arXiv:2305.15398v6 [quant-ph] 21 May 2024

Learning t-doped stabilizer states

Lorenzo Leone[1,2], Salvatore F.E. Oliviero[1,3], and Alioscia Hamma[4,5]

[1]Physics Department, University of Massachusetts Boston, 02125, USA
[2]Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany
[3]NEST, Scuola Normale Superiore and Istituto Nanoscienze, Consiglio Nazionale delle Ricerche, Piazza dei Cavalieri 7, IT-56126 Pisa, Italy
[4]Dipartimento di Fisica 'Ettore Pancini', Università degli Studi di Napoli Federico II, Via Cintia 80126, Napoli, Italy
[5]INFN, Sezione di Napoli, Italy

In this paper, we present a learning algorithm aimed at learning states obtained from computational basis states by Clifford circuits doped with a finite number t of T-gates. The algorithm learns an exact tomographic description of t-doped stabilizer states in terms of Pauli observables. This is possible because such states are countable and form a discrete set. To tackle the problem, we introduce a novel algebraic framework for t-doped stabilizer states, which extends beyond T-gates and includes doping with any kind of local non-Clifford gate. The algorithm requires resources of complexity $\mathrm{poly}(n, 2^t)$ and exhibits an exponentially small probability of failure.

1 Introduction

The task of learning an unknown quantum state usually refers to the ability to build a classical representation of the state that is "close" enough, based on a specified measure of distance, to the unknown state. However, it is well known that learning an arbitrary many-body quantum state requires an exponential number of experiments due to the exponential growth of the Hilbert space with the number of particles.

Let us be more precise, let us consider the Hilbert space of n qubits and denote $d \equiv 2^n$ its dimension. We can define the group of Pauli operators as the collection of all possible products of Pauli matrices applied to each qubit. Pauli tomography [1–6] serves as a prevalent and widely employed technique for learning a given state ψ. Specifically, Pauli tomography entails acquiring knowledge about the expectation values $\mathrm{tr}(P\psi)$ for every Pauli string P. To achieve a classical reconstruction of the state vector ψ, a total of d^2 Pauli operators must be measured and it becomes evident that tomography is generally a resource-intensive task. The primary challenge in achieving efficiency in quantum state tomography arises from our limited knowledge of the state of interest. Nevertheless, there exist different classes of states, for which tomography can be performed with remarkable efficiency, e.g. Matrix Product States [2], quantum phase states [7], non-interacting fermionic states [8] and stabilizer states [9]. The latter is obtained by the computational basis state $|0\rangle^{\otimes n}$ by the action of the Clifford group – the subgroup of the unitary group that sends Pauli operators in Pauli operators [9]. Each stabilizer state $|\sigma\rangle$ corresponds to a stabilizer group G_σ, a subgroup of the Pauli group, comprising d mutually commuting Pauli operators P satisfying the condition $P|\sigma\rangle = \pm|\sigma\rangle$, i.e. elements of the stabilizer group G_σ stabilize the stabilizer state $|\sigma\rangle$. Thus, to find the tomographic description of σ, one needs to learn the stabilizer group G_σ and the relative phases. Every stabilizer group G_σ admits (more than) a set of generators g_σ, i.e. $G_\sigma = \langle g_\sigma \rangle$ with cardinality $|g_\sigma| = n$. Thus, it is sufficient to find a set of n generators and phases to completely characterize σ. Montanaro [10] showed an algorithm that learns the tomographic decomposition of any stabilizer state with $O(n)$ queries to $|\sigma\rangle$, thus gaining an exponential speed-up for stabilizer states overall tomographic methods [11].

However, stabilizer states are not universal for quantum computation and cannot provide quantum speed-up of any kind [12]. To make the set of stabilizer states universal for quantum computation, one must use unitaries lying outside the Clifford group [12]. One common choice is to use the single qubit T-gate defined as $T = \mathrm{diag}(1, e^{i\pi/4})$. States obtained from $|0\rangle^{\otimes n}$ by the action of Clifford unitaries plus t T-gates are usually referred to as t-doped stabilizer states [13, 14].

Whether Montanaro's procedure could be ex-

Lorenzo Leone: lorenzo.leone@fu-berlin.de
Salvatore F.E. Oliviero: salvatore.oliviero@sns.it
Alioscia Hamma: alioscia.hamma@unina.it

tended to states beyond the stabilizer formalism, in particular to t-doped stabilizer states, has been a research question since then. There has been a noteworthy attempt in [15], in which the authors cleverly discovered an extension of the stabilizer formalism for those states obtained by a stabilizer state acting with a row of t T-gates followed by a Clifford circuit: T-*depth* 1 circuits. Such states can be learned by $O(3^t n)$ query accesses and time $O(n^3 + 3^t n)$. However, their protocol is limited only to those states achievable through a specific architecture of Clifford+T circuits.

In this paper, we finally show that it is possible to extend learning algorithms to general states obtained by Clifford+T unitaries. We propose an innovative algebraic framework for t-doped stabilizer states by employing concepts from stabilizer entropy [16]. Building upon this newly established structure, we devise two algorithms that aim at learning an unknown t-doped stabilizer state exactly. The first one involves sampling from a distribution Ξ obtained by squaring the expectation values of Pauli operators, also known as *characteristic distribution*, that can be achieved by a Bell sampling on both the state and its conjugate in the computational basis [10]. The second approach relaxes the requirement of accessing samples from the characteristic distribution. Instead, it relies on the sampling from a probability distribution $\tilde{\Xi}$ obtained by Bell measurements on two copies of the state at a time, without the need to access its conjugate. A key factor of both algorithms above is that, being limited in learning a discrete set of states obtained by the action of Clifford+T circuits, they learn an exact tomographic description in terms of Pauli observables.

To enhance clarity, we summarize the results on the sample and computational complexity of both methods below. Since both algorithms have access to samples from a probability distribution on Pauli operators, Ξ and $\tilde{\Xi}$ respectively, in what follows we split the sample complexity coming from sampling from such distributions from the sample complexity employed for additional Pauli measurements, which we refer to as *measurement shots*.

Algorithm 1. *Assuming having access to sample from the characteristic distribution Ξ_{ψ_t}, the algorithm that learns a exact classical description of t-doped stabilizer state requires $O(2^t n + t2^{5t})$ Ξ-samples, $O(2^{7t} + 2^{4t} n(n+t))$ measurement shots, $O(4^{2t} n^2)$ additional computational steps, and fails with probability $O(n2^{-n})$.*

Algorithm 2. *Having access to sample from $\tilde{\Xi}_{\psi_t} = d^{-1}|\langle\psi_t|P|\psi_t^*\rangle|^2$, the algorithm that learns a exact classical description of t-doped stabilizer state requires $O(2^{6t} n)$ $\tilde{\Xi}$-samples, $O(2^{9t} n(n+6t))$ measurement shots, $O(n^2)$ additional computational steps, and fails with probability $O(n2^{-n})$.*

Furthermore, it is worth noting that for $t = 0$, both algorithms reduce to Montanaro's algorithm.

2 Algebraic structure of t-doped stabilizer states

Denote $\mathbb{P}_n$ the Pauli group on n qubits and $\mathcal{C}_n$ the Clifford group. We define t-doped Clifford unitaries, denoted as C_t, unitary operators comprised of Clifford unitaries $C \in \mathcal{C}_n$ plus t l-qubits non-Clifford gates with $l = O(1)$. Let $|\psi_t\rangle$ be a t-doped stabilizer state – i.e. a state obtained as $|\psi_t\rangle = C_t |0\rangle^{\otimes n}$ – and let ψ_t be its density matrix. Define $S_{\psi_t} := \{P \in \mathbb{P}_n \,|\, \mathrm{tr}(P\psi_t) \neq 0\}$ the set of Pauli operators with nonzero expectation over $|\psi_t\rangle$. For a stabilizer state ($t = 0$) $|S_{\psi_0}| = d$. Further, one can define the probability distribution Ξ_{ψ_t} with support on S_{ψ_t} and components $\Xi_{\psi_t}(P) = \mathrm{tr}^2(P\psi_t)/d$. We denote the *stabilizer entropy* [16] of the state ψ_t as $M_\alpha(\psi_t) = S_\alpha(\Xi_{\psi_t}) - n$, that corresponds to the Rényi entropy $S_\alpha(\Xi_{\psi_t})$ of order α of the probability distribution Ξ_ψ up to an offset n. As we shall see, the stabilizer entropy can be operationally interpreted as the entropy of the tomography in the Pauli basis.

