Efficient learning of t-doped stabilizer states with single-copy measurements

Nai-Hui Chia[1], Ching-Yi Lai[2], and Han-Hsuan Lin[3]

[1]Department of Computer Science, Rice University, TX 77005-1892, United States
[2]Institute of Communications Engineering, National Yang Ming Chiao Tung University, Hsinchu 300093, Taiwan
[3]Department of Computer Science, National Tsing Hua University, Hsinchu 30013, Taiwan

One of the primary objectives in the field of quantum state learning is to develop algorithms that are time-efficient for learning states generated from quantum circuits. Earlier investigations have demonstrated time-efficient algorithms for states generated from Clifford circuits with at most $\log(n)$ non-Clifford gates. However, these algorithms necessitate multi-copy measurements, posing implementation challenges in the near term due to the requisite quantum memory. On the contrary, using solely single-qubit measurements in the computational basis is insufficient in learning even the output distribution of a Clifford circuit with one additional T gate under reasonable post-quantum cryptographic assumptions. In this work, we introduce an efficient quantum algorithm that employs only single-copy measurements to learn states produced by Clifford circuits with a maximum of $O(\log(n))$ non-Clifford gates, filling a gap between the previous positive and negative results.

1 Introduction

Quantum state tomography stands as a pivotal task in the realm of quantum information sciences [1, 2, 3]. In scenarios where numerous independent instances of an unknown state ρ are available, the objective of a state tomography algorithm is to provide an output state $\hat{\rho}$ that closely approximates ρ. Deducing the requisite quantity of state copies and time resources to address this problem stands as a fundamental investigation in quantum information theory.

Ching-Yi Lai: cylai@nycu.edu.tw

It has been shown by Haah et al. [4] and O'Donnell and Wright [5] that the optimal sample complexity for the tomography of a quantum pure state of dimension d is $O(d/\epsilon^2)$, where ϵ represents the trace distance between $\hat{\rho}$ and ρ. These results indicate that the endeavor to learn an arbitrary n-qubit state mandates an exponential abundance of state copies and an inherent investment of exponential time resources.

A natural question arises: which specific subsets of quantum states of n qubits can be efficiently learned using at most $\mathsf{poly}(n)$ copies or even in $\mathsf{poly}(n)$ time? Intuitively, these subsets of quantum states should have concise representations. Chung and Lin [6] showed that the set of states generated by quantum circuits of polynomial size can be learned with $\mathsf{poly}(n)$ copies. This result indicates the feasibility of sample-efficient learning for a general class of states.

Aaronson and Gottesman [7, 8] and Montanaro [9] considered the class of stabilizer states, where n-qubit states can be described in the stabilizer formalism using $O(n^2)$ bits [10]. Stabilizer states can be generated by Clifford circuits, comprising Hadamard, Phase, and controlled-NOT gates, on input computational basis states. They showed that the sample complexity for learning stabilizer states is $O(n)$ and the time complexity is $O(n^3)$, given the capability to concurrently measure multiple copies of a state.

Building upon this foundation, a reasonable progression is to consider quantum states generated by Clifford circuits augmented with a few non-Clifford gates, such as the $\pi/8$-gate (T gate). Notably, the Clifford gates and the T gate constitute a universal gate set enabling universal quantum computation [11]. Lai and Cheng [12] initiated this exploration, demonstrating

time-efficient learning algorithms for Clifford circuits with one layer of $\log(n)$ T gates [12]. Arunachalam et al. introduced time-efficient algorithms for learning a category of constant-degree quantum phase states that also extend beyond the realm of stabilizer states [13].

A quantum circuit is called a *t-doped stabilizer circuit* if it comprises of Clifford gates and, at most, t single-qubit non-Clifford gates. The resulting state of the circuit when applied to a computational basis state is referred to as a *t-doped stabilizer state*. Following [12], it is shown that t-doped stabilizer states with $t = O(\log(n))$ can be learned in polynomial time with polynomial samples by multiple concurrent results [14, 15, 16].

Nonetheless, the algorithms in [12, 14, 15, 16] require measurements on multiple copies of the states. This could potentially demand extra quantum resources during algorithm implementation, such as quantum memory. On the contrary, Hinsche et al. [17] demonstrated that if restricted to single-qubit measurements in the computational basis, learning the output distribution of a 1-doped stabilizer circuit is hard under the assumption that quantum algorithms cannot efficiently solve the learning parity with noise problem.

Noticing the gap between the above results, we aim to investigate the following question: Using only single-copy measurements, whether there exist efficient ($O(\mathsf{poly}(n, \epsilon))$) algorithms that use copies of an n-qubit t-doped stabilizer state $|\psi\rangle$ with $t = O(\log(n))$ and generate a representation of a state that is ϵ-close to $|\psi\rangle$ in trace distance. We give an affirmative answer to this question in this paper and our main theorem (Theorem 10) provides an efficient algorithm relying solely on single-copy measurements.

