality, enabling any quantum gate to be approximated with arbitrary precision. A well-known non-Clifford gate is the T gate, which can be implemented highly precisely even in surface codes, which are commonly used in quantum error correction, through a technique called magic state distillation. However, T gates are costlier than Clifford gates, which can be implemented transversally [2]. In terms of diamond distance, which quantifies distinguishability as a quantum channel, approximating a quantum gate with high precision below an allowed error ε is called ε-approximation. Here, an efficient ε-approximation of a quantum gate in Clifford+T refers to an approximation that achieves high precision below ε with fewer T gates, i.e., an approximation with a smaller T-count.

Numerous studies have attempted to approximate quantum gates by synthesizing Clifford+T gates and have revealed much about the lower bound of the T-count for single-qubit gates, and methods have also been proposed to achieve this lower bound. The lower bound for the ε-approximation of all single-qubit gates is $O(\log(1/\varepsilon))$ [12]. Specifically, it is $3\log_2(1/\varepsilon)+o(\log(1/\varepsilon))$ for all but an inverse-polynomially small fraction of target single-qubit gates (In such cases, we append "with high probability (w.h.p.)". For details, refer to Section 2.2) [9]. On the other hand, much remains unknown regarding multi-qubit gates. Although the lower bound for the T-count is $O(\log(1/\varepsilon))$ when the number of qubits n is fixed, as it can be reduced to single-qubit gate synthesis on the basis of decomposition into single-qubit gates, the dependence on n and the coefficient of the leading term have not yet been revealed. Controlled gates appear in various quantum algorithms such as state preparation [4], quantum phase estimation [10], quantum signal processing [6], and Hamiltonian simulation [7], and for improving the performance of these diverse quantum algorithms, the T-count for their approximation needs to be reduced. Similarly to the other multi-qubit gate, little is known about controlled gates. However, if the blocks in matrix representation are limited to SU(2), an ε-approximation can be achieved with an $O(\sqrt{2^n\log(1/\varepsilon)}+\log(1/\varepsilon))$ T-count, and this achieves the lower bound [4].

In this study, we derive the optimal constant in the $\log(1/\varepsilon)$ term for all but an inverse-polynomially small fraction of target gates , the same as that of a single-qubit gate synthesis. We also show that

Submitted to:
QPL 2026

© S. Yamazaki & S. Akibue
This work is licensed under the
Creative Commons Attribution License.

this coefficient matches the lower bound as long as the form of the approximate circuit of Clifford+T preserves the form of the controlled gate.

Theorem 1 ($\mathrm{SU}(2)^{\oplus 2^n}$ controlled gate synthesis with optimal T-count)**.** *For $n \geq 1$, n-qubit controlled gates whose diagonal blocks are composed of SU(2) can be implemented up to error ε by a Clifford+T circuit using*

$$3\log_2(1/\varepsilon) + O\left(\sqrt{2^n \log(1/\varepsilon)}\right) + o\left(\log(1/\varepsilon)\right) \quad \text{w.h.p.} \tag{1}$$

T gates and ancillae. Furthermore, when n is fixed, no Clifford+T circuit with a diagonal block form can use asymptotically fewer T gates.

Furthermore, we also show that the $\mathrm{SU}(2) \oplus \mathrm{SU}(2)$ targets can be implemented as an ancilla-free circuit.

Theorem 2 ($\mathrm{SU}(2) \oplus \mathrm{SU}(2)$ ancilla-free controlled gate synthesis)**.** *Controlled gates whose diagonal blocks are composed of SU(2) can be implemented up to error ε by a Clifford+T circuit using*

$$3\log_2(1/\varepsilon) + o\left(\log(1/\varepsilon)\right) \quad \text{w.h.p.} \tag{2}$$

T gates and without ancilla. Furthermore, no Clifford+T circuit with a diagonal block form can use asymptotically fewer T gates.

1.1 Applications

Although Theorems 1 and 2 have various applications in quantum algorithms as stated above, here we showcase some of their more primitive applications in gate synthesis.

Theorem 3 (Controlled gate synthesis)**.** *For $n \geq 1$, n-qubit controlled gates can be implemented up to error ε as a CPTP mapping by a Clifford+T circuit using*

$$6\log_2(1/\varepsilon) + O\left(\sqrt{2^n \log(1/\varepsilon)}\right) + o\left(\log(1/\varepsilon)\right) \quad \text{w.h.p.} \tag{3}$$

T gates and ancillae.

Using Theorem 2, we can also synthesize an ancilla-free Clifford+T circuit to approximate controlled gates.

Theorem 4 ($\mathrm{SU}(2)^{\oplus 2^n}$ ancilla-free controlled gate synthesis)**.** *For $n \geq 2$, n-qubit controlled gates whose diagonal blocks are composed of SU(2) can be implemented up to error ε by a Clifford+T circuit using*

$$\frac{3(2^n+1)}{2}\log_2(1/\varepsilon) + O(n2^n) + o\left(2^n \log(1/\varepsilon)\right) \quad \text{w.h.p.} \tag{4}$$

T gates and without ancilla.

Furthermore, general 2-qubit gates SU(4) beyond controlled gates can also be synthesized.

Theorem 5 (SU(4) gate synthesis)**.** *SU(4) gates can be implemented up to error ε by a Clifford+T circuit using*

$$9\log_2(1/\varepsilon) + o(\log(1/\varepsilon)) \quad \text{w.h.p.} \tag{5}$$

T gates and without ancilla.

This substantially reduces T-count compared to the $21\log_2(1/\varepsilon) + o(\log(1/\varepsilon))$ scaling obtained via the KAK decomposition [14].

1.2 Discussion

In this study, the minimum T-count of multi-qubit controlled gate synthesis was determined to have ε scaling less than or equal to that of the single-qubit gate synthesis, but whether it can go lower than this is unclear, when general SU(2^n) form Clifford+T circuits are allowed. However, we expect that it will not. This is because if the coefficient of the logarithm is $k < 3$ for some n when the general form is allowed, then performing probabilistic synthesis on the top-left block will imply that adaptive single-qubit synthesis could be performed with a T-count of $(k/2)\log_2(1/\varepsilon) + o(\log(1/\varepsilon))$. This will be lower than the best published result of $1.5\log_2(1/\varepsilon) + o(\log(1/\varepsilon))$ [5]. In addition, the coefficient of $\sqrt{2^n \log(1/\varepsilon)}$ remains unclear. These two issues are left as open problems.

Furthermore, the accidental isomorphism between $\mathrm{SU}(4)/\mathbb{Z}_2$ and SO(6) guarantees that all SU(4) gates can be constructed by using the construction method in the proof of Theorem 5. For a general SU(2^n), no such guarantee exists, so a similar construction cannot be made. However, if we assume that SU(2^n) can be decomposed into $(4^n - 1)$ rotations, then the leading term for the T-count with respect to ε would be $(3 \cdot 2^n - 3)\log_2(4^n/\varepsilon)$.

2 Preliminaries

2.1 Basic notations

There are 2^n computational bases for n-qubit pure states, and we denote them as $|0\rangle, |1\rangle, \cdots, |2^n - 1\rangle$. Each basis $|i\rangle = |i_n i_{n-1} \cdots i_{1\,(2)}\rangle$ corresponds to the first qubit being $|i_1\rangle$, the second qubit being $|i_2\rangle$, $\cdots$, and the n-th qubit being $|i_n\rangle$, where the subscript $_{(2)}$ denotes the binary representation. An n-qubit quantum gate is a member of the $2^n \times 2^n$ unitary group $\mathrm{U}(2^n) = \{U \in \mathbb{C}^{2^n \times 2^n} |\ U^\dagger U = UU^\dagger = I_{2^n}\}$, where I_{2^n} denotes the identity. Since the global phase has no physical meaning, we can identify two gates that differ only by the global phase, and the gates are also considered as members of the special unitary group $\mathrm{SU}(2^n) = \{U \in \mathrm{U}(2^n) |\ \det(U) = 1\}$. Among $(n+1)$-qubit gates, we denote an n-qubit controlled gate as follows:

$$\begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_{2^n} \end{pmatrix} \in \mathrm{U}(2^{n+1}) \qquad (A_1, A_2, \cdots, A_{2^n} \in \mathrm{U}(2)). \tag{6}$$

Let $\mathrm{U}(2)^{\oplus 2^n}$ be the set consisting of all such gates. In particular, $\mathrm{SU}(2)^{\oplus 2^n}$ is a subset of $\mathrm{U}(2)^{\oplus 2^n}$ consisting of elements where all diagonal blocks $A_1, A_2, \cdots, A_{2^n}$ belong to SU(2).