Consider $M_0(\psi_t) \equiv \log(|S_{\psi_t}|/d)$. One has $M_0(\psi_t) \leq 2lt$ [16] and thus $|S_{\psi_t}| \leq d2^{2lt}$. Furthermore, a t-doped stabilizer state ψ_t admits a stabilizer group G_{ψ_t} [17], i.e. a subgroup of $\mathbb{P}_n$ such that $\forall P \in G_{\psi_t}\ P|\psi_t\rangle = \pm|\psi_t\rangle$. However, unlike stabilizer states, the stabilizer group of a generic t-doped stabilizer state has a cardinality $|G_{\psi_t}|$ strictly less than d and is bounded from below

$$\frac{d}{2^{2lt}} \leq |G_{\psi_t}| \leq d\,, \tag{1}$$

i.e. the set of Pauli operators stabilizing a given t-doped state gets (at most) halved every non-Clifford gate used to build $|\psi_t\rangle$ from $|0\rangle^{\otimes n}$. Since G_{ψ_t} is a subgroup of the Pauli group, it is finitely generated and there exist $g_1, \ldots, g_m$ generators, with $m \equiv \log_2 |G_{\psi_t}|$, such that every element $Q \in G_{\psi_t}$ can be obtained by a product of $g_1, \ldots, g_m$ with relative phases $\phi_{g_1}, \ldots, \phi_{g_m}$ defined by $g_i |\psi_t\rangle = \phi_{g_i} |\psi_t\rangle$. Since there are at most $|S_{\psi_t}| \leq d2^{2lt}$ Pauli operators with nonzero expectation over ψ_t and at least $d/2^{2lt}$ of those stabilize $|\psi_t\rangle$, there exist Pauli operators $h_1, \ldots, h_k \in S_{\psi_t}$ ($k \leq 4^{2lt} - 1$) such that the set S_{ψ_t} can be written as the union of left disjoint cosets (see Appendix C.1)

$$S_{\psi_t} = G_{\psi_t} \cup h_1 G_{\psi_t} \cup \ldots \cup h_k G_{\psi_t}\,. \tag{2}$$

Throughout the manuscript, we refer to the coset representatives $h_1, \dots, h_k$ as *bad-generators* of the t-doped stabilizer state ψ_t. Note that the number m of generators g_i and the number k of bad-generators h_i must obey $2^m(k+1) = |S_{\psi_t}|$. Thanks to the structure of S_{ψ_t} in Eq. (2), a t-doped stabilizer state can be expressed in the Pauli basis as

$$\psi_t = \frac{1}{d} \sum_{i=0}^{k} \mathrm{tr}(h_i \psi_t) h_i \prod_{j=1}^{m} \left(\mathbb{1} + \phi_{g_j} g_j\right) , \quad (3)$$

where $h_0 \equiv \mathbb{1}$. Notice that the operator $\prod_{j=1}^{m}(\mathbb{1} + \phi_{g_j} g_j) = 2^m \Pi_{\psi_t}$ is proportional to the projector Π_{ψ_t} onto the stabilizer group G_{ψ_t}, which automatically implies that bad generators commute with every $P \in G_{\psi_t}$ to ensure hermiticity and positivity of ψ_t. Through the decomposition in Eq. (3), we can easily derive the corollary of the results in [18, 19] that will be useful later on. Define $\mathcal{D} \in \mathcal{C}_n$ a Clifford operator that obeys $\mathcal{D}\Pi_{\psi_t}\mathcal{D}^\dagger = |0\rangle\langle 0|^{\otimes m} \otimes \mathbb{1}_{[n-m]}$, where $\mathbb{1}_{[n-m]}$ denotes the identity on the last $n-m$ qubits. Then since h_i are coset representative and do commute with Π_{ψ_t}, the following decomposition holds

$$|\psi_t\rangle = \mathcal{D}^\dagger (|0\rangle^{\otimes m} \otimes |\phi\rangle) , \quad (4)$$

where $|\phi\rangle$ is a state defined on the last $(n-m)$ qubits. The density matrix associated to $|\phi\rangle$ can be written as $|\phi\rangle\langle\phi| = 2^{n-m} \sum_{i=0}^{k} \mathrm{tr}(h_i \psi_t) \tilde{h}_i$, where $\tilde{h}_i \equiv \mathcal{D} h_i \mathcal{D}^\dagger$. Moreover the following relation, useful for what follows, holds $G_{\mathcal{D}\psi_t\mathcal{D}^\dagger} = \mathcal{D} G_{\psi_t} \mathcal{D}^\dagger$. To be consistent with the terminology used in Refs. [18, 19], we refer to the Clifford operator $\mathcal{D}$ as the *diagonalizer*.

As another consequence of Eq. (3), a direct computation of the stabilizer entropy $M_\alpha(\psi_t)$ returns $M_\alpha(\psi_t) = E_\alpha(\chi_{\psi_t}) - \nu(\psi_t)$, where $\nu(\psi_t) \equiv n - m$ is the stabilizer nullity introduced in [20], while $E_\alpha(\chi_{\psi_t})$ is the α-Rényi entropy of the probability distribution χ_{ψ_t} with support on the cosets $h_i G_{\psi_t}$ and components $\chi_{\psi_t}(h_i) = \mathrm{tr}^2(h_i \psi_t)|G_{\psi_t}|/d$. The probability distribution χ_{ψ_t} can be interpreted as the entropy of bad generators $h_1, \dots, h_k$, e.g. $E_0(\psi_t) = \log(k+1)$.

While all the results presented so far are general, let us conclude the section by directing our attention toward t-doped stabilizer states resulting from the application of Clifford+T circuits. For T-gates, the previously derived bounds can be obtained by substituting $2l$ with 1. Indeed, $l = 1$ for single-qubit gates, and the additional $1/2$ factor arises when considering diagonal gates, see [17]. As these states form a discrete set, it is expected that the expectation values of Pauli operators exhibit discrete values. Hence, there should exist a finite resolution, strictly dependent on t, enabling one to exactly distinguish these values by employing a sufficient number of samples. This intuition is made rigorous in the following discussion. Consider a t-doped stabilizer state obtained by the action of t T-gates. Then, for every $P, Q \in \mathbb{P}_n$, the following lower bound holds

$$|\,\mathrm{tr}(P\psi_t) - \mathrm{tr}(Q\psi_t)| \geq \frac{\sqrt{2}}{6} \left(\frac{1}{\sqrt{2}} - \frac{1}{2}\right)^t \quad (5)$$

provided that $\mathrm{tr}(P\psi_t) \neq \mathrm{tr}(Q\psi_t)$. See Appendix C.4 for the proof. Therefore, for $t = O(\log n)$, the expectation values of Pauli operators either coincide or exhibit a polynomial separation. This fact will enable us to say that by employing a sufficient number of samples – though polynomial in n for $t = O(\log n)$ – to measure Pauli expectation values, one can learn t-doped stabilizer states *exactly*. Let us remark again that, contrary to all statements presented in the section, Eq. (5) does not hold for the broader scenario of doping with $O(1)$-qubit non-Clifford gates; rather, it specifically applies to the case involving T-gates exclusively.

3 Learning algorithm from Ξ_{ψ_t}-samples

In the previous section, we explicitly revealed the algebraic structure of a generic t-doped stabilizer state. Let us provide the algorithm able to learn a t-doped stabilizer state. While the majority of our results can be generalized to states doped by l-local non-Clifford gates (with $l = O(1)$), we will focus our discussion on the T-gate case in order to employ the finite resolution result in Eq. (5). In particular, a state ψ_t doped with a number t of T-gates is characterized by (i) $m \geq n - t$ generators g_i of G_{ψ_t} with m relative phases ϕ_{g_i}; (ii) by $k \leq 4^t - 1$ bad generators h_i with k expectation values $\mathrm{tr}(h_i \psi_t)$. Therefore, the learning of a classical description of a t-doped stabilizer state requires the knowledge of $2m + 2k \leq 2n + 2 \times 4^t$ objects, and therefore for $t = O(\log n)$ we have $2m + 2k = O(\mathrm{poly}(n))$[1].

Let us assume to be able to sample from the distribution Ξ_{ψ_t}. Later on, in Section 4, we discuss in which situations an efficient sampling from Ξ_{ψ_t} is possible by querying the t-doped state ψ_t. We first aim to learn a basis for the stabilizer group

[1] Essentially, the complexity stems from the fact that the support $|S_{\psi_t}| \leq 2^t d$. However, it's worth noting that a weaker form of such a bound, i.e., $|S_{\psi_t}| \leq 3^t d$, was previously demonstrated in Ref. [15].

G_{ψ_t}, i.e. m generators g_i. Sampling from Ξ_{ψ_t} we get a Pauli operator $P \in G_{\psi_t}$ with probability

$$\Pr(P \in G_{\psi_t}) = \frac{|G_{\psi_t}|}{d} \geq \frac{1}{2^t}\,. \tag{6}$$

Therefore, after $O(2^t)$ samples one gets a Pauli operator sampled uniformly from G_{ψ_t} with high probability. To check whether a sampled Pauli operator P stabilizes $|\psi_t\rangle$ is sufficient to measure M times P. If all the measurement outcomes are equal, then $P \in G_{\psi_t}$ with failure probability at most $(1-2^{-t})(h_{\max}/2+1/2)^M$ (see Appendix C), where $h_{\max} \equiv \max_{h_i} |\operatorname{tr}(h_i\psi_t)|$. We remark that the above procedure also reveals the stabilizing phase ϕ_P corresponding to $P \in G_{\psi_t}$. Following the reasoning introduced by Montanaro [10], the extraction of $m+n$ random Pauli operators $\in G_{\psi_t}$ suffices to identify a set of generators $g_1, \ldots, g_m$ with failure probability at most 2^{-n}. Indeed, determining a basis for G_{ψ_t} is equivalent to determining a basis for the m-dimensional subspace T of $\mathbb{F}_2^{2n}$; the probability that $n+m$ random samples from T lie in a $(m-1)$-dimensional subspace of T is 2^{-m-n} and – by the union bound – the probability that these samples lie in one of the 2^m $(m-1)$-dimensional subspaces of T is at most 2^{-n}. We conclude that $O(2^t(n+m))$ samples from the probability distribution Ξ_{ψ_t}, plus $O(2^t(n+m)M)$ additional measurement shots, are sufficient to learn all the generators $g_1, \ldots, g_m$ and phases ϕ_{g_i} with failure probability $O(2^t(n+m)(h_{\max}/2+1/2)^M + 2^{-n})$.