A key observation from [12, 14, 15, 16] is that an n-qubit t-doped stabilizer state is encompassed within a stabilizer code space of dimension at most 2^{2t}, so we can efficiently map it to a $2t$-qubit state space (refer to Lemma 1 and Lemma 3). Consequently, the task of learning a t-doped n-qubit stabilizer state reduces to the identification of its corresponding stabilizer group and the related $2t$-qubit state. When $t = O(\log(n))$, the state can then be efficiently learned using a state tomography algorithm. To identify the corresponding stabilizer group, Bell sampling on multiple copies of the target state was used in [12, 14, 15, 16], but we seek algorithms that exclusively rely on single-copy measurements. Fortunately, Aaronson and Gottesman [8] have demonstrated that learning an n-qubit stabilizer state can be achieved using just single-copy measurements, requiring mere $O(n^2)$ copies of the target state. Our algorithm adapts this method to pinpoint the associated stabilizer group of a t-doped stabilizer state.

2 Stabilizer Formalism

We introduce the basics of stabilizer formalism along with the corresponding notation.

A single-qubit state space has a (computational) basis $\{|0\rangle, |1\rangle\}$. The Pauli matrices in the computational basis are $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, and $Y = iXZ$. Let $\mathcal{G}_n = \Big\{cM_1 \otimes \cdots \otimes M_n : M_i \in \{I, X, Y, Z\}, c \in \{\pm 1, \pm i\}\Big\}$ denote the n-fold Pauli group, which has $2n$ independent Pauli generators up to a phase. Any two Pauli operators either commute or anticommute with each other.

An n-qubit state $|\psi\rangle$ is said to be stabilized by a Pauli operator $g \in \mathcal{G}_n$ if $g|\psi\rangle = |\psi\rangle$. A stabilizer group is an Abelian subgroup of $\mathcal{G}_n$ that does not contain the minus identity. The *rank* of a stabilizer group is referred to as the smallest number of independent generators that span the stabilizer group.

Suppose that $\mathcal{S}$ is a stabilizer group of rank r for some $r \leq n$ and $|\mathcal{S}| = 2^r$. Let $C(\mathcal{S})$ denote the subspace

$$C(\mathcal{S}) = \Big\{ |\psi\rangle \in \mathbb{C}^{2^n} : g|\psi\rangle = |\psi\rangle\,,\ \forall g \in \mathcal{S} \Big\}. \quad (1)$$

It can be shown that $C(\mathcal{S})$ is a complex vector space of dimension 2^{n-r} and we can view $C(\mathcal{S})$ as the code space of a quantum code which encodes $n - r$ logical qubits into n physical qubits [10].

There exists a one-to-one correspondence between the code space $C(\mathcal{S})$ and the raw $(n-r)$-qubit space through the encoding and decoding Clifford circuits. Moreover, the process of finding the encoding Clifford circuit, which consists of Hadamard, phase, and controlled-NOT gates, for a given stabilizer group is well-established [18, 19].

Lemma 1 For any n-qubit state $|\psi\rangle \in C(\mathcal{S})$ with $|\mathcal{S}| = 2^r$, we have

$$|\psi\rangle = V\Big(|0\rangle^{\otimes r} \otimes |\phi\rangle\Big), \tag{2}$$

where $|\phi\rangle$ is an $(n-r)$-qubit state and V is a Clifford circuit. Furthermore, V can be efficiently constructed in $O(rn^2)$ time if a set of generators for S are given.

If $\mathcal{S}$ is of rank n, the subspace $C(\mathcal{S})$ is of dimension one and is called a *stabilizer state*.

Definition 2 For an n-qubit state $|\psi\rangle$, the maximum integer r such that $|\psi\rangle \in C(\mathcal{S})$ for some stabilizer group $\mathcal{S} \subset \mathcal{G}_n$ of rank r is called the *stabilizer dimension* of $|\psi\rangle$.

It can be shown that in a stabilizer group, at most two independent stabilizer generators do not commute with a specific single-qubit non-Clifford gate. Consequently, the following result can be established.

Lemma 3 [20, Lemma 4.2] Every n-qubit t-doped stabilizer state has stabilizer dimension at least $n - 2t$.

We are interested in learning quantum states of high stabilizer dimensions as they exhibit behaviors closely resembling stabilizer states.

We define the distance between a quantum state $|\psi\rangle$ to a stabilizer group $\mathcal{S}$ as

$$D(|\psi\rangle, \mathcal{S}) \triangleq \inf_{|\phi\rangle \in C(\mathcal{S})} D(|\psi\rangle, |\phi\rangle), \tag{3}$$

where $D(\rho, \sigma)$ denotes the trace distance between the density operators of two quantum states ρ and σ [19]:

$$D(\rho, \sigma) = \max_{0 \le P \le I} \mathrm{tr}(P(\rho - \sigma)). \tag{4}$$

Our approach relies solely on projective measurements of Pauli operators with eigenvalues ± 1. Let $|\psi\rangle \in C(\mathcal{S})$, where $\mathcal{S} \subset \mathcal{G}_n$ is a stabilizer group. Consider a Pauli operator $g \in \mathcal{G}_n$ with eigenvalues ± 1. The projectors onto the eigenspaces of g are given by $\frac{1}{2}(I \pm g)$. If $|\psi\rangle$ is stabilized by g (or $-g$), measuring g on $|\psi\rangle$ will yield outcome $+1$ (or -1) with certainty. However, if g anticommutes with one of the stabilizers of $|\psi\rangle$, measuring g on $|\psi\rangle$ will result in outcome $+1$ with a probability of $1/2$ and outcome -1 with a probability of $1/2$.