A quantum channel from n-qubit states to n-qubit states is completely positive and trace preserving (CPTP) mapping. Given two quantum channels, the diamond distance is a metric that measures the maximum bias of the success probability of distinguishing between them when the input can be freely chosen.

Definition 6 (Diamond distance)**.** *Let $\mathscr{E}_1, \mathscr{E}_2$ be two quantum channels from n-qubit states to n-qubit states.*

$$D_\diamond(\mathscr{E}_1, \mathscr{E}_2) = \frac{1}{2} \max_\rho \|((\mathscr{E}_1 - \mathscr{E}_2) \otimes \mathscr{I}_n)(\rho)\|, \tag{7}$$

where $\mathscr{I}_n$ is an identity channel on a n-qubit system and $\|\cdot\|$ is a trace norm.

A quantum channel $\mathscr{E}_U$ of unitary U is $\mathscr{E}_U(\rho) = U\rho U^\dagger$ where ρ is a positive semidefinite matrix with trace 1, or a density operator. The diamond distance between two unitary channels U, V can be calculated

by the following equation:

$$D_\diamond(\mathscr{E}_U, \mathscr{E}_V) = \sqrt{1 - \min_\rho |\mathrm{tr}(\rho U V^\dagger)|^2}. \tag{8}$$

Throughout the paper, we adopt a slight abuse of notation and use $D_\diamond(U,V)$ to represent $D_\diamond(\mathscr{E}_U, \mathscr{E}_V)$.

Channel representation $\widehat{U}$ of an n-qubit unitary $U \in \mathrm{U}(2^n)$ can be explicitly written as a member of $\mathrm{O}(4^n)$:

$$\widehat{U}_{i,j} = \frac{1}{2^n}\mathrm{tr}(U P_i U^\dagger P_j), \tag{9}$$

where $i, j = 0, 1, \cdots, 4^n - 1$ and

$$P_i = \bigotimes_{k=1}^{n} \sigma_{i_k} \qquad (\sigma_0 = I_2,\ \sigma_1 = X,\ \sigma_2 = Y,\ \sigma_3 = Z,\ (i_1 i_2 \cdots i_n)_{(4)} = i). \tag{10}$$

2.2 Asymptotic notation

Let $(\Omega, \mu, \mathscr{F})$ be a probability space. Given an event E_ε or $F_{n,\varepsilon}$, which depends on some parameters n and ε, we say that

$$E_\varepsilon\ (F_{n,\varepsilon}) \text{ holds w.h.p. as } \varepsilon \to 0\ (n \to \infty,\ \varepsilon \to 0) \tag{11}$$

if the following equation holds for some constant $c, d > 0$:

$$\Pr_{\omega\sim\mu}[E_\varepsilon] = 1 - O(\varepsilon^c) \text{ as } \varepsilon \to 0 \quad \left(\Pr_{\omega\sim\mu}[F_{n,\varepsilon}] = 1 - O(n^{-d}\varepsilon^c) \text{ as } n \to \infty,\ \varepsilon \to 0\right). \tag{12}$$

2.3 Clifford+T gate synthesis

A set of single-qubit Pauli gates is defined as follows:

$$\mathrm{Pauli}_1 = \left\{ i^k \sigma \,\middle|\, k \in \mathbb{Z},\ \sigma \in \left\{ I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\} \right\}, \tag{13}$$

and a set of n-qubit Pauli gates is defined as follows:

$$\mathrm{Pauli}_n = \left\{ \bigotimes_{i=1}^{n} \sigma_i \,\middle|\, \sigma_i \in \mathrm{Pauli}_1 \right\}. \tag{14}$$

When a group operation is defined as the matrix product, it forms the n-qubit Pauli group, and its normalizer is the n-qubit Clifford group written as $\mathrm{Clifford}_n$. Ignoring the global phase, all elements of $\mathrm{Clifford}_n$ can be identified with elements that can be constructed using a finite number of H, S, and CNOT gates defined as follows (for $n = 1$, a CNOT gate is not needed):

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},\ S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix},\ \mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{15}$$

Adding the T gate defined below to the Clifford gate set yields Clifford+T, which allows approximation of any unitary with arbitrary precision:

$$T = \begin{pmatrix} 1 & 0 \\ 0 & \zeta \end{pmatrix}, \tag{16}$$

where $\zeta = e^{i\pi/4}$. Given a target n-qubit unitary $U \in \mathrm{U}(2^n)$ and an error $\varepsilon > 0$, Clifford+T gate synthesis within ε with n_a ancillae consists of finding a Clifford+T gate sequence that satisfies $D_\diamond(U, C_1T_1C_2T_2\cdots T_kC_{k+1}) < \varepsilon$, where $C_1, C_2, \cdots, C_{k+1} \in \mathrm{Clifford}_{n+n_a}$ and $T_1, T_2, \cdots, T_k$ are T gates on some qubits. T-count is the number of T gates in a Clifford+T gate sequence or circuit.

Some controlled gates can be exactly implemented by Clifford+T. Specifically, the controlled H gate $I_2 \oplus H$ can be exactly implemented by a T-count 2 Clifford+T circuit, and the controlled S gate $I_2 \oplus S$ can be exactly implemented by a T-count 3 Clifford+T circuit [1].

For single-qubit gate synthesis, Matsumoto and Amano's normal form expresses how Clifford+T behaves. It states that any Clifford+T circuit can be reduced to a T-count m circuit of the following form:

$$F\left(\prod_{i=1}^{m} M_i\right) C \qquad (F \in \{I_2,\, H,\, SH\},\, M_i \in \{TH,\, TSH\},\, C \in \mathrm{Clifford}_1). \tag{17}$$

Furthermore, among the Clifford+T circuits with the same unitary operation, this form is unique and has the minimum T-count.

3 n-qubit controlled gate synthesis

In this section, we prove our main result, Theorem 1, which we restate below:

Theorem 1 ($\mathrm{SU}(2)^{\oplus 2^n}$ controlled gate synthesis with optimal T-count)**.** *For $n \geq 1$, n-qubit controlled gates whose diagonal blocks are composed of SU(2) can be implemented up to error ε by a Clifford+T circuit using*

$$3\log_2(1/\varepsilon) + O\left(\sqrt{2^n \log(1/\varepsilon)}\right) + o\left(\log(1/\varepsilon)\right) \quad \text{w.h.p.} \tag{1}$$

T gates and ancillae. Furthermore, when n is fixed, no Clifford+T circuit with a diagonal block form can use asymptotically fewer T gates.