At this point, let us learn the k bad generators $h_1, \ldots, h_k$. Suppose the algorithm already found l out of k bad generators, say $h_1, \ldots, h_l$. To find the $(l+1)$-th bad generator, we keep sampling from Ξ_{ψ_t}. The probability π_l that the sampled Pauli operator P does not belong to $G_{\psi_t} \cup h_1 G_{\psi_t} \cup \ldots \cup h_l G_{\psi_t}$ is

$$\pi_l = 1 - \frac{|G_{\psi_t}|}{d}\left(1 + \sum_{i=1}^{l} \operatorname{tr}^2(h_i\psi_t)\right)\,. \tag{7}$$

To find a useful lower bound to π_l, let us exploit the unit purity of the state ψ_t. In Appendix C, we obtain

$$\pi_l \geq |G_{\psi_t}|(k-l)h_{\min}^2/d \tag{8}$$

with $h_{\min} := \min_{h_i} |\operatorname{tr}(h_i\psi_t)|$. However, a learner needs an efficient way to check whether a sampled Pauli operator belongs to $G_{\psi_t} \cup h_1 G_{\psi_t} \cup \ldots \cup h_l G_{\psi_t}$. Let us provide a simple algorithm to efficiently check whether a Pauli operator P belongs to $G_{\psi_t} \cup h_1 G_{\psi_t} \cup \ldots \cup h_l G_{\psi_t}$ or not. Let us assume $P \in h_0 G_{\psi_t} \cup h_1 G_{\psi_t} \cup \cdot \cup h_l G_{\psi_t}$, where $h_0 = \mathbb{1}$. Then for some $i \in 0 \ldots l$, there exists h_i such that $h_i P \in G_{\psi_t}$. Thus the problem reduces to check if there exists an $h_i \in \{h_0, \ldots, h_l\}$ such that $h_i P \in G_{\psi_t}$. The latter can be solved by adding $h_i P$ to a generating set G_{ψ_t} and performing Gaussian elimination over $\mathbb{F}_2^{2n}$. The task requires $O(n^3)$ steps and has to be repeated l times, meaning that the full task requires $O(n^3 l)$ computational steps, and so to learn all the k bad generators one needs $O(n^3k^2)$. In appendix B we provide a slightly more efficient algorithm relying instead on the notion of diagonalizer[18, 19] where the number of computational steps to verify the containment of one bad generator is $O(n^2k)$, and so reducing the computational steps to learn all the bad generators to $O(n^2k^2)$. The total number of samples scales as $\sum_{l=0}^{k-1} \pi_l^{-1} \leq 2^t h_{\min}^{-2} \sum_{l=0}^{k-1}(k-l)^{-1} \leq 2^t h_{\min}^{-2}(\gamma + \log(k+1))$ for γ being the Euler's constant. Therefore using $O\left(2^t h_{\min}^{-2}\log(k+1)\right)$ samples from Ξ_{ψ_t}, plus $O(n^2k^2)$ computational steps, one learns the k bad generators $h_1, \ldots, h_k$. To evaluate $h_{\min}$ and $h_{\max}$, let us recall that the state $|\psi_t\rangle$ is obtained from the computational basis state $|0\rangle^{\otimes n}$ by a Clifford circuit polluted with t single qubit T-gates, that generate a discrete set of states, which ultimately implies the existence of a finite resolution $\delta_t \equiv \min |\operatorname{tr}[(P-Q)\psi_t]|$ for $\operatorname{tr}(P\psi_t) \neq \operatorname{tr}(Q\psi_t)$. From Eq. (5), one has $\delta_t = \Omega(2^{-bt})$ for $b \simeq 2.27$. Therefore $O(2^{2bt})$ measurement shots are sufficient to determine the expectation value $\operatorname{tr}(h_i\psi_t)$ exactly. In addition, one has $h_{\min} = \Omega(2^{-bt})$ and $h_{\max} < 1 - O(2^{-bt})$. In summary, to learn k bad generators and the corresponding expectations, the learner employs $O(2^{(2b+1)t}\log(k+1))$ samples from Ξ_{ψ_t}, $O(k2^{2bt})$ measurement shots, and $O(n^2k^2)$ additional computational steps.

Let us count the total number of resources to learn a t-doped stabilizer state employing the algorithm proposed above. Set $m \leq n$, $k < 4^t$, $b < 3$ and $M = 2^{3t+1}(n+t)$. The total number of samples from the probability distribution Ξ_{ψ_t} is $O(2^t n + t2^{5t})$ plus $O(4^t n^2)$ additional computational steps. The total number of measurement shots is $O(2^{7t} + 2^{4t}n(n+t))$ and the algorithm fails with probability at most $O(n2^{-n})$. Therefore for $t = O(\log n)$, the algorithm learns the tomographic description of a t-doped stabilizer state of Eq. (3) with polynomial resources and overwhelming probability.

4 Sampling from Ξ_{ψ_t}

In Section 3, we provided an algorithm that learns a t-doped stabilizer state with $\operatorname{poly}(n, 2^t)$ resources. In particular, the algorithm uses $O(2^t n +$

$t2^{5t}$) samples from the probability distribution Ξ_{ψ_t} with elements $\Xi_{\psi_t}(P) = \mathrm{tr}^2(P\psi_t)/d$. Let us discuss the connection between queries to the unknown state $|\psi_t\rangle$ and samples from the distribution Ξ_{ψ_t}. Having query access to the t-doped stabilizer state $|\psi_t\rangle$ and its conjugate (in the computational basis) $|\psi_t^*\rangle$, one can easily achieve the task via Bell sampling. Define the Bell basis on two copies of Hilbert space $\mathcal{H}$ as $|P\rangle \equiv \mathbb{1} \otimes P\,|\mathbb{1}\rangle$ with $|\mathbb{1}\rangle = 2^{-n/2}\sum_{i=1}^{2^n} |i\rangle \otimes |i\rangle$ and $P \in \mathbb{P}_n$. Then, measuring $|\psi_t \otimes \psi_t^*\rangle$ in the basis $|P\rangle$ is equivalent to sample from the distribution Ξ_{ψ_t}:

$$\Pr(|\psi_t \otimes \psi_t^*\rangle \mapsto |P\rangle) = \Xi_{\psi_t}(P)\,. \tag{9}$$

Therefore a single query to $|\psi_t\rangle$ and its conjugate $|\psi_t^*\rangle$ suffices to obtain one sample from the distribution Ξ_{ψ_t}.

At this point, the careful reader may wonder how the learner can prepare the conjugate state $|\psi_t^*\rangle$ in order to use the algorithm. We have a manifold of answers to this. First of all, an important situation in which learning is important is that of the study of ground states of quantum many-body systems. An example is provided by stabilizer Hamiltonians [21] perturbed by local impurities, which exhibit t-doped stabilizer eigenstates as shown in [22]. Generically, as long as time-reversal is not broken, these are real states, and thus $|\psi_t^*\rangle = |\psi_t\rangle$. Moreover, in many scenarios, the preparation itself of the state $|\psi_t\rangle$ can be thought of as made by a quantum circuit. In this case then, the task of preparing $|\psi_t^*\rangle$ is straightforward. Indeed, it is sufficient to replace the gate $S = \mathrm{diag}(1, i)$ with $S^* = \mathrm{diag}(1, -i)$ and the T-gate with TS^* to obtain U_t^* and thus constructing $|\psi_t^*\rangle$ from $|0\rangle^{\otimes n}$.

In any case, while distilling the conjugate state is a hard task in general, the states under examination in this paper for which the learning is efficient, i.e. t-doped stabilizer states with $t = O(\log n)$, have fine structure and hardness proofs fail at capturing the hardness of distilling $|\psi_t^*\rangle$ from samples of $|\psi_t\rangle$. For example, the hardness proof in Ref. [23] uses pseudorandom quantum states and it is known that pseudorandom quantum states contain $\omega(\log n)$ many T-gates [24]. Indeed, from the knowledge of the algebraic structure in Eq. (3), sampling from the characteristic distribution is straightforward: it is sufficient to flip a k-faceted dice with probabilities $\chi_{\psi_t}(h_i)$ – defined above in Section 2 – and outcomes h_i, and uniformly sample a Pauli operator $P \in G_{\psi_t}$ through m generators. As a result, one samples a Pauli operator $h_i P$ according to Ξ_{ψ_t}. This procedure is readily efficient for $k = O(\mathrm{poly}(n))$, i.e. for $t = O(\log(n))$. Therefore, for $t = O(\log n)$, there is no reason to believe that sampling from the distribution Ξ_{ψ_t}, with queries limited to $|\psi_t\rangle$ alone and without knowing the algebraic structure (3) (i.e. bypassing the a priori learning of the t-doped stabilizer state), is hard and, as such, it remains an ongoing subject of research. Remarkably, in Ref. [25], an algorithm is presented capable of sampling from the characteristic distribution that includes, but is not limited to, states with $t = O(\log n)$ and low entanglement.