In the following discussion, instead of ± 1, measurement outcomes will be denoted by binary values 0 or 1, corresponding to $(-1)^0$ or $(-1)^1$, respectively, for the ease of notation.

Lemma 4 (Gentle measurement [21]) Consider a quantum state $|\psi\rangle$ and a positive operator M with eigenvalues no larger than one. Suppose that $\langle\psi| M |\psi\rangle \ge 1 - \epsilon$, where $0 \le \epsilon \le 1$. Then the post-measurement state is $2\sqrt{\epsilon}$-close to $|\psi\rangle$ in trace distance.

Lemma 5 Consider two Pauli operators $g, h \in \mathcal{G}_n$. Suppose that $\mathrm{tr}\left(\frac{I+g}{2} |\psi\rangle\langle\psi|\right) \ge 0.99$ and $\mathrm{tr}\left(\frac{I+h}{2} |\psi\rangle\langle\psi|\right) \ge 0.99$ for some state $|\psi\rangle$. Then g and h commute.

Proof. Let $\rho = |\psi\rangle\langle\psi|$. Let σ and τ be the states resulting from measuring $\frac{I+g}{2}$ and $\frac{I+h}{2}$ on ρ, respectively. Clearly, we have $g\sigma g^\dagger = \sigma$ and $h\tau h^\dagger = \tau$.

Based on the assumption of the statement and the gentle measurement lemma (Lemma 4), we know that $D(\rho, \sigma) \le 0.2$ and $D(\rho, \tau) \le 0.2$. As a result, $D(\sigma, \tau) \le 0.4$ by the triangle inequality. Consequently, we have $\mathrm{tr}\left(\frac{I+g}{2}\tau\right) \ge \mathrm{tr}\left(\frac{I+g}{2}\sigma\right) - 0.4 \ge 0.59$.

However, if g and h anticommute, we would have $\mathrm{tr}\left(\frac{I+g}{2}\tau\right) = \mathrm{tr}\left(\frac{I+g}{2}h\tau h^\dagger\right) = \mathrm{tr}\left(h\frac{I-g}{2}\tau h^\dagger\right) = \mathrm{tr}\left(\frac{I-g}{2}\tau\right)$. Thus $\mathrm{tr}\left(\frac{I+g}{2}\tau\right) = 0.5 < 0.59$, which leads to a contradiction. Therefore, g and h commute. □

Lemma 6 Let $\mathcal{S} \subset \mathcal{G}_n$ be a stabilizer group of r independent generators $g_1, \ldots, g_r$. Suppose that $D(|\psi\rangle, \mathcal{S}) > \epsilon$. Then measuring $g_1, \ldots, g_r$ on $|\psi\rangle$ returns outcome 0^r with probability at most

$$1 - \epsilon^2.$$

Proof. Assume that

$$|\psi\rangle = \alpha |\phi\rangle + \beta |\phi^\perp\rangle,$$

where $|\phi\rangle \in C(\mathcal{S})$, and $\langle\phi|\phi^\perp\rangle = 0$. Since $D(|\psi\rangle, \mathcal{S}) > \epsilon$, we have $|\beta| > \epsilon$ and $|\alpha|^2 < 1 - \epsilon^2$.

Let P denote the projector onto $C(\mathcal{S})$. Then the probability of outcome 0^r by measuring $g_1, \ldots, g_r$ on $|\psi\rangle$ is $\langle\psi| P |\psi\rangle = |\alpha|^2 < 1 - \epsilon^2$.

□

3 Learning quantum states of high stabilizer dimension

Herein we provide an algorithm to approximately identify the stabilizer group $\mathcal{S}$ from provided copies of a state $|\psi\rangle \in C(\mathcal{S})$.

For two stabilizer groups $\mathcal{S}$ and $\mathcal{T}$, we denote

$$\mathcal{S} \cap \mathcal{T} \triangleq \{g \in \mathcal{G}_n : g \in \mathcal{S}, g \text{ or } -g \in \mathcal{T}\}. \quad (5)$$

Lemma 7 Let $r < n$, given a stabilizer group $\mathcal{S} \subset \mathcal{G}_n$ of size 2^r, choose a stabilizer group $\mathcal{T} \subset \mathcal{G}_n$ of size 2^n at random. Then

$$\Pr\{\mathcal{S} \cap \mathcal{T} \neq \{I\}\} \geq \frac{1}{2^{n-r+1}+1}. \quad (6)$$

Proof. First, we consider the case where a stabilizer group $\mathcal{S}' \subset \mathcal{G}_n$ of rank n is given, and a stabilizer group $\mathcal{T}' \subset \mathcal{G}_n$ of rank r is chosen randomly.