Note that only $3\log_2(1/\varepsilon) + O(n) + o(\log(1/\varepsilon))$ w.h.p. ancillae need to be clean in Equation (1) and the remaining ancillae can be dirty, i.e., their quantum state can be arbitrary. We will show that by constructing a Clifford+T circuit that approximates a given controlled gate, it can be approximated with a T-count represented by Equation (1). The qualifier w.h.p. here means

$$\exists \kappa > 0, \quad \forall \gamma, \iota > 0, \quad \exists c, d > 0,$$
$$\Pr\left[\left|\mathscr{T}_{n,\varepsilon} - \left(3\log_2(1/\varepsilon) + \kappa\sqrt{2^n \log_2(1/\varepsilon)}\right)\right| \leq \iota\sqrt{2^n \log_2(1/\varepsilon)} + \gamma \log_2(1/\varepsilon)\right] = 1 - O(n^{-d}\varepsilon^c). \tag{18}$$

Furthermore, from a discussion using channel representation, we will show a lower bound for the T-count for a fixed number of qubits and demonstrate that it matches Equation (1).

3.1 Circuit construction

Given a n-qubit controlled gate $U_1 \oplus U_2 \oplus \cdots \oplus U_{2^n} \in \mathrm{SU}(2)^{\oplus 2^n}$ and an error ε, we first apply ε-approximate single-qubit gate synthesis to each of $U_1, U_2, \cdots, U_{2^n}$ and obtain 2^n Clifford+T even-number T-count m_i circuits (we can always have even-number T-count circuits; see details in Appendix A for the proof.) in Matsumoto and Amano's normal form (Equation (17)):

$$D_\diamond\left(U_i,\, F_i\left(\prod_{j=1}^{m_i} M_{j,i}\right) C_i\right) < \varepsilon \quad (i = 1, 2, \cdots, 2^n,\, F_i \in \{I_2,\, H,\, SH\},\, M_{j,i} \in \{TH,\, TSH\},\, C_i \in \mathrm{Clifford}_1). \tag{19}$$

By multiplying a complex number of unit modulus, we can set C_i to be in the form of the product of S and H gates. We will use the following form, which is equivalent to the one derived by Matsumoto and Amano's normal form:

$$D_\diamond\left(F_i\left(\prod_{j=1}^{m_i} M_{j,i}\right)C_i,\ \ \zeta^{s_i}F_i\left(\prod_{j=1}^{\frac{m_i+m}{2}} M'_{j,i}\right)H\left(\prod_{j=\frac{m_i+m}{2}+1}^{m} M'_{j,i}\right)C'_i\right)=0 \tag{20}$$

$$\left(M'_{j,i}=\begin{cases}\zeta TH & \text{if } j\le m_i \text{ and } M_{j,i}=TH,\\ TSH & \text{if } j\le m_i \text{ and } M_{j,i}=TSH,\\ \zeta TH & \text{if } m_i+1\le j\le \frac{m_i+m}{2},\\ \zeta TH & \text{if } \frac{m_i+m}{2}+1\le j \text{ and } j\equiv \frac{m_i+m}{2}+2 \mod 3,\\ TSH & \text{otherwise,}\end{cases} \quad C'_i=\begin{cases}HZC_i & \text{if } \frac{m-m_i}{2}\equiv 1 \mod 3,\\ HXC_i & \text{if } \frac{m-m_i}{2}\equiv 2 \mod 3,\\ HC_i & \text{if } \frac{m-m_i}{2}\equiv 0 \mod 3\end{cases}\right),$$

where s_i is chosen from $\{0,1,\cdots,7\}$ such that the second argument in Equation (20) is closest to U_i in the Frobenius norm (to ensure that its eigenvalues become sufficiently close to that of U_i's) and $m=\max_i m_i$. Equation (20) holds because

$$(TH)^\dagger = HTSH\cdot HZ, \tag{21}$$
$$(THTH)^\dagger = \zeta^{-1}HTSHTH\cdot HX, \tag{22}$$
$$(THTHTH)^\dagger = \zeta^{-1}HTSHTHTSH\cdot H. \tag{23}$$

Then, we consider a circuit that consists of the following subcircuits to approximate U within the error ε, where $\mathscr{A},\mathscr{B},\mathscr{C},\mathscr{D}$ are quantum registers with $n,1,2m-\min_i(m_i)+O(1),O(\sqrt{m2^n})$ qubits each ($\mathscr{A}$ is composed of the control qubits of U, $\mathscr{B}$ is composed of the target qubit of U, $\mathscr{C}$ is composed of clean ancillae initialized to $|0\rangle$, and $\mathscr{D}$ is composed of dirty ancillae):

1. (Boolean layer) controlled Boolean function on $\mathscr{AC}$ using $\mathscr{D}$;
2. controlled gates on $\mathscr{BC}$;
3. inverse Boolean layer to make C clean again.

The details of each subcircuit are described below.

For any Boolean function $f:\{0,1\}^n\to\{0,1\}^b$, we can implement a unitary U_f defined as below by the divide-and-conquer method [8]:

$$U_f|x\rangle|y\rangle=|x\rangle|y\oplus f(x)\rangle \qquad (x=0,1,\cdots,2^n,\ y=0,1,\cdots,2^b). \tag{24}$$

Lemma 7 (Boolean oracle)**.** *Let $f:\{0,1\}^n\to\{0,1\}^b$ be an arbitrary Boolean function. U_f can be exactly implemented by a Clifford+T circuit using*

$$O(\sqrt{b2^n}) \tag{25}$$

T gates and dirty ancillae.

By using Lemma 7, we implement the product of the following block matrices, defined using s_i, F_i, $M'_{j,i}$, and C'_i from Equation (20):

$$\left(\bigoplus_{i=1}^{2^n} U'_i\right)=\left(\bigoplus_{i=1}^{2^n}\zeta^{s_i}I_2\right)\left(\bigoplus_{i=1}^{2^n}F_i\right)\prod_{j=1}^{l-1}\left(\bigoplus_{i=1}^{2^n}M'_{j,i}\right)\prod_{j=l}^{m}\left(\left(\bigoplus_{i=1}^{2^n}M'_{j,i}\right)\left(\bigoplus_{i=1}^{2^n}H_{j,i}\right)\right)\left(\bigoplus_{i=1}^{2^n}C'_i\right), \tag{26}$$

where $l = \frac{m+\min_i(m_i)}{2}$, U_i' is defined as the second term of the diamond distance function appeared in Equation (20), and

$$H_{j,i} = \begin{cases} H & \text{if } \frac{m_i+m}{2} = j, \\ I_2 & \text{otherwise.} \end{cases} \tag{27}$$

From Equation (26), we can define a Boolean function $g : \{0,1\}^n \to \{0,1\}^b$ ($b = 2m-l+10$) as follows:

$$g(i)_j = \begin{cases} d_{2c+1-j,i} & \text{if } j \le 2c, \\ 0 & \text{if } 2c < j \le 2m-2l+2c+2 \text{ and } j \text{ is odd and } H_{m+c-(j-1)/2,i} \neq H, \\ 1 & \text{if } 2c < j \le 2m-2l+2c+2 \text{ and } j \text{ is odd and } H_{m+c-(j-1)/2,i} = H, \\ 0 & \text{if } 2c < j \le 2m-2l+2c+2 \text{ and } j \text{ is even and } M'_{m+c-(j-2)/2,i} \neq \zeta TH, \\ 1 & \text{if } 2c < j \le 2m-2l+2c+2 \text{ and } j \text{ is even and } M'_{m+c-(j-2)/2,i} = \zeta TH, \\ 0 & \text{if } 2m-2l+2c+2 < j \le 2m-l+2c+1 \text{ and } M'_{2m-l+2c+2-j,i} \neq \zeta TH, \\ 1 & \text{if } 2m-2l+2c+2 < j \le 2m-l+2c+1 \text{ and } M'_{2m-l+2c+2-j,i} = \zeta TH, \\ 0 & \text{if } j = 2m-l+2c+2 \text{ and } F_i = I_2, \\ 1 & \text{if } j = 2m-l+2c+2 \text{ and } F_i \neq I_2, \\ 0 & \text{if } j = 2m-l+2c+3 \text{ and } F_i \neq SH, \\ 1 & \text{if } j = 2m-l+2c+3 \text{ and } F_i = SH, \\ 0 & \text{if } 2m-l+2c+3 < j \text{ and } s_i < j-(2m-l+2c+3), \\ 1 & \text{if } 2m-l+2c+3 < j \text{ and } s_i \ge j-(2m-l+2c+3), \end{cases} \tag{28}$$

where $g(i)_j$ is the j-th element of $g(i)$ ($j \in \{1,2,\cdots,b\}$), c is the minimum number of S and H gates to implement all C_i', and $d_{j,i}$ is defined as

$$C_i' = S^{d_{1,i}} H^{d_{2,i}} S^{d_{3,i}} H^{d_{4,i}} \cdots S^{d_{2c-1,i}} H^{d_{2c,i}}. \tag{29}$$