5 Learning algorithm without access to Ξ_{ψ_t}

We discussed a simple and intuitive learning algorithm that works whenever one has access to samples from the distribution Ξ_{ψ_t}. However, as we saw in Section 4, known methods for sampling from Ξ_{ψ_t} require query access to the t-doped stabilizer state and its conjugate in the computational basis, which is not always available in real scenarios. In this section, we present an algorithm similar in spirit to the one in Section 3, but we relax the hypothesis of having samples from Ξ_{ψ_t}.

As measuring $|\psi_t \otimes \psi_t^*\rangle$ in the Bell basis $|P\rangle$ returns samples from Ξ_{ψ_t}, measuring $|\psi_t \otimes \psi_t\rangle$ in the Bell basis returns samples from

$$\widetilde{\Xi}_{\psi_t}(P) \equiv \frac{|\,\langle\psi_t|P|\psi_t^*\rangle\,|^2}{d}\,. \tag{10}$$

Let us show that samples from $\widetilde{\Xi}_{\psi_t}$ are still sufficient to learn the stabilizer group G_{ψ_t} and, ultimately, the t-doped stabilizer state ψ_t exactly. To see this, it is useful to show how the algebraic structure changes from ψ_t to ψ_t^*. Naively, from Eq. (3), we can write the density matrix associated to ψ_t^* as

$$\psi_t^* = \frac{1}{d}\sum_{i=0}^{k} \mathrm{tr}(h_i\psi_t^*)h_i \prod_{j=1}^{m}(\mathbb{1} + \phi_{g_j} g_j^*)\,. \tag{11}$$

To understand the algebraic structure of ψ_t^*, it is useful to look back at the simple case of stabilizer states, i.e. $t = 0$. As shown by Montanaro in Ref. [10], given a stabilizer state $|\sigma\rangle$, its conjugate $|\sigma^*\rangle$ can be obtained with a Pauli rotation as $|\sigma^*\rangle = P_\sigma\,|\sigma\rangle$ for some Pauli operator P_σ. Similarly, since the projector Π_{ψ_t} in Eq. (3), onto the stabilizer group G_{ψ_t}, can be completed to represent a pure stabilizer state (by completion of the stabilizer group G_{ψ_t}), it is immediate to see that there exist a Pauli operator P_{ψ_t} such that (see Appendix D)

$$P_{\psi_t}\Pi_{\psi_t}P_{\psi_t} = \Pi_{\psi_t}^*\,, \tag{12}$$

where $\Pi^*_{\psi_t} \equiv 2^{-m} \prod_{j=1}^{m} (\mathbb{1} + \phi_{g_j} g_j^*)$. In other words, analogously to the case of stabilizer states, the projectors onto the stabilizer groups $\Pi_{\psi_t}, \Pi^*_{\psi_t}$, of ψ_t and ψ_t^* respectively, can be obtained from one another by the application of a Pauli operator P_{ψ_t}. Hence, the state $|\psi_t^{*\prime}\rangle := P_{\psi_t} |\psi_t^*\rangle$ has the same stabilizer group G_{ψ_t} of ψ_t, by construction.

As explained in Section 2, from the projector Π_{ψ_t} onto the stabilizer group G_{ψ_t}, one can define a diagonalizer $\mathcal{D}$. Since the stabilizer groups are the same, $\mathcal{D}$ diagonalizes $|\psi_t\rangle$ and $|\psi_t^{*\prime}\rangle$ at the same time as $\mathcal{D}|\psi_t\rangle = |0\rangle^{\otimes m} \otimes |\phi\rangle$ and $\mathcal{D}|\psi_t^{*\prime}\rangle = |0\rangle^{\otimes m} \otimes |\phi^*\rangle$, cfr. Eq. (4). By simple manipulations, we can thus rewrite the probability in Eq. (10) as only depending on the nonstabilizer part $|\phi\rangle$ of the t-doped stabilizer state $|\psi_t\rangle$ as

$$\widetilde{\Xi}_{\psi_t}(P) = \frac{|\langle \phi | \bar{P} | \phi^* \rangle|^2}{d}, \tag{13}$$

with $\bar{P} \equiv \langle 0^{\otimes m} | \mathcal{D} P P_{\psi_t} \mathcal{D}^\dagger | 0^{\otimes m} \rangle$. It is easy to be convinced that the probability $\widetilde{\Xi}_{\psi_t}(P)$ is different from zero only if $P P_{\psi_t} \in \mathcal{D}^\dagger (\mathbb{1}_m \otimes \bar{P}) \mathcal{D} G_{\psi_t}$ for any $\bar{P} \in \mathbb{P}_{n-m}$ living on the last $(n-m)$ qubits. Hence, samples from $\widetilde{\Xi}_{\psi_t}(P)$ returns Pauli operators $P \in \{\mathcal{D}^\dagger (\mathbb{1}_m \otimes \bar{P}) \mathcal{D} G_{\psi_t} \,|\, \bar{P} \in \mathbb{P}_{n-m}\}$ with probability (13). As in the case of stabilizer states, to gain knowledge of the stabilizer group G_{ψ_t}, it is sufficient to obtain two Pauli operators P, P' belonging to the same left coset $P, P' \in \mathcal{D}^\dagger (\mathbb{1}_m \otimes \bar{P}) \mathcal{D} G_{\psi_t}$, and consider the product $PP' \in G_{\psi_t}$. At this point, the joint probability that two samples give a product Pauli operator belonging to G_{ψ_t} is lower bounded by

$$\Pr(PP' \in G_{\psi_t}) \geq \frac{1}{2^{6t}} \tag{14}$$

where the proof is in Appendix D. Therefore, repeating the reasoning outlined in Section 3 after Eq. (6), we conclude that $O(2^{6t}(n+m))$ samples from $\widetilde{\Xi}_{\psi_t}$, plus $O(2^{9t} n(n+6t))$ additional measurement shots, are sufficient to learn all the generators $g_1, \ldots, g_m$ and phases ϕ_{g_i} with exponentially small probability of failure $O(n 2^{-n})$.

Having learned the generators g_i and relative phases ϕ_{g_i}, it is thus possible, through standard tableau manipulation techniques (see Ref. [18]), to construct and distill the diagonalizer $\mathcal{D}$ in Eq. (4) using $O(n^2)$ computational steps and up to $O(n)$ Clifford gates [26]. Applying $\mathcal{D}$ on the t-doped stabilizer state $|\psi_t\rangle$, one gets $\mathcal{D}|\psi_t\rangle = |0\rangle^{\otimes m} \otimes |\phi\rangle$. At this point, one is left to learn the tomographic description of $|\phi\rangle$ in terms of Pauli operators $\tilde{h}_i \equiv \mathcal{D} h_i \mathcal{D}^\dagger$. To achieve this task, it is sufficient to individually measure each Pauli operator $\tilde{h}_i$ for $i = 1, \ldots, k$. In virtue of Eq. (5), to estimate the expectation values $\mathrm{tr}(h_i \psi_t)$ exactly, $O(2^{2bt})$ samples are sufficient, and thus to learn the expectation values of k bad generators $h_i, \ldots, h_k$ one needs $O(4^t 2^{2bt})$ total measurement shots. In summary, the above algorithm learns an exact tomographic description of a t-doped stabilizer state using $O(2^{6t} n)$ samples from the distribution $\tilde{\Xi}$ (which in turn can be obtained by measuring 2 copies of ψ_t in the basis $|P\rangle$), $O(2^{9t} n(n+6t))$ measurement shots, $O(n^2)$ additional computational steps, and fails with probability $O(n 2^{-n})$.

The careful reader might have noticed similarities between the procedure outlined above and the subroutine known as *Bell difference sampling* [27], where one considers two samples from the distribution $\widetilde{\Xi}_{\psi_t}$ and, subtracting the results, obtain sample Pauli operators $P \in G^\perp_{\psi_t} = \{P \in \mathbb{P} \,|\, [P, G_{\psi_t}] = 0\}$ whose knowledge allows to reconstruct the stabilizer group G_{ψ_t}, as shown in [28]. There are two key insights here: first, the derivation outlined above solely descends from the algebraic structure of t-doped stabilizer states developed in this paper that provide a simple proof of the results. Secondly, the algorithm outlined above and the Bell difference sampling routine exhibit similarities, yet they are not entirely identical. Specifically, the above algorithm exclusively accommodates pairs of Pauli operators, denoted as P and P', whose product resides within $G_{\psi_t} \subset G^\perp_{\psi_t}$. Hence, it does not need any classical postprocessing. This fact allows for the complete and precise determination of the stabilizer group G_{ψ_t} with overwhelming probability, albeit at the expense of an exponential increase in computational cost with respect to t, a scaling that Bell difference sampling does not possess.