We start by counting the number of stabilizer groups of rank r in the following manner. To choose the first generator, we have $2^{2n}-1$ options. Then we choose the second generator from an equivalent space of 2^{2n-1} operators, half of which anticommute with the first generator. Thus the number of nontrivial options for the second generator is $2^{2n-2}-1$. Consequently, the number of distinct stabilizer groups in $\mathcal{G}_n$ of rank r is given by

$$\left(2^{2n}-1\right)\left(2^{2n-2}-1\right)\cdots\left(2^{2n-2(r-1)}-1\right).$$

Next, we want to determine the number of stabilizer groups of rank r that have only trivial intersections with the given stabilizer group $\mathcal{S}'$. To choose the first generator, we have $2^{2n} - 2^n$ options since $|\mathcal{S}'| = 2^n$. Then we choose the second generator from an equivalent space of 2^{2n-1} operators, half of which anticommute with the first generator. Note that half of the operators in $\mathcal{S}'$ also anticommute with the first generator. Thus the nontrivial options for the second generator is $2^{2n-2} - 2^{n-1}$. Consequently, the number of stabilizer groups of rank r that have only trivial intersections with $\mathcal{S}'$ is given by:

$$\prod_{j=0}^{r-1}\left(2^{2n-2j}-2^{n-j}\right).$$

Therefore, the probability that a randomly chosen $\mathcal{T}'$ and the given $\mathcal{S}'$ have a nontrivial intersection is:

$$\begin{aligned}\Pr\{\mathcal{S}' \cap \mathcal{T}' \neq \{I\}\} &= 1 - \frac{\prod_{j=0}^{r-1}\left(2^{2n-2j}-2^{n-j}\right)}{\prod_{j=0}^{r-1}\left(2^{2n-2j}-1\right)} \\ &\geq 1 - \frac{2^{2n-2(r-1)}-2^{n-(r-1)}}{2^{2n-2(r-1)}-1} = \frac{1}{2^{n-r+1}+1}.\end{aligned}$$

In the above proof, we use the fact that each nontrivial Pauli operator anticommutes with half of the n-fold Pauli operators.

Given that any two stabilizer groups of the same size can be transformed into each other by a Clifford unitary, and Clifford unitaries preserve the commutation relations of Pauli operators, we can deduce that for any stabilizer groups $\mathcal{S}_1$ and $\mathcal{S}_2$ both of rank r_1, the number of stabilizer groups of rank r_2 that share only a trivial intersection with $\mathcal{S}_1$ is equal to the number of stabilizer groups of rank r_2 that share only a trivial intersection with $\mathcal{S}_2$, for any values of r_1 and r_2. By applying Bayes's theorem, we can establish the desired statement.

□

Next we show how to find the stabilizer group for given copies of a quantum state through single-copy measurements on $O(n^2)$ copies of the target state. We extend the algorithm for learning stabilizer states presented in [8] to our specific context, outlined in Algorithm 1.

Theorem 8 There is a quantum algorithm that identifies the stabilizer group associated with an unknown n-qubit quantum state $|\psi\rangle$ of stabilizer dimension $r = n - t$, where $t = O(\log(n))$, given access to copies of $|\psi\rangle$. For any $\epsilon > 0$, the algorithm produces a stabilizer group $\mathcal{S} \subset \mathcal{G}_n$ of rank at least r such that $D(|\psi\rangle, \mathcal{S}) < \epsilon$. The algorithm employs single-copy measurements on $O(n^2 2^t + \frac{1}{\epsilon^2} n^2)$ copies of $|\psi\rangle$, runs in time $O(n^4 2^t + \frac{1}{\epsilon^2} n^4)$, and fails with probability exponentially small in n.

Proof. Suppose that $|\psi\rangle \in C(\mathcal{S}')$. To find $r = n - t$ independent generators for $\mathcal{S}'$, we can adapt the approach of sampling random stabilizer groups and determining their nontrivial intersections with the target stabilizer group $\mathcal{S}'$, as described in [8].

However, the situation is more complex in our case. Let $\mathcal{N}(\mathcal{S}') \triangleq \{h \in \mathcal{G}_n : hg = gh, \forall g \in \mathcal{S}'\}$ denote the normalizer group of $\mathcal{S}'$ in $\mathcal{G}_n$. Since $\mathcal{S}'$

is of rank $r < n$, $\mathcal{N}(\mathcal{S}')$ contains generators not in $\mathcal{S}'$ that commute with any operators in $\mathcal{S}'$. This additional complexity may affect the correctness of our algorithm.