Then, a Boolean layer in the list of subcircuits is defined as U_g whose controlled qubits are in $\mathscr{A}$ and target qubits are in $\mathscr{C}$. Clifford+T can implement it as a result of Lemma 7 by using $\mathscr{D}$ as dirty ancillae. After applying a Boolean layer to $\mathscr{A}\mathscr{C}$, we apply controlled gates sequentially. For each j, we apply a controlled gate $P_j \oplus Q_j$, controlled by the j-th qubit of $\mathscr{C}$ and targeting the qubit in $\mathscr{B}$. P_j and Q_j are determined as follows:

$$(P_j,\ Q_j) = \begin{cases} (I_2,\ H) & \text{if } j \le 2c \text{ and } j \text{ is odd}, \\ (I_2,\ S) & \text{if } j \le 2c \text{ and } j \text{ is even}, \\ (I_2,\ H) & \text{if } 2c < j \le 2m-2l+2c+2 \text{ and } j \text{ is odd}, \\ (TSH,\ \zeta TH) & \text{if } 2c < j \le 2m-2l+2c+2 \text{ and } j \text{ is even}, \\ (TSH,\ \zeta TH) & \text{if } 2m-2l+2c+2 < j \le 2m-l+2c+1, \\ (I_2,\ H) & \text{if } j = 2m-l+2c+2, \\ (I_2,\ S) & \text{if } j = 2m-l+2c+3, \\ (I_2,\ \zeta I_2) & \text{if } 2m-l+2c+3 < j. \end{cases} \tag{30}$$

Finally, applying the inverse Boolean layer restores a product structure of the global state. In particular, the register $\mathscr{C}$ returns to the state $|0\rangle$ and becomes factorized from $\mathscr{A}\mathscr{B}$. It finishes the implementation of $U_1' \oplus U_2' \oplus \cdots \oplus U_{2^n}'$, where it controls the qubit in $\mathscr{B}$ from the qubits in $\mathscr{A}$.

Eventually, the gate represented as Equation (26) is implemented. Since the T-count is an even number for the approximate syntheses of $U_1, U_2, \cdots, U_{2^n}$ and s_i was chosen to minimize the Frobenius norm, the eigenvalues for each $U_j^\dagger U_j'$ can be written as $e^{i\theta_j}$ and $e^{-i\theta_j}$, where

$$-\frac{\pi}{2} \leq \theta_j \leq \frac{\pi}{2} \text{ and } |\sin\theta_j| < \varepsilon. \tag{31}$$

Thus,

$$D_\diamond(U_1 \oplus U_2 \oplus \cdots \oplus U_{2^n},\ U_1' \oplus U_2' \oplus \cdots \oplus U_{2^n}') = \max_{j\in\{1,2,\cdots,2^n\}} D_\diamond(U_j,\ U_j') < \varepsilon. \tag{32}$$

3.2 T-count analysis

In this section, we will prove Theorem 1. To estimate the maximum length m of Matsumoto and Amano's normal form in Section 3.1, we will show the following lemma:

Lemma 8 (Bound on T-count of SU(2) Syntheses)**.** *Let $\mathscr{T}_\varepsilon(U)$ for $U \in \mathrm{SU}(2)$ be the minimum even-number T-count to approximate U within an error ε by a Clifford+T circuit. Then, for $U_1, U_2, \cdots, U_k \in \mathrm{SU}(2)$, the following two equations hold*

$$\max_{i\in\{1,2,\cdots,k\}} \mathscr{T}_\varepsilon(U_i) = 3\log_2(1/\varepsilon) + O(\log(k)) + o(\log(1/\varepsilon)) \quad \text{w.h.p.}, \tag{33}$$

and

$$\min_{i\in\{1,2,\cdots,k\}} \mathscr{T}_\varepsilon(U_i) = 3\log_2(1/\varepsilon) - O(\log(k)) - o(\log(1/\varepsilon)) \quad \text{w.h.p.} \tag{34}$$

Proof of Lemma 8. For any $\gamma > 0$,

$$\Pr[\mathscr{T}_\varepsilon(U) > (3+\gamma)\log_2(1/\varepsilon)] = O(\varepsilon^\gamma \mathrm{polylog}(1/\varepsilon)), \tag{35}$$

and

$$\Pr[\mathscr{T}_\varepsilon(U) \leq (3-\gamma)\log_2(1/\varepsilon)] = O(\varepsilon^\gamma), \tag{36}$$

hold (see details in Appendix A for the proof.). By Equation (35), for any $\gamma > 0$ and any $\iota > 1$,

$$\begin{aligned} \Pr\left[\max_{i\in\{1,2,\cdots,k\}} \mathscr{T}_\varepsilon(U_i) > (3+\gamma)\log_2(1/\varepsilon) + \iota\log_2(k)\right] &\leq k\Pr[\mathscr{T}_\varepsilon(U) > (3+\gamma)\log_2(1/\varepsilon) + \iota\log_2(k)] \\ &= O(k^{-(\iota-1)}\varepsilon^\gamma \mathrm{polylog}(1/\varepsilon)), \end{aligned} \tag{37}$$

and

$$\begin{aligned} \Pr\left[\min_{i\in\{1,2,\cdots,k\}} \mathscr{T}_\varepsilon(U_i) > (3+\gamma)\log_2(1/\varepsilon)\right] &= \Pr[\mathscr{T}_\varepsilon(U) > (3+\gamma)\log_2(1/\varepsilon)]^k \\ &\leq O(k^{-(\iota-1)}\varepsilon^\gamma \mathrm{polylog}(1/\varepsilon)). \end{aligned} \tag{38}$$

By Equation (36), for any $\gamma > 0$ and any $\iota > 1$

$$\begin{aligned} \Pr\left[\min_{i\in\{1,2,\cdots,k\}} \mathscr{T}_\varepsilon(U_i) \leq (3-\gamma)\log_2(1/\varepsilon) - \iota\log_2(k)\right] &\leq k\Pr[\mathscr{T}_\varepsilon(U) < (3-\gamma)\log_2(1/\varepsilon) - \iota\log_2(k)] \\ &\leq O(k^{-(\iota-1)}\varepsilon^\gamma), \end{aligned} \tag{39}$$

and

$$\begin{aligned}\Pr\left[\max_{i\in\{1,2,\cdots,k\}}\mathscr{T}_\varepsilon(U_i)\leq(3-\gamma)\log_2(1/\varepsilon)\right] &\leq \Pr[\mathscr{T}_\varepsilon(U)\leq(3-\gamma)\log_2(1/\varepsilon)]^k\\ &\leq O(k^{-(\iota-1)}\varepsilon^\gamma).\end{aligned}\tag{40}$$

Combining Equations (37) and (40) yields Equation (33). Combining Equations (38) and (39) yields Equation (34). □