6 Concurrent work

During the finalization of this manuscript, we became aware of two works [28, 29] sharing several similarities with ours, presenting an efficient approach for learning t-doped stabilizer states. This section aims to compare algorithms. The algorithms presented separately in [28] and [29] are quite similar. Hence, we focus on comparing the one from [28] with ours for simplicity.

The algorithm in [28] has a significant advantage: it uses Bell difference sampling to approximate the stabilizer group G_{ψ_t} associated with the t-doped stabilizer state $|\psi_t\rangle$ using $O(n)$ resources, avoiding exponential scaling with the number t of non-Clifford gates. However, it only learns an approximate version of the stabilizer group, which might not suit cases where an exact description of

a t-doped stabilizer state is required. For T-gates, exact learning is desirable since these states are countable and form a discrete set. Whether the algorithm [28] can be employed to learn the exact stabilizer group in light of the finite resolution proven in Eq. (5) is not clear. The algorithm presented in Section 5 of this paper, leveraging the algebraic structure introduced here, can precisely learn the stabilizer group G_{ψ_t} from copies of $|\psi_t\rangle$, with an exponentially small probability of failure. However, this precise learning comes at the cost of exponential resource scaling with the number of T-gates. Compared to the algorithm in [28], our algorithm's primary strength lies in its exact learning ability for states created by Clifford+T circuits, enabled by Eq. (5). Both algorithms in Section 3 and 5, with different methods, whose limitations have been explored above, achieve the exact learning of the algebraic structure of t-doped stabilizer state displayed in Eq. (3). However, it's important to note that these states are not the only ones with polynomially many bad generators, and therefore our algorithms do not cover the larger class of states learnable according to the algorithm in Ref. [28], which, in this regard, is more general. Overall, we conclude that the two algorithms exhibit distinct ranges of applicability and employ different techniques to achieve the same task, each with its own set of strengths and limitations.

7 Conclusions

In conclusion, we presented an efficient and general algorithm that can learn a classical description of states obtained from the computational basis by the action of the Clifford group plus a few T gates. To address this challenge, we introduced a new algebraic structure for t-doped stabilizer states that is of independent interest and plays a crucial role in the learning algorithm.

In perspective, there are several open questions. First, we ask whether the algebraic structure presented in this paper can be instrumental in solving tasks beyond quantum state tomography for t-doped stabilizer state, e.g. in computing quantity as entanglement or magic. Second, we would like to know whether the knowledge of both the generators and the bad generators can be utilized to synthesize a Clifford+T circuit able to construct the state $|\psi_t\rangle$ from $|0\rangle^{\otimes n}$. Indeed, note that the task is conceivable for two reasons: 1) because the complexity (i.e. the number of gates) of Clifford+T circuits scales as $O(n^2 + t^3)$ [2] as a consequence of the results of [18, 19, 26]; 2) given a t-doped stabilizer state, one can learn exactly the Clifford circuit $\mathcal{D}$, reducing the task of learning the circuit description to u_t only. Lastly, the estimated resources are computed for the worst case. We ask whether the average case complexity for the exact learning of t-doped stabilizer states doped with T-gates is more favorable in terms of the exponential scaling in t.

[2] By Theorem 2 of [18] a Clifford+T circuit C_t with $t \leq n$ has the following decomposition $C_t = C_1(\mathbb{1} \otimes u_t)C_2$, with $C_1, C_2 \in \mathcal{C}_n$ and u_t a t-doped Clifford circuit on t-qubits consisting of at most t many T gates. From [26], any Clifford circuit can be implemented with at most $O(n^2)$ gates. Thus, $\#(C_i) = O(n^2)$ for $i, 1, 2$ and $\#(u_t) = O(t^3)$, and consequently the total complexity is $O(n^2 + t^3)$

Acknowledgments

The authors acknowledge discussions with M. Hinsche, M. Ioannou, S. Jerbi, J. Carrasco and G. Esposito. The authors would like to express their gratitude to Daniel Miller for his valuable insight regarding the existence of a finite resolution for t-doped stabilizer states. The authors thank the anonymous Reviewer 1 for their constructive comments and suggestions that helped to improve the manuscript. Special thanks go to Lennart Bittel for fundamental inceptions for the proof of the lower-bound in Eq. (5). AH was supported by the ENEA project I53C22003030001, the PNRR MUR project PE0000023-NQSTI and PNRR MUR project CN 00000013-ICSC. L.L. S.F.E.O. acknowledge support from NSF award number 2014000. L.L. and S.F.E.O. contributed equally to this work.

References

[1] Matteo Paris and Jaroslav Řeháček, editors. "Quantum State Estimation". Volume 649 of Lecture Notes in Physics. Springer. Berlin, Heidelberg (2004).

[2] Marcus Cramer, Martin B. Plenio, Steven T. Flammia, Rolando Somma, David Gross, Stephen D. Bartlett, Olivier Landon-Cardinal, David Poulin, and Yi-Kai Liu. "Efficient quantum state tomography". Nat. Commun. **1**, 149–149 (2010).

[3] David Gross, Yi-Kai Liu, Steven T. Flammia, Stephen Becker, and Jens Eisert. "Quantum State Tomography via Compressed Sensing". Phys. Rev. Lett. **105**, 150401–150401 (2010).

[4] Scott Aaronson. "Shadow Tomography of Quantum States". In Proceedings of the 50th

Annual ACM SIGACT Symposium on Theory of Computing. Pages 325–338–325–338. Association for Computing Machinery (2018).

[5] Cupjin Huang, Fang Zhang, Michael Newman, Junjie Cai, Xun Gao, Zhengxiong Tian, Junyin Wu, Haihong Xu, Huanjun Yu, Bo Yuan, et al. "Classical simulation of quantum supremacy circuits" (2020). arxiv:2005.06787.

[6] Hsin-Yuan Huang, Richard Kueng, and John Preskill. "Predicting many properties of a quantum system from very few measurements". Nat. Phys. **16**, 1050–1057 (2020).

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

[8] Scott Aaronson and Sabee Grewal. "Efficient Tomography of Non-Interacting-Fermion States". In Omar Fawzi and Michael Walter, editors, 18th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2023). Volume 266 of Leibniz International Proceedings in Informatics (LIPIcs), pages 12:1–12:18. Dagstuhl, Germany (2023). Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[9] Daniel Gottesman. "The Heisenberg Representation of Quantum Computers" (1998). arxiv:quant-ph/9807006.

[10] Ashley Montanaro. "Learning stabilizer states by Bell sampling" (2017). arxiv:1707.04012.

[11] Dagmar Bruß and Chiara Macchiavello. "Optimal state estimation for d-dimensional quantum systems". Phys. Lett. A **253**, 249–251 (1999).

[12] Daniel Gottesman. "Theory of fault-tolerant quantum computation". Phys. Rev. A **57**, 127–137–127–137 (1998).

[13] Lorenzo Leone, Salvatore F. E. Oliviero, You Zhou, and Alioscia Hamma. "Quantum Chaos is Quantum". Quantum **5**, 453–453 (2021).

[14] Salvatore F. E. Oliviero, Lorenzo Leone, and Alioscia Hamma. "Transitions in entanglement complexity in random quantum circuits by measurements". Phys. Lett. A **418**, 127721–127721 (2021).

[15] Ching-Yi Lai and Hao-Chung Cheng. "Learning Quantum Circuits of Some T Gates". IEEE Transactions on Information Theory **68**, 3951–3964–3951–3964 (2022).

[16] Lorenzo Leone, Salvatore F. E. Oliviero, and Alioscia Hamma. "Stabilizer Rényi Entropy". Phys. Rev. Lett. **128**, 050402–050402 (2022).

[17] Jiaqing Jiang and Xin Wang. "Lower bound for the t count via unitary stabilizer nullity". Phys. Rev. Appl. **19**, 034052 (2023).

[18] Lorenzo Leone, Salvatore F. E. Oliviero, Seth Lloyd, and Alioscia Hamma. "Learning efficient decoders for quasichaotic quantum scramblers". Phys. Rev. A **109**, 022429 (2024).

[19] Salvatore F. E. Oliviero, Lorenzo Leone, Seth Lloyd, and Alioscia Hamma. "Unscrambling quantum information with clifford decoders". Phys. Rev. Lett. **132**, 080402 (2024).

[20] Michael Beverland, Earl Campbell, Mark Howard, and Vadym Kliuchnikov. "Lower bounds on the non-Clifford resources for quantum computations". Quantum Sci. and Technol. **5**, 035009–035009 (2020).

[21] Nolan J. Coble, Matthew Coudron, Jon Nelson, and Seyed Sajjad Nezhadi. "Hamiltonians whose low-energy states require $\Omega(n)$ T gates" (2023). arxiv:2310.01347.

[22] Andi Gu, Salvatore F. E. Oliviero, and Lorenzo Leone. "Doped stabilizer states in many-body physics and where to find them" (2024). arXiv:2403.14912.