For $\mathcal{S}'$ of rank $r = n-t$, according to Lemma 7, a random stabilizer $\mathcal{T}$ of size 2^n would have a nontrivial intersection with $\mathcal{S}'$ with probability $\frac{1}{2^{t+1}+1}$. To achieve a failure probability of 2^{-n} for $O(n)$ randomly picked stabilizer groups to have nontrivial intersections with $\mathcal{S}'$, we need to make $O(n2^t)$ random picks of $\mathcal{T}$ using the Hoeffding inequality. As $\mathcal{S}'$ has fewer than n independent generators, its basis can be found from $O(n)$ elements in $\mathcal{S}'$ with a failure probability of 2^{-n}.

Next, we outline the procedure for finding the nontrivial intersection of $\mathcal{S}'$ and an arbitrary stabilizer group $\mathcal{T}$ with n independent generators $g_1, g_2, \ldots, g_n \subset \mathcal{G}_n$.

An arbitrary element in $\mathcal{T}$ can be expressed as

$$g(a) = \prod_i g_i^{a_i}, \tag{7}$$

where $a_i \in \{0,1\}$. Since $g_1, g_2, \ldots, g_n$ commute with each other, we can sequentially measure them on one copy of $|\psi\rangle$. Let the measurement outcomes be $b_1, b_2, \ldots, b_n \in \{0,1\}$, respectively. Then, we can compute the binary outcome of measuring $g(a)$ on $|\psi\rangle$ as:

$$b \cdot a = \sum_i a_i b_i, \tag{8}$$

which can be computed for any $a \in \{0,1\}^n$ from the single-copy measurement outcomes $b_1, b_2, \ldots, b_n$.

The following cases describe the possible values of $b \cdot a$ based on the properties of $g(a)$ and its relation to stabilizers of $|\psi\rangle$: a) $b \cdot a = 0$ (respectively, $b \cdot a = 1$) with certainty if $|\psi\rangle$ is stabilized by $g(a)$ (respectively, $-g(a)$). b) $b \cdot a = 0$ or 1 with probabilities $1/2$ and $1/2$, respectively, if $g(a)$ anticommutes with a stabilizer of $|\psi\rangle$. c) $b \cdot a = 0$ or 1 with nontrivial probabilities if $g(a) \in \mathcal{N}(\mathcal{S}') \setminus \pm\mathcal{S}'$.

Suppose that each of $g_1, g_2, \ldots, g_n$ is measured on m copies of $|\psi\rangle$. Let $b_{i,j} \in \{0,1\}$ be the binary of measurement outcome of g_j on the i-th copy of $|\psi\rangle$. If $h(a)$ is a stabilizer of $|\psi\rangle$ for some $a \in \{0,1\}^n$, then $a \in \{0,1\}^n$ is a solution to the following linear system of equations:

$$Ba = 0^m, \tag{9}$$

where $B = [b_{i,j}] \in \{0,1\}^{m \times n}$. Note that for the sake of analysis convenience, we do not consider solutions to $Ba = 1^m$ such that $-h(a)$ is a stabilizer, but this exclusion does not affect the overall complexity, which remains unchanged up to a constant.

Now consider a Pauli operator $h(a) \notin \mathcal{S}$ with $\langle\psi| \frac{I+h(a)}{2} |\psi\rangle < 0.99$. If $Ba = 0^m$, then $h(a)$ could be chosen as a solution to Step 2)-c), which can cause Algorithm 1 to fail. Choosing $m \geq 300n$, the probability of such an event is given by:

$$\Pr\Big\{Ba = 0^m \Big| h(a) \notin \mathcal{S} \text{ and } \langle\psi| \frac{I+h(a)}{2} |\psi\rangle < 0.99\Big\} \leq (0.99)^m \approx e^{-0.01m} = e^{-3n}.$$

Since $|\mathcal{T}| = 2^n$ and Step 2) is repeated $10n2^t = \mathsf{poly}(n)$ times, by applying the union bound, the probability of Step 2) failing is at most e^{-n}.

By Lemma 5 and the choice of m, the generators in $\mathcal{B}$ at Step 3) will commute with a probability of at least $1 - e^{-n}$.

In Step 4), the basis $\mathcal{B}$ is checked by measuring m' copies of $|\psi\rangle$ in the basis of $\mathcal{B}$, where m' is to be determined. If any outcome of 1 is observed, a Gaussian process can be performed to remove the independent generators that contribute to the outcomes of 1s.

It remains to bound the probability that the algorithm outputs a stabilizer group $\mathcal{S}$ with $D(|\psi\rangle, \mathcal{S}) > \epsilon$. Such a stabilizer group would pass the verification step 4) if the outcomes of measuring m' copies of $|\psi\rangle$ in the basis of $\mathcal{B}$ are all 0s. According to Lemma 6, measuring a basis of $\mathcal{S}$ on $|\psi\rangle$ will return outcome 0^r with probability at most $1 - \epsilon^2$. By choosing $m' \geq \frac{1}{\epsilon^2}(n^2 + 2n)$, the probability of this event is no larger than $(1-\epsilon^2)^{m'} \approx e^{-m'\epsilon^2} \leq e^{-n^2-2n}$. As there are no more than 2^{n^2+n} different stabilizer groups, the total probability of these error events is no larger than e^{-n} by the union bound.