Proof of Theorem 1. First, we count the number of T gates and ancillae in Section 3.1 and show that they match the values in Equation (1). Lemma 8 implies that

$$m=3\log_2(1/\varepsilon)+O(\log(k))+o(\log(1/\varepsilon))\quad\text{w.h.p.},\tag{41}$$

and

$$m-l=O(\log(k))+o(\log(1/\varepsilon))\quad\text{w.h.p.},\tag{42}$$

where k is the number of types of SU(2) appearing in $U_1,U_2,\cdots,U_{2^n}$. Furthermore, the following equations hold:

$$\begin{aligned}TSH\oplus\zeta TH &= STH\oplus SXTXH\\ &= (I_2\otimes S)\mathrm{CNOT}(I_2\otimes T)\mathrm{CNOT}(I_2\otimes H),\end{aligned}\tag{43}$$

and

$$I_2\oplus(\zeta I_2)=T\otimes I_2.\tag{44}$$

With these in hand, all $P_j\oplus Q_j$ in Equation (30) can be implemented by

$$m+2(m-l)+5c+14=3\log_2(1/\varepsilon)+O(\log(k))+o(\log(1/\varepsilon))\quad\text{w.h.p.}\tag{45}$$

T gates and no ancilla. Since m can also be written as $O(\log(1/\varepsilon))$ for any target SU(2) [13], Lemma 7 assures that $O\left(\sqrt{2^n\log(1/\varepsilon)}\right)$ T gates and ancillae are enough to implement the Boolean layer and its inverse by a Clifford+T gate set. The whole algorithm uses the following number of T gates and ancillae matching the value in Equation (1):

$$3\log_2(1/\varepsilon)+O\left(\sqrt{2^n\log(1/\varepsilon)}\right)+o(\log(1/\varepsilon))\quad\text{w.h.p.}\tag{46}$$

Second, we calculate the lower bound of the T-count from discussions using channel representation and show that it matches Equation (1) when n is fixed. Since

$$\begin{aligned}\left(\sum_{\sigma\in S_n}\sigma_{i,i}\sigma\right)\otimes I_2=\left(\bigoplus_{j=1}^{i-1}\begin{pmatrix}0&0\\0&0\end{pmatrix}\right)\oplus(2^nI_2)\oplus\left(\bigoplus_{j=i+1}^{2^n}\begin{pmatrix}0&0\\0&0\end{pmatrix}\right)\\ \left(i\in\{1,2,\cdots,2^n\},\ S_n=\left\{\bigotimes_{j=1}^n\sigma_j\,\middle|\,\sigma_j\in\{I_2,\,Z\}\right\}\right),\end{aligned}\tag{47}$$

the following equation holds for a Clifford+T circuit $V_1\oplus V_2\oplus\cdots\oplus V_{2^n}$:

$$\left(\widehat{V_i}\right)_{a,b}=\sum_{k\in K}(P_k)_{i,i}\left(\widehat{\bigoplus_{l=1}^{2^n}V_l}\right)_{4k+a,b},\tag{48}$$

where K is a set of integers from 0 to 4^n-1 whose base-4 representation contains only digits 0 and 3 and P_k here is what is defined at Equation (10). The channel representation of Clifford gates only has 0 or ± 1 for their matrix elements from their definition and

$$\widehat{T} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \tag{49}$$

so the smallest denominator exponent (sde) defined below becomes the lower bound for the T-count of a Clifford+T circuit $V \in \mathrm{SU}(2^n)$:

$$sde(\widehat{V}) = \max_{i,j} \left(\arg\min_{k \geq 0} \left(\sqrt{2}^k \left(\widehat{V} \right)_{i,j} \in \mathbb{Z}[\sqrt{2}] \right) \right). \tag{50}$$

(For a single-qubit case, this lower bound coincides with the minimum T-count [3].) Let $\bigoplus_{l=1}^{2^n} V_l$ be a Clifford+T circuit and satisfy $D_\diamond(\tilde{V}, \bigoplus_{l=1}^{2^n} V_l) \leq \varepsilon$ for a target unitary $\tilde{V} = \bigoplus_{l=1}^{2^n} \tilde{V}_l$. Thus, the following inequality holds:

$$\begin{aligned} \mathscr{T}_0 \left(\bigoplus_{l=1}^{2^n} V_l \right) &\geq sde \left(\widehat{\bigoplus_{l=1}^{2^n} V_l} \right) \\ &\geq \max_l sde \left(\widehat{V_l} \right) \qquad (51) \\ &= \max_l \mathscr{T}_0(V_l). \qquad (52) \end{aligned}$$

Since $\varepsilon \geq D_\diamond(\tilde{V}, \bigoplus_{l=1}^{2^n} V_l) = \max_l D_\diamond(\tilde{V}_l, V_l)$, we can safely say that at least

$$3\log_2(1/\varepsilon) - o(\log(1/\varepsilon)) \quad \text{w.h.p.} \tag{53}$$

T-counts are required for an ε-approximation of $\mathrm{SU}(2)^{\oplus 2^n}$ when the form of the Clifford+T circuit for the approximation is restricted to a block-diagonal form $\mathrm{U}(2)^{\oplus 2^n}$. This value matches Equation (1) when n is fixed. □

3.3 Ancilla-free controlled gate synthesis

In Section 3.1, controlled gates $P_j \oplus Q_j$ in Equation (30) take the qubits in $\mathscr{C}$ as control qubits and the qubit in $\mathscr{B}$ as a target qubit. However, if we limit ourselves to the 2-qubit case (i.e., $n = 1$), we can construct an equivalent Clifford+T circuit without ancilla.

Theorem 2 ($\mathrm{SU}(2) \oplus \mathrm{SU}(2)$ ancilla-free controlled gate synthesis)**.** *Controlled gates whose diagonal blocks are composed of SU(2) can be implemented up to error ε by a Clifford+T circuit using*

$$3\log_2(1/\varepsilon) + o(\log(1/\varepsilon)) \quad \text{w.h.p.} \tag{2}$$

T gates and without ancilla.

Furthermore, no Clifford+T circuit with a diagonal block form can use asymptotically fewer T gates.

Proof of Theorem 2. Since $\mathscr{A}$ is a single-qubit register when $n = 1$, multi-bit control at Section 3.1 is just single-bit control. Thus, by directly using the qubit in $\mathscr{A}$ as the control qubit instead of controlling via qubits in $\mathscr{C}$, the need for the Boolean layers is eliminated, allowing an ancilla-free Clifford+T circuit to be constructed for the approximation. The T-count for it is the same as Equation (45) with $k \leq 2$. This T-count coincides with Equation (2) and the lower bound provided in the previous section (Equation (53)). □

4 Applications

In this section, we present several applications of Theorems 1 and 2. First, Theorem 1 can be generalized to cover the synthesis of unitaries from $\mathrm{SU}(2)^{\oplus 2^n}$ to $\mathrm{U}(2)^{\oplus 2^n}$.

Theorem 3 (Controlled gate synthesis)**.** *For $n \geq 1$, n-qubit controlled gates can be implemented up to error ε as a CPTP mapping by a Clifford+T circuit using*

$$6\log_2(1/\varepsilon) + O\left(\sqrt{2^n \log(1/\varepsilon)}\right) + o\left(\log(1/\varepsilon)\right) \quad \text{w.h.p.} \tag{3}$$

T gates and ancillae.