[23] Tobias Haug, Kishor Bharti, and Dax Enshan Koh. "Pseudorandom unitaries are neither real nor sparse nor noise-robust" (2023). arxiv:2306.11677.

[24] Sabee Grewal, Vishnu Iyer, William Kretschmer, and Daniel Liang. "Improved stabilizer estimation via bell difference sampling" (2024). arXiv:2304.13915.

[25] Marcel Hinsche, Marios Ioannou, Sofiene Jerbi, Lorenzo Leone, Jens Eisert, and Jose Carrasco. "Efficient distributed inner product estimation via Pauli sampling" (2024) arXiv:2405.06544.

[26] Sergey Bravyi and Dmitri Maslov. "Hadamard-Free Circuits Expose the Structure of the Clifford Group". IEEE Transactions on Information Theory **67**, 4546–4563 (2021).

[27] David Gross, Sepehr Nezami, and Michael Walter. "Schur–Weyl duality for the Clifford group with applications: Property testing, a robust Hudson theorem, and de Finetti representations". Communications in Mathematical Physics **385**, 1325–1393–1325–1393 (2021).

[28] Sabee Grewal, Vishnu Iyer, William Kretschmer, and Daniel Liang. "Efficient Learning of Quantum States Prepared With Few Non-Clifford Gates" (2023). arxiv:2305.13409.

[29] Dominik Hangleiter and Michael J. Gullans.

"Bell sampling from quantum circuits" (2023). arxiv:2306.00083.

[30] M. Ram Murty and Purusottam Rath. "Liouville's Theorem". In M. Ram Murty and Purusottam Rath, editors, Transcendental Numbers. Pages 1–6. Springer, New York, NY (2014).

A Technical preliminaries

In this section, we will introduce some technical preliminaries that may prove beneficial to the reader.

A.1 Pauli Group, Clifford group, and stabilizer states

The Pauli group $\mathcal{P}_n$ is the n-tensor fold product of the single-qubit Pauli group $\mathcal{P}_1$, which consists of the elements $\mathbb{1}, X, Y, Z$, each multiplied by a scaling factor of $\pm 1, \pm i$, where X, Y and Z are the standard single-qubit Pauli matrices. Let us introduce the quotient group $\mathbb{P}_n$ of the Pauli group $\mathbb{P} := \mathcal{P}/\{\pm 1, \pm i\}$. In the main text, we refer to the quotient group as Pauli group. The Clifford group $\mathcal{C}(n)$ on n qubit, i.e. a subgroup of the unitary group is defined as the normalizer of the Pauli group $\mathcal{P}_n$:

$$\mathcal{C}_n := \{C \in \mathcal{U}(n) \mid C^\dagger P C \in \mathcal{P}, \quad \forall P \in \mathcal{P}_n\}. \tag{15}$$

With the notion of Pauli and Clifford group, one can then define the notion of a stabilizer state. Given a Pauli operator $P \in \mathbb{P}_n$, we say that P stabilizes the state $|\psi\rangle$ if

$$P|\psi\rangle = \pm|\psi\rangle \tag{16}$$

A state $|\sigma\rangle$ is a stabilizer states if $|\sigma\rangle$ is stabilized by an group G of d commuting Pauli operators

$$P|\sigma\rangle = \pm|\sigma\rangle \quad \forall P \in G \tag{17}$$

Equivalently, one can define a stabilizer state as $|\sigma\rangle \equiv C|0\rangle^{\otimes n}$ with $C \in \mathcal{C}_n$. It is noteworthy to notice that a stabilizer state can be written as an equal superposition of Pauli operators that stabilizes it

$$\sigma = \frac{1}{d}\sum_{P\in G} \sigma_P P \tag{18}$$

where σ is the density matrix associated to $|\sigma\rangle$ and $\sigma_p = \pm 1$ is the phase associated to P. Being G an Abelian group, there exists a set of generators $S \equiv \{g_1, \ldots, g_n\}$ such that $G = \langle S \rangle$. Thus, given S the set of generators associate with G the state σ can be expressed in terms of the generator $g_i \in S$ as

$$\sigma = \prod_i \left(\frac{\mathbb{1} + \phi_{g_i} g_i}{2}\right) \tag{19}$$

where ϕ_{g_i} are the ± 1 phases associated with the generators g_is.

A.2 Bell Sampling

In this section, we will review the concept of Bell sampling [10] and its application in learning a stabilizer state. To grasp the idea behind Bell sampling, let's begin by considering the 2-qubit maximally entangled state, denoted as $|\mathbb{1}\rangle$, which is defined as $(|00\rangle + |11\rangle)/\sqrt{2}$. If we apply the operator $\mathbb{1} \otimes P$, where $P = \mathbb{1}, X, Y, Z$, to the state $|\mathbb{1}\rangle$, we obtain the set of states: $|\mathbb{1}\rangle$, $|X\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$, $|Y\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$, and $|Z\rangle = (|00\rangle - |11\rangle)/\sqrt{2}$. This set of states corresponds to the 2-qubit Bell basis. This equivalence between Pauli operators and states can be extended to the n-qubit case. The reason behind this extension lies in the fact that the n-qubit Pauli group is constructed as the n-fold tensor product of the 1-qubit Pauli group. Consequently, we can tensor 2-qubit states $|P\rangle$ to establish an equivalence between the n-qubit Pauli group and the $2n$-qubit Bell basis. In this context, a generic basis element can be written as $|P\rangle \equiv \mathbb{1} \otimes P|\mathbb{1}\rangle$, where $|\mathbb{1}\rangle$ denotes the $2n$-qubit maximally entangled state, defined as $|\mathbb{1}\rangle = 2^{-n/2}\sum_i^d |i\rangle \otimes |i\rangle$. Let us consider the state $|\psi^*\rangle \otimes |\psi\rangle$, it is not difficult to show that

measuring in the Bell basis return outcome P with probability $\mathrm{tr}(P\psi)^2/d$, with ψ the density matrix associated to the state ψ. The probability to obtain P is given by $|\langle P|\psi^*\otimes\psi\rangle|^2$

$$
\begin{aligned}
|\langle P|\psi^*\otimes\psi\rangle|^2 &= \langle\mathbb{1}|\mathbb{1}\otimes P[\psi^*\otimes\psi]\mathbb{1}\otimes P|\mathbb{1}\rangle &(20)\\
&= \langle\mathbb{1}|\mathbb{1}\otimes P\psi P\psi|\mathbb{1}\rangle &(21)\\
&= \mathrm{tr}(P\psi P\psi)/2^n = \mathrm{tr}(P\psi)^2/2^n &(22)
\end{aligned}
$$

where we used the properties of the maximally entangled state that $O\otimes\mathbb{1}|\mathbb{1}\rangle = \mathbb{1}\otimes O^T|\mathbb{1}\rangle$, and that the state ψ is pure. If instead of having access to $|\psi^*\rangle\otimes|\psi\rangle$ one has instead access to $|\psi\rangle\otimes|\psi\rangle$ the probability of sampling P is given by $|\langle\psi|P|\psi^*\rangle|^2/2^n$. Through Bell sampling, one can learn a stabilizer state $|\sigma\rangle$ if provided access to $|\sigma^*\rangle\otimes|\sigma\rangle$. In this process, Bell basis measurements are performed K times, and the resulting measurement outcomes yield a set of strings denoted as T. This set T consists of $2n$-dimensional strings, each identifying a Pauli operator P such that $P\in G_\sigma$, where G_σ is the stabilizer group of $|\sigma\rangle$. Finding an n-dimensional basis for the T is equivalent to finding a set of generators for the stabilizer group G_σ.

The potential failure of this process occurs when all the K samples lie in a subspace of T with dimension less than n. The probability that all the obtained samples fall within such a subspace is 2^{-K}. By applying the union bound, we find that the probability of these samples lying in one of the 2^n $(n-1)$-dimensional subspaces of T is 2^{-K+n}. To mitigate this probability of failure, one can choose $K=2n$, resulting in an exponentially vanishing probability of failure. With the set of generators for G_σ obtained, one can learn the phases by making a single-shot measurement of the expectation value of the learned Pauli generators.

In cases where access is limited to $|\sigma\rangle\otimes|\sigma\rangle$, rather than $|\sigma^*\rangle\otimes|\sigma\rangle$, it is still possible to learn the stabilizer state through a similar procedure. First, it is worth noting that for a stabilizer state $|\sigma^*\rangle = \bar{P}|\sigma\rangle$, where P is a Pauli string consisting of $Z,\mathbb{1}$ operators. Consequently, the probability of sampling the Pauli operator P can be rewritten as $|\langle\sigma|P\bar{P}|\sigma\rangle|^2/2^n$. Although P does not stabilize $|\sigma\rangle$, the Pauli operator $P\bar{P}$ does it; otherwise, the sampling probability would be zero. Thus, when two Pauli operators, P_1 and P_2, are sampled, their product stabilizes $|\sigma\rangle$. This can be demonstrated straightforwardly by noting that both $P_1\bar{P}$ and $P_2\bar{P}$ stabilize $|\sigma\rangle$, and their product, $P_1\bar{P}P_2\bar{P}$, remains a Pauli operator that stabilizes $|\sigma\rangle$. Furthermore, it is proportional to P_1P_2, with the proportionality factor possibly being ±1 due to the commutation relations between $\bar{P}$ and P_2.