As a result, the overall failure probability is 2^{-n}.

Finally, we analyze the time complexity. In Step 2)-a), sampling a stabilizer group of rank n can be done in $\mathcal{O}(n^2)$ [22, 23]. In Step 2)-b), measuring an n-fold Pauli operator takes time $O(n)$. Thus, measuring $|\psi\rangle$ in the basis of a stabilizer group takes time $O(n^2)$, and each Step 2)-b) takes time $O(n^3)$.

Step 2)-c) also takes time $O(n^3)$ for Gaussian elimination. In Step 2)-d), determining whether

$\mathcal{S} \cap \mathcal{T} \notin \langle \mathcal{R} \rangle$ can also be done by Gaussian elimination in $O(n^3)$. Step 2) is repeated $O(n2^t)$ times, which takes time $O(n^4 2^t)$.

Step 3) takes time $O(n^3)$.

Step 4) takes time $O(\frac{1}{\epsilon^2} n^4)$ as measuring each copy in the basis of $\mathcal{B}$ takes time $O(n^2)$.

Therefore, the overall time complexity is $O(n^4 2^t + \frac{1}{\epsilon^2} n^4)$. □

Algorithm 1: Learning an unknown stabilizer group of a quantum state

Input : $O(n^2 2^t + \frac{1}{\epsilon^2} n^2)$ copies of a state $|\psi\rangle$ of stabilizer dimension $n - t$ where $t = O(\log(n))$ and a parameter ϵ.

Output: A set of independent generators for a stabilizer group $\mathcal{S}$ with $D(|\psi\rangle, \mathcal{S}) < \epsilon$.

1) Initialize $\mathcal{R} = \{I\}$.
2) Repeat the following steps $10n2^t$ times:
   a) Pick a stabilizer group $\mathcal{T}$ of rank n at random.
   b) Measure $300n$ copies of $|\psi\rangle$ in the basis of $\mathcal{T}$.
   c) Find a generating set for $\mathcal{S} \cap \mathcal{T}$ by solving Eq. (9).
   d) Add any elements of the generating set that are not in $\langle \mathcal{R} \rangle$ to $\mathcal{R}$.
3) Find a basis $\mathcal{B}$ for $\mathcal{R}$ by Gaussian elimination.
4) Measure $\frac{1}{\epsilon^2}(n^2 + 2n)$ copies of $|\psi\rangle$ in the basis of $\mathcal{B}$. Keep the generators that give all-zero outcomes. Return them as generators of $\mathcal{S}$.

4 Learning t-doped stabilizer states

To characterize an n-qubit t-doped stabilizer state with stabilizer dimension at least $n-2t$, one can specify its stabilizer encoding circuit along with the corresponding raw $2t$-qubit state, as described in Lemma 1. Utilizing Theorem 8, one can learn the stabilizer encoding circuit using single-copy measurements on copies of the target state. Subsequently, the decoding circuit can be applied to the target state, thus obtaining its raw $2t$-qubit state. In this context, we adopt the following fast state tomography algorithm to learn this $2t$-qubit state.

Lemma 9 (fast state tomography [24]) There exists a quantum algorithm that for any unknown n-qubit pure state $|\psi\rangle$, uses $O(2^n n \log(\frac{1}{\delta})\epsilon^{-4})$-copies of $|\psi\rangle$ and generates a representation of a state $|\tilde{\psi}\rangle$ such that $D(|\psi\rangle, |\tilde{\psi}\rangle) \leq \epsilon$ with probability $1 - \delta$ in $O(2^{2n} n^3 \log(\frac{1}{\delta})\epsilon^{-5})$ time. The algorithm requires only single-copy Clifford measurements and classical post processing.

Our main result is as follows.

Theorem 10 There exists a quantum algorithm that identifies an unknown n-qubit t-doped stabilizer state $|\psi\rangle$, where $t = O(\log(n))$, given access to copies of $|\psi\rangle$. For any $\epsilon > 0$, the algorithm generates a representation of a state $|\psi'\rangle$ such that $D(|\psi\rangle, |\psi'\rangle) < \epsilon$.

The algorithm employs single-copy measurements on $O(n^2 2^{2t} + \frac{2^{4t} n^2}{\epsilon^8})$ copies of $|\psi\rangle$, runs in time $O(n^4 2^{2t} + \frac{2^{4t} n^4}{\epsilon^8})$, and fails with probability exponentially small in n.[1]

Proof. It is mentioned that a t-doped stabilizer state has stabilizer dimension at least $n - 2t$. By Theorem 8, we can learn an approximate stabilizer group $\mathcal{S}$ of $|\psi\rangle$ such that $D(|\psi\rangle, \mathcal{S}) < \epsilon' = O(\frac{\epsilon^4}{2^{2t}})$ with $O(n^2 2^{2t} + \frac{2^{4t} n^2}{\epsilon^8})$ samples and $O(n^4 2^{2t} + \frac{2^{4t} n^4}{\epsilon^8})$ time.