Proof of Theorem 3. Let $U_1 \oplus U_2 \oplus \cdots \oplus U_{2^n}$ be an arbitrary element of $\mathrm{U}(2)^{\oplus 2^n}$. It can be decomposed into two matrices

$$\bigoplus_{j=1}^{2^n} U_j = \left(\bigoplus_{j=1}^{2^n} V_j\right)\left(\bigoplus_{j=1}^{2^n} e^{i\theta_j} I_2\right) \qquad (V_j \in \mathrm{SU}(2),\ \theta_j \in [0, 2\pi)). \tag{54}$$

The first gate can be approximately synthesized within an error of $\varepsilon/2$ as a consequence of Theorem 1. The second gate can be approximately implemented by adding one clean ancilla initialized to $|0\rangle$. When $D = \mathrm{diag}(e^{i\theta_1}, e^{i\theta_2}, \cdots, e^{i\theta_{2^n}})$, $D \oplus D^\dagger$ becomes $\bigoplus_{j=1}^{2^n} \begin{pmatrix} e^{i\theta_j} & 0 \\ 0 & e^{-i\theta_j} \end{pmatrix} \in \mathrm{SU}(2)^{\oplus 2^n}$ by conjugating by swap gates, so it can be approximated by a Clifford+T circuit E with an error within $\varepsilon/2$, according to Theorem 1:

$$D_\diamond(\mathscr{E}_{D\oplus D^\dagger}, \mathscr{E}_E) < \frac{\varepsilon}{2}. \tag{55}$$

Let $\mathscr{D}$ be an n-qubit state to n-qubit state CPTP mapping consisting of ancilla addition, E, and ancilla trace-out. Then $\mathscr{D}$ will have a diamond distance of less than $\varepsilon/2$ from $\mathscr{E}_D$ [15]. Combining these two yields the CPTP mapping approximating the target gate $U_1 \oplus U_2 \oplus \cdots \oplus U_{2^n}$. Since we used Theorem 1 twice for $SU(2)^{\oplus 2^n}$ and no T gate other than that, the total number of T gates and ancillae becomes the one in Equation (3). □

Second, $\mathrm{SU}(2)^{\oplus 2^n}$ can be synthesized without ancilla using the proof of Theorem 2. Before that, we will show the following useful lemma:

Lemma 9 (SU(2) synthesis subroutine by $\mathrm{SU}(2) \oplus \mathrm{SU}(2)$)**.** *Given $U \in \mathrm{SU}(2)$, an ancilla-free Clifford+T circuit with*

$$1.5\log_2(1/\varepsilon) + o(\log(1/\varepsilon)) \quad \text{w.h.p.} \tag{56}$$

T-count that has the form

$$U_1 \oplus U_2 \in \mathrm{SU}(2) \oplus \mathrm{SU}(2) \ \ s.t.\ \ D_\diamond(U_1 U_2^\dagger, U) < \varepsilon \tag{57}$$

can be constructed.

Proof of Lemma 9. There exists a Clifford+T gate sequence that approximates U with an even-number T-count and a $3\log_2(1/\varepsilon)+o(\log(1/\varepsilon))$ w.h.p. T-count. This sequence is divided into two halves, one denoted as U_1' and the other as $U_2'^{\dagger}$, such that the T-count is halved. When the circuit construction method from the proof of Theorem 2 is applied, $U_1' \oplus U_2'$ can be constructed as an ancilla-free circuit with a T-count of $1.5\log_2(1/\varepsilon)+o(\log(1/\varepsilon))$ w.h.p. □

Theorem 4 ($\mathrm{SU}(2)^{\oplus 2^n}$ ancilla-free controlled gate synthesis)**.** *For $n \geq 2$, n-qubit controlled gates whose diagonal blocks are composed of SU(2) can be implemented up to error ε by a Clifford+T circuit using*

$$\frac{3(2^n+1)}{2}\log_2(1/\varepsilon)+O(n2^n)+o\left(2^n\log(1/\varepsilon)\right) \quad \text{w.h.p.} \tag{4}$$

T gates and without ancilla.

Proof of Theorem 4. By using Lemma 9 (2^n-1) times and one SU(2) synthesis for an error $\varepsilon/2^n$, an ancilla-free Clifford+T circuit can be constructed that approximates $\mathrm{SU}(2)^{\oplus 2^n}$ within an error ε [16]. Considering Lemma 8, the total T-count is

$$((2^n-1)\,(1.5\log_2(2^n/\varepsilon)+O(n)+o(\log(1/\varepsilon))))+(3\log_2(1/\varepsilon)+o(\log(1/\varepsilon))) \quad \text{w.h.p.} \tag{58}$$

This matches Equation (4). □

Third, SU(4) can be approximately synthesized by using Theorem 2 and Lemma 9.

Theorem 5 (SU(4) gate synthesis)**.** *SU(4) gates can be implemented up to error ε by a Clifford+T circuit using*

$$9\log_2(1/\varepsilon)+o(\log(1/\varepsilon)) \quad \text{w.h.p.} \tag{5}$$

T gates and without ancilla.

Proof of Theorem 5. $\mathrm{SU}(4)/\mathbb{Z}_2$ is known to be isomorphic to SO(6). If the basis is chosen appropriately, the $4^2-1=15$ Pauli-direction rotations of SU(4) correspond to $\binom{6}{2}=15$ rotations in planes parallel to two axes. The correspondence is listed at Appendix B.

Let U be a member of SU(4). First, we decompose U into the following six matrices:

$$U = e^{i\theta_1 X\otimes I_2}e^{i\theta_2 Y\otimes I_2}e^{i\theta_3 Z\otimes X}e^{i\theta_4 Z\otimes Y}e^{i\theta_5 Z\otimes Z}U_1 \qquad ((\text{SO(6) representation of } U_1)\in \mathrm{SO}(5)\oplus\{I_1\}). \tag{59}$$

By Lemma 9, we can construct a Clifford+T circuit $V_1\oplus V_2$ with T-count $1.5\log_2(1/\varepsilon)+o(\log(1/\varepsilon))$ w.h.p. that satisfies $D_\diamond(V_1V_2^\dagger,\ e^{i\theta_3 X}e^{i\theta_4 Y}e^{2i\theta_5 Z}e^{i\theta_4 Y}e^{i\theta_3 X})<\varepsilon/4$.

Second, we decompose $\left(I_2\otimes\left(V_1^\dagger e^{i\theta_3 X}e^{i\theta_4 Y}e^{i\theta_5 Z}\right)\right)U_1$ into the following five matrices:

$$\left(I_2\otimes\left(V_1^\dagger e^{i\theta_3 X}e^{i\theta_4 Y}e^{i\theta_5 Z}\right)\right)U_1 = e^{i\theta_6 Z\otimes I_2}e^{i\theta_7 Y\otimes X}e^{i\theta_8 Y\otimes Y}e^{i\theta_9 Y\otimes Z}U_2$$

$$((\text{SO(6) representation of } U_2)\in \mathrm{SO}(4)\oplus\{I_2\}). \tag{60}$$

The single-qubit gate synthesis allows us to synthesize a T-count $3\log_2(1/\varepsilon)+o(\log(1/\varepsilon))$ w.h.p. Clifford+T circuit V_3 to approximate $e^{i\theta_1 X}e^{i\theta_2 Y}e^{i\theta_6 Z}$ within an error of $\varepsilon/4$. By Lemma 9, we can also construct a Clifford+T circuit $V_4\oplus V_5$ with T-count $1.5\log_2(1/\varepsilon)+o(\log(1/\varepsilon))$ w.h.p. that satisfies $D_\diamond(V_4V_5^\dagger, e^{i\theta_7 X}e^{i\theta_8 Y}e^{2i\theta_9 Z}e^{i\theta_8 Y}e^{i\theta_7 X})<\varepsilon/4$.

Third, since $\left(I_2 \otimes \left(V_4^\dagger e^{i\theta_7 X} e^{i\theta_8 Y} e^{i\theta_9 Z}\right)\right)(H \otimes I_2)U_2(H \otimes I_2) \in \mathrm{SU}(2) \oplus \mathrm{SU}(2)$, it can be approximately synthesized by $3\log_2(1/\varepsilon) + o(\log(1/\varepsilon))$ w.h.p. T-count circuit $V_6 \oplus V_7$ within an error $\varepsilon/4$ by Theorem 2.