Thanks to this property, instead of sampling K times, one only needs to sample $K+1$ times to determine the set of generators for G_σ, while maintaining the same failure probability.

B Efficient verification of containment

In this section, we provide an alternative algorithm based on the notion of diagonalizer to efficiently verify the containment of a Pauli operator P to the set $G_{\psi_t}\cup h_1G_{\psi_t}\cup\ldots\cup h_lG_{\psi_t}$. Let $\mathbb{Z}_n\subset\mathbb{P}_n$ the subgroup of the Pauli group generated by $\{\sigma_i^z\}_{i=1}^n$, with $\sigma_i^z=\mathrm{diag}(1,-1)$ on the i-th qubit. Then let $\mathcal{D}\in\mathcal{C}_n$ be a Clifford circuit such that $\tilde{G}_{\psi_t}\equiv\mathcal{D}G_{\psi_t}\mathcal{D}^\dagger\subset\mathbb{Z}_n$. Notice that $\mathcal{D}$ can be found from a set of generators of G_{ψ_t} in time $O(n^2)$ [18, 19]. Define $\tilde{h}_i\equiv\mathcal{D}h_i\mathcal{D}^\dagger$, which requires computational complexity $O(n^2l)$. To check whether $P\notin G_{\psi_t}\cup h_1G_{\psi_t}\cup\ldots\cup h_kG_{\psi_t}$ is sufficient to check that $\mathcal{D}P\mathcal{D}^\dagger\notin\tilde{G}_{\psi_t}\cup\tilde{h}_i\tilde{G}_{\psi_t}\cup\ldots\cup\tilde{h}_l\tilde{G}_{\psi_t}$ that – thanks to the local support of σ_i^zs – can be easily achieved by a qubit by qubit checking in time $O(nl)$. Consequently, the final runtime to verify if a Pauli operator P belongs to $G_{\psi_t}\cup h_1G_{\psi_t}\cup\ldots\cup h_lG_{\psi_t}$ is $O(n^2k)$.

C Proofs

C.1 Disjoint cosets.

In this section, we will prove the disjointedness of the cosets. Let us consider $P\in S_{\psi_t}$ such that $P\notin G_{\psi_t}$, then it is easy to notice that $\mathrm{tr}(Pg\psi_t)=\pm\,\mathrm{tr}(P\psi_t)$, and so $Pg\in S_{\psi_t}\,\forall g\in G_{\psi_t}$. To prove disjointedness let us consider two Pauli operators $P_1,P_2\in S_{\psi_t}$ such that $P_1,P_2\notin G_{\psi_t}$, then if $P_1G_{\psi_t}\cap P_2G_{\psi_t}\neq0$ would imply that $\exists g_1,g_2\in G_{\psi_t}$ such that $P_1g_1=P_2g_2$. However, we would get that $P_1\in P_2G_{\psi_t}$, thanks to the group property of G_{ψ_t}, and thus $P_1G_{\psi_t}\equiv P_2G_{\psi_t}$.

C.2 Failure probability

Let us discuss the failure probability to sample a Pauli operator P belonging to G_{ψ_t}. The event that has to be analyzed is the case where, sampled a Pauli $P \notin G$ after a set of measurements M we are unable to distinguish it from a $P \in G_{\psi_t}$. Consequently, the failure probability is given by the joint probability that a measurement yields 1 M times and $P \notin G_{\psi_t}$. The probability that $P \notin G_{\psi_t}$ is given by $1 - 2^{-t}$, and denoting p as the probability of obtaining 1 ($p = \frac{1}{2}(\mathrm{tr}(h\psi_t) + 1)$, where h represents one bad generator), the failure probability is bounded by $(1 - 2^{-t})(h_{\max}/2 + 1/2)^M$.

C.3 *Proof of Eq.* (8)

Given the probability π_l defined in Eq. (7), let us write explicitly the unity purity of the state ψ_t. From Eq. (3), we obtain

$$1 = \frac{|G_{\psi_t}|}{d}\left(1 + \sum_{i=1}^{l} \mathrm{tr}^2(h_i\psi_t) + \sum_{i=l+1}^{k} \mathrm{tr}^2(h_i\psi_t)\right) \tag{23}$$

Therefore, one can express π_l as

$$\pi_l = \frac{|G_{\psi_t}|}{d} \sum_{i=l+1}^{k} \mathrm{tr}^2(h_i\psi_t) \geq \frac{|G_{\psi_t}|}{d}(k-l)h_{\min}^2 \tag{24}$$

which concludes the proof.

C.4 Finite resolution

In this section, we present the proof of the finite resolution of the expectation values of Pauli operators for a t-doped stabilizer state. We will proceed as follows: we first bound $\min_{P\in S_{\psi_t}} |\mathrm{tr}(P\psi_t)|$ and then we bound the gap δ_t, as the second will be just a trivial generalization of the first one. We will indeed find that

$$\min_{P\in S_{\psi_t}} |\mathrm{tr}(P\psi_t)| \geq \frac{1}{3\sqrt{2}^{t-1}}\left(1 - \frac{1}{\sqrt{2}}\right)^t \tag{25}$$

while

$$\delta_t \geq \frac{1}{6\sqrt{2}^{t-1}}\left(1 - \frac{1}{\sqrt{2}}\right)^t \tag{26}$$

Since a t-doped stabilizer state is built out from a t-doped Clifford circuit, we can alternatively bound $\min_P |\mathrm{tr}(C_t P C_t^\dagger \sigma)|$ for σ being an arbitrary stabilizer state. Let us look at the action of C_t on a Pauli operator. First decompose $C_t = \prod_{i=1}^{t} C_1^{(i)}$ where $C_1^{(i)}$ is a $(t=1)$-doped Clifford circuit. Let us set up the following notation.

$$C_1^{(1)} P C_1^{(1)\dagger} = x_{(0)}P_{(0)} + \frac{x_{(1)}}{\sqrt{2}}P_{(1)} + \frac{x_{(2)}}{\sqrt{2}}P_{(2)} \tag{27}$$

where $x_{(0)}, x_{(1)}, x_{(2)} \in \{-1, 0, +1\}$. Eq. (27) must be understood as: there is a choice of $x_{(0)}, x_{(1)}, x_{(2)}$ and the respective Pauli operators $P_{(0)}, P_{(1)}, P_{(2)}$ such that the l.h.s. is equal to the r.h.s. of Eq. (27). Before generalizing to the generic t, it is useful to act again on $C_1^{(1)} P C_1^{(1)\dagger}$ with $C_1^{(2)}$.

$$\begin{aligned} C_1^{(2)} C_1^{(1)} P C_1^{(1)\dagger} C_1^{(2)\dagger} &= x_{(00)}P_{(00)} + \frac{1}{\sqrt{2}}(x_{(10)}P_{(10)} + x_{(01)}P_{(01)} + x_{(20)}P_{(20)} + x_{(02)}P_{(02)}) \\ &+ \frac{1}{2}(x_{(11)}P_{(11)} + x_{(12)}P_{(12)} + x_{(21)}P_{(21)} + x_{(22)}P_{(22)}) \end{aligned} \tag{28}$$

where each variable $x_{(ij)}$ for $i = 0, 1, 2$ can take values in $x_{(ij)} \in \{-1, 0, +1\}$. As one can see, the subscript string (ij) attached to each variable $x_{(ij)}$ reveals how many times a T-gate splits the Pauli operator P in 2 Pauli operator with the corresponding $\frac{1}{\sqrt{2}}$ factor. Again, Eq. (28) must be understood as there exists a choice of the variables $x_{(ij)}$ and the respective Pauli operators $P_{(ij)}$ for which the l.h.s.

and the r.h.s. of Eq. (28) agrees. Now, that we set up the above general and powerful notation, we can easily generalize the action to C_t. We have the following

$$C_t P C_t^\dagger = \sum_{k=0}^{t} \sum_{\pi \in S_k} \frac{x_{\pi(\boldsymbol{y}_k)}}{\sqrt{2}^k} P_{\pi(\boldsymbol{y}_k)} \,. \tag{29}$$

In Eq. (29) above, we have defined a few elements. First of all, we defined the t-long string $\boldsymbol{y}_k$ with Hamming weight k as

$$\boldsymbol{y}_k = (\underbrace{1, 1, \ldots, 1}_{k}, 0, \ldots, 0) \tag{30}$$

Next, we defined a set S_k of operations π that act on $\boldsymbol{y}_k$. Sk is the set containing all the permutations of the k 1s in $\boldsymbol{y}_k$ into t spots, combined with the operation that transforms $1 \leftrightarrow 2$, in accordance with Eq. (28). Let's illustrate this with an example. Set $t = 2$ and $k = 1$, so $\boldsymbol{y}_1 = (10)$. All the possible permutations of (10), combined with the operation $1 \leftrightarrow 2$, result in the strings $(10), (01), (20), (02)$. Similarly, for $t = 2$ and $k = 2$, $\boldsymbol{y}_2 = (11)$ and the set of operations in S_2 returns $(11), (22), (21), (12)$.