Let the rank of $\mathcal{S}$ be r'. By measuring $O(2^{2t}\epsilon^{-4})$ copies of $|\psi\rangle$ in the basis of $\mathcal{S}$, we will expect that due to the choice of ϵ', the outcomes will be all 0s with a negligible probability of failure. Let the post measurement state be $|\psi'\rangle$ and we have $O(2^{2t}\epsilon^{-4})$ copies of $|\psi'\rangle$ from the previous measurements.

By Lemma 1, we can find the encoding circuit V for the stabilizer group $\mathcal{S}$. Applying $V^\dagger$ to each copy of $|\psi'\rangle$, we get copies of $|0\rangle^{r'} \otimes |\phi\rangle$, where $|\phi\rangle$ has $2t$-qubits and this process takes $O(2^{2t}\epsilon^{-4}) \times O(n^3)$ time. With $O(2^{2t}\epsilon^{-4})$ copies of $|\phi\rangle$, we can apply Lemma 9 to get an estimate $|\phi'\rangle$ with $O(\epsilon)$ error.

Finally, our estimate of $|\psi\rangle$ is $V(|0\rangle^{r'} \otimes |\phi'\rangle)$, which is $O(\epsilon)$-close to $|\psi'\rangle$ in trace distance and thus $O(\epsilon)$-close to $|\psi\rangle$ in trace distance. □

5 Discussion

The existence of an efficient learning algorithm for states generated from Clifford circuits equipped

[1] If $t = \log(n)$, the sample and time complexities are $O(n^6/\epsilon^8)$ and $O(n^8/\epsilon^8)$, respectively. If $t = O(\log(n))$, sample and time complexities are both polynomial in n.

with a polynomial count of T gates would imply the feasibility of efficiently learning states generated by quantum circuits of polynomial size. Our algorithm extended previous results to learning quantum states generated from Clifford circuits augmented with $\log(n)$ non-Clifford gates, using only single-copy measurements. This exploration holds the potential to usher in practical applications in quantum physics and quantum computing, such as comprehending noise within quantum devices and delving into the correlations present within enigmatic quantum systems.

A natural follow-up question is whether using arbitrary single-qubit measurements, efficiently learning t-doped stabilizer states is possible. This will fill the gap between our result and [17].

Our technique applies to quantum process tomography [25] of t-doped stabilizer circuits as well. More specifically, one can efficiently identify the Choi–Jamiołkowski state [26, 27] of t-doped stabilizer circuit using single-copy measurements with polynomially many uses of the circuit. However, note that efficiently deriving a circuit decomposition from a provided representation of a Choi–Jamiołkowski state is not a straightforward task, especially when dealing with a combination of Clifford and non-Clifford gate sets.

While preparing this manuscript, we became aware of a similar result independently discovered by Grewal et al. [28]. Our main results in Theorem 8 and Algorithm 1 correspond to Theorem 5.9 and Algorithm 1 in [28], respectively. However, our algorithm exhibits improved time and sample complexities, particularly with a better dependence on the number of qubits n. Learning a t-doped stabilizer state involves identifying its corresponding (non-full rank) stabilizer group. We demonstrate that this can be achieved through single-copy measurements, extending the algorithm introduced by Aaronson and Gottesman [8]. Lemma 7 establishes that a random stabilizer group and the target stabilizer group have a nontrivial intersection with a nontrivial probability. Subsequently, in Theorem 8, single-copy measurement outcomes in the basis of a random stabilizer group can be utilized to deduce a stabilizer generator of the target stabilizer group with high probability. As a result, the time complexity dependence on n in our algorithm aligns with that in [8]. On the contrary, Grewal et al. [28] choose a different strategy. They introduce a computational difference sampling based on the outcomes of single-copy measurements to emulate the Bell difference sampling, a method they had previously demonstrated for learning the target stabilizer [14]. This approach relies heavily on a complex boolean Fourier analysis.

Acknowledgements

NHC was supported by NSF award FET-2243659, Google Scholar Award, and DOE award DE-SC0024301.

CYL was supported by the National Science and Technology Council (NSTC) in Taiwan, under Grant 111-2628-E-A49-024-MY2, 112-2119-M-A49-007, and 112-2119-M-001-007.

HHL was supported by NSTC QC project under Grant no. 111-2119-M-001-004- and 110-2222-E-007-002-MY3.

References

[1] Z. Hradil. "Quantum-state estimation". Physical Review A **55**, R1561–R1564 (1997).

[2] G. Mauro D'Ariano, Matteo G.A. Paris, and Massimiliano F. Sacchi. "Quantum tomography". In Advances in Imaging and Electron Physics. Pages 205–308. Elsevier (2003).