After these three steps, we can have

$$(V_3 \otimes I_2)(V_1 \oplus V_2)(SH \otimes I_2)(V_4 \oplus V_5)\left(HS^\dagger H \otimes I_2\right)(V_6 \oplus V_7)(H \otimes I_2) \tag{61}$$

that approximates the target U within an error ε (see details in Appendix C).

□

Acknowledgments

SY is supported by JSPS KAKENHI Grant No. JP24KJ0907 and the Forefront Physics and Mathematics Program to Drive Transformation (FoPM). SA is partially supported by JST PRESTO Grant No.JPMJPR2111, JST Moonshot R&D MILLENNIA Program (Grant No.JPMJMS2061), JPMXS0120319794, and CREST (Japan Science and Technology Agency) Grant No.JPMJCR2113.

References

[1] Matthew Amy, Dmitrii L. Maslov, Michele Mosca & Martin Rötteler (2012): 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, pp. 818–830.

[2] Sergey Bravyi & Alexei Kitaev (2005): Universal quantum computation with ideal Clifford gates and noisy ancillas. *Phys. Rev. A* 71, p. 022316, doi:10.1103/PhysRevA.71.022316. Available at https://link.aps.org/doi/10.1103/PhysRevA.71.022316.

[3] David Gosset, Vadym Kliuchnikov, Michele Mosca & Vincent Russo (2014): An algorithm for the T-count. *Quantum Info. Comput.* 14(15–16), p. 1261–1276.

[4] David Gosset, Robin Kothari & Kewen Wu: Quantum State Preparation with Optimal T-Count, pp. 3378–3406. doi:10.1137/1.9781611978971.122. arXiv:https://epubs.siam.org/doi/pdf/10.1137/1.9781611978971.122.

[5] Vadym Kliuchnikov, Kristin Lauter, Romy Minko, Adam Paetznick & Christophe Petit (2023): Shorter quantum circuits via single-qubit gate approximation. *Quantum* 7, p. 1208, doi:10.22331/q-2023-12-18-1208. Available at https://doi.org/10.22331/q-2023-12-18-1208.

[6] Guang Hao Low & Isaac L. Chuang (2017): Optimal Hamiltonian Simulation by Quantum Signal Processing. *Phys. Rev. Lett.* 118, p. 010501, doi:10.1103/PhysRevLett.118.010501. Available at https://link.aps.org/doi/10.1103/PhysRevLett.118.010501.

[7] Guang Hao Low & Isaac L. Chuang (2019): Hamiltonian Simulation by Qubitization. *Quantum* 3, p. 163, doi:10.22331/q-2019-07-12-163. Available at https://doi.org/10.22331/q-2019-07-12-163.

[8] Guang Hao Low, Vadym Kliuchnikov & Luke Schaeffer (2018): Trading T gates for dirty qubits in state preparation and unitary synthesis. *Quantum* 8, p. 1375.

[9] Hayata Morisaki, Kaoru Sano & Seiseki Akibue (2025): Optimal ancilla-free Clifford+T synthesis for general single-qubit unitar arXiv:2510.05816.

[10] Michael A. Nielsen & Isaac L. Chuang (2010): Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge University Press.

[11] Ori Parzanchevski & Peter Sarnak (2018): Super-Golden-Gates for PU(2). *Advances in Mathematics* 327, pp. 869–901, doi:https://doi.org/10.1016/j.aim.2017.06.022. Available at https://www.sciencedirect.com/science/article/pii/S0001870817301640. Special volume honoring David Kazhdan.

[12] Neil J. Ross & Peter Selinger (2016): Optimal ancilla-free Clifford+T approximation of z-rotations. *Quantum Info. Comput.* 16(11–12), p. 901–953.

[13] Peter Selinger (2015): Efficient Clifford+T approximation of single-qubit operators. *Quantum Info. Comput.* 15(1–2), p. 159–180.

[14] Robert R. Tucci (2005): An Introduction to Cartan's KAK Decomposition for QC Programmers. arXiv:quant-ph/0507171.

[15] John Watrous (2018): The Theory of Quantum Information. Cambridge University Press.

[16] Soichiro Yamazaki & Seiseki Akibue (2025): Clifford+V synthesis for multi-qubit unitary gates. arXiv:2510.08312.

A Even-number T-count SU(2) synthesis

Morisaki et al. showed that every $U \in \mathrm{SU}(2)$ can be synthesized by

$$3\log_2(1/\varepsilon) + o(\log(1/\varepsilon)) \quad \text{w.h.p.} \tag{62}$$

T gates [9]. In this section, we prove that a Clifford+T circuit can be constructed that approximates a single-qubit gate, consists of an even number of T gates, and has the same asymptotic T-count scale as Equation (62).

Lemma 10 (even-number T-count SU(2) gate synthesis)**.** *Single-qubit gate SU(2) can be implemented up to error ε by an ancilla-free Clifford+T circuit using*

$$3\log_2(1/\varepsilon) + o(\log(1/\varepsilon)) \quad \text{w.h.p.} \tag{63}$$

T gates even if the T-count is limited to even numbers.

Proof of Lemma 10. U(2) gates that can be exactly constructed with an even number of T gates can be reduced to the following form by adjusting their phase:

$$U = \begin{pmatrix} u_1 & -u_2^\dagger \\ u_2 & u_1^\dagger \end{pmatrix} \qquad \left(u_1, u_2 \in \mathbb{Z}\left[\frac{1}{\sqrt{2}}, i\right] \right). \tag{64}$$

For some non-negative integers k, a subset of $(\mathbb{Z}[1/\sqrt{2}])^4$, consisting of the real and imaginary parts of u_1, u_2 of U such that $k \geq sde(U)$, becomes a subset of $(\mathbb{Z}[\sqrt{2}])^4$ by multiplying all its elements by $\sqrt{2}^k$.

Let $S(m) = \{(a,\ b,\ c,\ d) \in (\mathbb{Z}[\sqrt{2}])^4 |\ a^2+b^2+c^2+d^2 = m\}$ and $\mathscr{T}_\varepsilon(U)$ be the minimum even number T-count for the ε-approximation of U. Then, the following equation holds [9]:

$$|S(m)| \geq N((m)), \tag{65}$$

where $N(\cdot)$ denotes the norm map. From [11] and [9], for any $\gamma > 0$ and $t \in \{0, 1, 2, \cdots\}$,

$$\Pr[\mathscr{T}_\varepsilon(U) > 2t] = O\left(\frac{N((2^t)) \left(\sum_{(k)|(2^t)} 1 \right)^2}{S(2^t)^2 B(\varepsilon)} \right) = O\left(\frac{t^2}{2^{2t}\varepsilon^3} \right). \tag{66}$$

Thus,

$$\Pr[\mathscr{T}_\varepsilon(U) > (3+\gamma)\log_2(1/\varepsilon)] = O(\varepsilon^\gamma \mathrm{polylog}(1/\varepsilon)). \tag{67}$$

By [9],

$$\Pr[\mathscr{T}_\varepsilon(U) \leq (3-\gamma)\log_2(1/\varepsilon)] \leq O(\varepsilon^\gamma). \tag{68}$$

□

B Correspondence between SU(4) and SO(6)

There exists an isomorphism between $\mathrm{SU}(4)/\mathbb{Z}_2$ and $\mathrm{SO}(6)$ whose correspondence between Paulis and rotations in planes parallel to two axes is as follows:

$$\begin{aligned}
&I_2\otimes X \leftrightarrow (2,3),\ I_2\otimes Y \leftrightarrow (1,3),\ I_2\otimes Z \leftrightarrow (1,2),\\
&X\otimes I_2 \leftrightarrow (5,6),\ Y\otimes I_2 \leftrightarrow (4,6),\ Z\otimes I_2 \leftrightarrow (4,5),\\
&X\otimes X \leftrightarrow (1,4),\ Y\otimes X \leftrightarrow (1,5),\ Z\otimes X \leftrightarrow (1,6),\\
&X\otimes Y \leftrightarrow (2,4),\ Y\otimes Y \leftrightarrow (2,5),\ Z\otimes Y \leftrightarrow (2,6),\\
&X\otimes Z \leftrightarrow (3,4),\ Y\otimes Z \leftrightarrow (3,5),\ Z\otimes Z \leftrightarrow (3,6).
\end{aligned} \tag{69}$$