[3] K Banaszek, M Cramer, and D Gross. "Focus on quantum tomography". New Journal of Physics **15**, 125020 (2013).

[4] Jeongwan Haah, Aram W. Harrow, Zhengfeng Ji, Xiaodi Wu, and Nengkun Yu. "Sample-optimal tomography of quantum states". IEEE Transactions on Information TheoryPages 1–1 (2017).

[5] Ryan O'Donnell and John Wright. "Efficient quantum tomography". In Proceedings of the forty-eighth annual ACM symposium on Theory of Computing. Pages 899–912. (2016).

[6] Kai-Min Chung and Han-Hsuan Lin. "Sample Efficient Algorithms for Learning Quantum Channels in PAC Model and the Approximate State Discrimination Problem". In 16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2021). Volume 197

of Leibniz International Proceedings in Informatics (LIPIcs), pages 3:1–3:22. (2021).

[7] Scott Aaronson and Daniel Gottesman. "Improved simulation of stabilizer circuits". Phys. Rev. A **70**, 052328 (2004).

[8] Scott Aaronson and Daniel Gottesman. "Identifying stabilizer states". Talk at PIRSA, available on video (2008). url: http://pirsa.org/08080052.

[9] Ashley Montanaro. "Learning stabilizer states by bell sampling". (2017). arXiv:1707.04012.

[10] D. Gottesman. "Stabilizer codes and quantum error correction". PhD thesis. California Institute of Technology. Pasadena, CA (1997).

[11] P.Oscar Boykin, Tal Mor, Matthew Pulver, Vwani Roychowdhury, and Farrokh Vatan. "A new universal and fault-tolerant quantum basis". Information Processing Letters **75**, 101–107 (2000).

[12] Ching-Yi Lai and Hao-Chung Cheng. "Learning quantum circuits of some t gates". IEEE Transactions on Information Theory **68**, 3951–3964 (2022).

[13] Srinivasan Arunachalam, Sergey Bravyi, Arkopal Dutt, and Theodore J. Yoder. "Optimal algorithms for learning quantum phase states". (2023). arXiv:2208.07851.

[14] Sabee Grewal, Vishnu Iyer, William Kretschmer, and Daniel Liang. "Efficient learning of quantum states prepared with few non-clifford gates". (2023). arXiv:2305.13409.

[15] Lorenzo Leone, Salvatore F. E. Oliviero, and Alioscia Hamma. "Learning t-doped stabilizer states". (2023). arXiv:2305.15398.

[16] Dominik Hangleiter and Michael J. Gullans. "Bell sampling from quantum circuits". (2023). arXiv:2306.00083.

[17] M. Hinsche, M. Ioannou, A. Nietner, J. Haferkamp, Y. Quek, D. Hangleiter, J.-P. Seifert, J. Eisert, and R. Sweke. "One t gate makes distribution learning hard". Phys. Rev. Lett. **130**, 240602 (2023).

[18] Richard Cleve and Daniel Gottesman. "Efficient computations of encodings for quantum error correction". Phys. Rev. A **56**, 76–82 (1997).

[19] Michel A. Nielsen and Isaac L. Chuang. "Quantum computation and quantum information". Cambridge University Press. Cambridge, UK (2000).

[20] Sabee Grewal, Vishnu Iyer, William Kretschmer, and Daniel Liang. "Improved stabilizer estimation via bell difference sampling" (2023). arXiv:2304.13915.

[21] A. Winter. "Coding theorem and strong converse for quantum channels". IEEE Transactions on Information Theory **45**, 2481–2485 (1999).

[22] Sergey Bravyi and Dmitri Maslov. "Hadamard-free circuits expose the structure of the clifford group". IEEE Transactions on Information Theory **67**, 4546–4563 (2021).

[23] Ewout Van Den Berg. "A simple method for sampling random clifford operators". In 2021 IEEE International Conference on Quantum Computing and Engineering (QCE). Pages 54–59. (2021).

[24] Daniel Stilck França, Fernando G.S L. Brandão, and Richard Kueng. "Fast and Robust Quantum State Tomography from Few Basis Measurements". In 16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2021). Volume 197 of Leibniz International Proceedings in Informatics (LIPIcs), pages 7:1–7:13. (2021).

[25] M. Mohseni, A. T. Rezakhani, and D. A. Lidar. "Quantum-process tomography: Resource analysis of different strategies". Physical Review A**77** (2008).

[26] Man-Duen Choi. "Completely positive linear maps on complex matrices". Linear Algebra and its Applications **10**, 285–290 (1975).

[27] A. Jamiołkowski. "Linear transformations which preserve trace and positive semidefiniteness of operators". Reports on Mathematical Physics **3**, 275–278 (1972).

[28] Sabee Grewal, Vishnu Iyer, William Kretschmer, and Daniel Liang. "Efficient learning of quantum states prepared with few non-clifford gates ii: Single-copy measurements". (2023). arXiv:2308.07175.