C Diamond distance between target SU(4) and its approximation

Lemma 11 (Diamond distance between target SU(4) and its approximation)**.** *Let* $V_1,V_2,V_3,V_4,V_5,V_6,V_7 \in \mathrm{SU}(2)$, $U,U_1,U_2 \in \mathrm{SU}(4)$ *and* $\varepsilon > 0$ *that satisfies the following conditions:*

$$U = e^{i\theta_1 X\otimes I_2} e^{i\theta_2 Y\otimes I_2} e^{i\theta_3 Z\otimes X} e^{i\theta_4 Z\otimes Y} e^{i\theta_5 Z\otimes Z} U_1 \qquad (\textit{(SO(6) representation of } U_1) \in \mathrm{SO}(5)\oplus\{I_1\}), \tag{70}$$

$$\left(I_2\otimes\left(V_1^\dagger e^{i\theta_3 X} e^{i\theta_4 Y} e^{i\theta_5 Z}\right)\right) U_1 = e^{i\theta_6 Z\otimes I_2} e^{i\theta_7 Y\otimes X} e^{i\theta_8 Y\otimes Y} e^{i\theta_9 Y\otimes Z} U_2 \qquad (\textit{(SO(6) representation of } U_2) \in \mathrm{SO}(4)\oplus\{I_2\}), \tag{71}$$

$$D_\diamond(V_1V_2^\dagger,\ e^{i\theta_3 X} e^{i\theta_4 Y} e^{2i\theta_5 Z} e^{i\theta_4 Y} e^{i\theta_3 X}) < \varepsilon/4, \tag{72}$$

$$D_\diamond(V_3,\ e^{i\theta_1 X} e^{i\theta_2 Y} e^{i\theta_6 Z}) < \varepsilon/4, \tag{73}$$

$$D_\diamond(V_4V_5^\dagger,\ e^{i\theta_7 X} e^{i\theta_8 Y} e^{2i\theta_9 Z} e^{i\theta_8 Y} e^{i\theta_7 X}) < \varepsilon/4, \tag{74}$$

$$D_\diamond\left(V_6\oplus V_7,\ \left(H\otimes\left(V_4^\dagger e^{i\theta_7 X} e^{i\theta_8 Y} e^{i\theta_9 Z}\right)\right) U_2 (H\otimes I_2)\right) < \varepsilon/4. \tag{75}$$

Then, the following equation holds:

$$D_\diamond\left(U,\ U'\right) < \varepsilon, \tag{76}$$

where

$$U' = (V_3\otimes I_2)(V_1\oplus V_2)(SH\otimes I_2)(V_4\oplus V_5)\left(HS^\dagger H\otimes I_2\right)(V_6\oplus V_7)(H\otimes I_2). \tag{77}$$

Proof of Theorem 11. U' and the following U_1' are located at a distance of $\varepsilon/4$ in the diamond distance:

$$U_1' = (V_3\otimes I_2)(V_1\oplus V_2)(SH\otimes I_2)(V_4\oplus V_5)\left(HS^\dagger\otimes I_2\right)\left(I_2\otimes\left(V_4^\dagger e^{i\theta_7 X} e^{i\theta_8 Y} e^{i\theta_9 Z}\right)\right) U_2. \tag{78}$$

U_1' and the following U_2' are located at a distance of $\varepsilon/4$ in the diamond distance:

$$\begin{aligned} U_2' &= (V_3 \otimes I_2)(V_1 \oplus V_2)\left(e^{i\theta_7 Y\otimes X} e^{i\theta_8 Y\otimes Y} e^{i\theta_9 Y\otimes Z}\right)\left(I_2 \otimes \left(e^{-i\theta_9 Z} e^{-i\theta_8 Y} e^{-i\theta_7 X} V_4\right)\right)\left(I_2 \otimes \left(V_4^\dagger e^{i\theta_7 X} e^{i\theta_8 Y} e^{i\theta_9 Z}\right)\right) U_2 \\ &= (V_3 \otimes I_2)(V_1 \oplus V_2)\left(e^{i\theta_7 Y\otimes X} e^{i\theta_8 Y\otimes Y} e^{i\theta_9 Y\otimes Z}\right) U_2 \end{aligned} \tag{79}$$

since

$$\begin{aligned} &D_\diamond\left(V_4 \oplus V_5,\ e^{i\theta_7 Z\otimes X} e^{i\theta_8 Z\otimes Y} e^{i\theta_9 Z\otimes Z}\left(I_2 \otimes e^{-i\theta_9 Z} e^{-i\theta_8 Y} e^{-i\theta_7 X} V_4\right)\right) \\ &\qquad = D_\diamond(V_5 V_4^\dagger,\ e^{-i\theta_7 X} e^{-i\theta_8 Y} e^{-2i\theta_9 Z} e^{-i\theta_8 Y} e^{-i\theta_7 X}) < \varepsilon/4. \end{aligned} \tag{80}$$

U_2' and the following U_3' are located at a distance of $\varepsilon/4$ in the diamond distance:

$$U_3' = (V_3 \otimes I_2)\left(e^{i\theta_3 Z\otimes X} e^{i\theta_4 Z\otimes Y} e^{i\theta_5 Z\otimes Z}\right)\left(I_2 \otimes \left(e^{-i\theta_5 Z} e^{-i\theta_4 Y} e^{-i\theta_3 X} V_1\right)\right)\left(e^{i\theta_7 Y\otimes X} e^{i\theta_8 Y\otimes Y} e^{i\theta_9 Y\otimes Z}\right) U_2. \tag{81}$$

U_3' and the following U_4' are located at a distance of $\varepsilon/4$ in the diamond distance:

$$\begin{aligned} U_4' &= \left(e^{i\theta_1 X\otimes I_2} e^{i\theta_2 Y\otimes I_2} e^{i\theta_6 Z\otimes I_2}\right)\left(e^{i\theta_3 Z\otimes X} e^{i\theta_4 Z\otimes Y} e^{i\theta_5 Z\otimes Z}\right)\left(I_2 \otimes \left(e^{-i\theta_5 Z} e^{-i\theta_4 Y} e^{-i\theta_3 X} V_1\right)\right)\left(e^{i\theta_7 Y\otimes X} e^{i\theta_8 Y\otimes Y} e^{i\theta_9 Y\otimes Z}\right) U_2 \\ &= \left(e^{i\theta_1 X\otimes I_2} e^{i\theta_2 Y\otimes I_2} e^{i\theta_3 Z\otimes X} e^{i\theta_4 Z\otimes Y} e^{i\theta_5 Z\otimes Z}\right)\left(I_2 \otimes \left(e^{-i\theta_5 Z} e^{-i\theta_4 Y} e^{-i\theta_3 X} V_1\right)\right)\left(e^{i\theta_6 Z\otimes I_2} e^{i\theta_7 Y\otimes X} e^{i\theta_8 Y\otimes Y} e^{i\theta_9 Y\otimes Z}\right) U_2 \\ &= \left(e^{i\theta_1 X\otimes I_2} e^{i\theta_2 Y\otimes I_2} e^{i\theta_3 Z\otimes X} e^{i\theta_4 Z\otimes Y} e^{i\theta_5 Z\otimes Z}\right) U_1 \\ &= U. \end{aligned} \tag{82}$$

By the triangle inequality, $D_\diamond(U,\ U') < \varepsilon$ holds.

□