It is useful to count the number of operations within S_k for fixed k. The set S_k is the combination of $\binom{t}{k}$ many ways to permute $\boldsymbol{y}_k = (1, 1, \ldots, 1, 0, \ldots, 0)$ times the 2^k different choices of either 1 or 2 at any site. The above simple counting thus returns:

$$\sum_{\pi \in S_k} = 2^k \binom{t}{k} \tag{31}$$

From Eq. (29), we can formally compute the expectation value of $C_t P C_t^\dagger$ with a generic stabilizer state σ and get

$$\mathrm{tr}(C_t P C_t^\dagger \sigma) = \sum_{k=0}^{t} \sum_{\pi \in S_k} \frac{\tilde{x}_{\pi(\boldsymbol{y}_k)}}{\sqrt{2}^k} \tag{32}$$

where we defined the variables $\tilde{x}_{\pi(\boldsymbol{y}_k)} := x_{\pi(\boldsymbol{y}_k)} \,\mathrm{tr}(P_{\pi(\boldsymbol{y}_k)}\sigma) \in \{-1, 0, +1\}$ because $\mathrm{tr}(P_{\pi(\boldsymbol{y}_k)}\sigma) \in \{-1, 0, +1\}$. Now, we set up all the necessary notation to prove Eq. (25).

We are interested in computing the minimum achievable value for $\mathrm{tr}(C_t P C_t^\dagger \sigma)$. Let us first multiply both sides for $\sqrt{2}^t$. We thus get

$$\sqrt{2}^t \,\mathrm{tr}(C_t P C_t^\dagger \sigma) = \sum_{k=0}^{t} \sum_{\pi \in S_k} \sqrt{2}^{t-k} \tilde{x}_{\pi(\boldsymbol{y}_k)} = \sum_{l=0}^{t} \sum_{\pi \in S_{t-l}} \sqrt{2}^{l} \tilde{x}_{\pi(\boldsymbol{y}_{t-l})}$$

where in the second equality, we defined $l = t - k$. Let us set t to be even and split odd and even terms in the sum

$$\sum_{l=0}^{t} \sum_{\pi \in S_{t-l}} \sqrt{2}^{l} \tilde{x}_{\pi(\boldsymbol{y}_{t-l})} = \sum_{l=0}^{t/2} 2^l \sum_{\pi \in S_{t-2l}} \tilde{x}_{\pi(\boldsymbol{y}_{t-2l})} + \sqrt{2} \sum_{l=0}^{t/2-1} 2^l \sum_{\pi \in S_{t-(2l+1)}} \tilde{x}_{\pi(\boldsymbol{y}_{t-(2l+1)})}$$

Define the following function of t

$$A(t) := \sum_{l=0}^{t/2} 2^l \sum_{\pi \in S_{t-2l}} \tilde{x}_{\pi(\boldsymbol{y}_{t-2l})} \tag{33}$$

$$B(t) := \sum_{l=0}^{t/2-1} 2^l \sum_{\pi \in S_{t-(2l+1)}} \tilde{x}_{\pi(\boldsymbol{y}_{t-(2l+1)})} \tag{34}$$

Note that $A(t), B(t) \in \mathbb{Z}$, i.e. they are positive and negative natural numbers, for any $t = 2t'$ for $t \in \mathbb{N}$. We can thus write

$$\sqrt{2}^t |\,\mathrm{tr}(C_t P C_t^\dagger \sigma)| = |A(t) + \sqrt{2} B(t)| = |B(t)| \left| \sqrt{2} + \frac{A(t)}{B(t)} \right| \tag{35}$$

Therefore, the lower bound deals with the approximation of the algebraic number $\sqrt{2}$ by a rational number $A(t)/B(t)$. To make it explicit we can lower bound the r.h.s. of Eq. (35) as

$$\sqrt{2}^t |\operatorname{tr}(C_t P C_t^\dagger \sigma)| \geq |B(t)| \left| \sqrt{2} - \frac{|A(t)|}{|B(t)|} \right| \tag{36}$$

and we can invoke the Liouville Theorem (see Ref. [30]) of approximating a algebraic number α with two rational numbers $p, q \in \mathbb{Q}$ that reads: there exist a constant $c(\alpha)$ independent from p, q such that

$$\left| \sqrt{2} - \frac{p}{q} \right| \geq \frac{c(\alpha)}{q^D} \tag{37}$$

where D is the degree of the algebraic number α. In the case of $\alpha = \sqrt{2}$ we have $D = 2$ because $\sqrt{2}$ corresponds to the solution to the irreducible polynomial $z^2 - 2 = 0$ which has degree 2, and $c(\sqrt{2}) = \frac{1}{6}$ [30]. Applying Eq. (37) to Eq. (36), we thus get

$$|\operatorname{tr}(C_t P C_t^\dagger \sigma)| \geq \frac{1}{6|B(t)|\sqrt{2}^t} \tag{38}$$

We are left to find an upper bound to $B(t)$. We proceed with the following equality

$$\begin{aligned} |B(t)| &= \left| \sum_{l=0}^{t/2-1} 2^l \sum_{\pi \in S_{t-(2l+1)}} \tilde{x}_{\pi(\boldsymbol{y}_{t-(2l+1)})} \right| \leq \sum_{l=0}^{t/2-1} 2^l \sum_{\pi \in S_{t-(2l+1)}} |\tilde{x}_{\pi(\boldsymbol{y}_{t-(2l+1)})}| \\ &= \sum_{l=0}^{t/2-1} 2^l \sum_{\pi \in S_{t-(2l+1)}} = \sum_{l=0}^{t/2-1} 2^l 2^{t-(2l+1)} \binom{t}{2l+1} \\ &= \frac{1}{\sqrt{8}} 2^t \left[\left(1 + \frac{1}{\sqrt{2}}\right)^t - \left(1 - \frac{1}{\sqrt{2}}\right)^t \right] \leq \frac{1}{\sqrt{8}} \left(1 - \frac{1}{\sqrt{2}}\right)^{-t} \end{aligned} \tag{39}$$

where in the second equality, we used the fact that $\tilde{x}_{\pi(\boldsymbol{y}_{t-(2l+1)})} \in \{-1, 0, +1\}$ and in the last inequality, we used the fact that

$$\frac{1}{\sqrt{8}} 2^t \left[\left(1 + \frac{1}{\sqrt{2}}\right)^t - \left(1 - \frac{1}{\sqrt{2}}\right)^t \right] \leq \frac{1}{\sqrt{8}} 2^t \left(1 + \frac{1}{\sqrt{2}}\right)^t = \frac{1}{\sqrt{8}} \left(1 - \frac{1}{\sqrt{2}}\right)^{-t} \tag{40}$$

An analogous procedure with $t = 2t' + 1$ with t' leads to the same exact bound. Therefore for any $t \in \mathbb{N}$, we find

$$|\operatorname{tr}(C_t P C_t^\dagger \sigma)| \geq \frac{\sqrt{8}}{6} \left(\frac{1}{\sqrt{2}} - \frac{1}{2}\right)^t \tag{41}$$

Now, let us turn to analyze the gap $\delta_t \equiv \operatorname{tr}[(P - P')\psi_t]$. Using the same notation as before, we can write the adjoint action of C_t on $P - P'$ as follows

$$C_t (P - P') C_t^\dagger = \sum_{k=0}^{t} \sum_{\pi \in S_k} \left(\frac{x_{\pi(\boldsymbol{y}_k)}}{\sqrt{2}^k} P_{\pi(\boldsymbol{y}_k)} + \frac{x'_{\pi(\boldsymbol{y}_k)}}{\sqrt{2}^k} P'_{\pi(\boldsymbol{y}_k)} \right) \tag{42}$$

and therefore, by repeating the same procedure, we can define

$$A'(t) := \sum_{l=0}^{t/2} 2^l \sum_{\pi \in S_{t-2l}} \tilde{x}_{\pi(\boldsymbol{y}_{t-2l})} + \tilde{x}'_{\pi(\boldsymbol{y}_{t-2l})} \tag{43}$$

$$B'(t) := \sum_{l=0}^{t/2-1} 2^l \sum_{\pi \in S_{t-(2l+1)}} \tilde{x}_{\pi(\boldsymbol{y}_{t-(2l+1)})} + \tilde{x}'_{\pi(\boldsymbol{y}_{t-(2l+1)})} \tag{44}$$

and write the gap as

$$\delta_t = \frac{1}{\sqrt{2}^t} |A'(t) + \sqrt{2} B'(t)| \geq \frac{|B'(t)|}{\sqrt{2}^t} \left| \sqrt{2} - \frac{|A'(t)|}{|B'(t)|} \right| \geq \frac{1}{6\sqrt{2}^t |B'(t)|} \tag{45}$$

Following the inequalities in Eq. (39), one can find

$$|B'(t)| \leq \frac{1}{\sqrt{2}} \left(1 - \frac{1}{\sqrt{2}}\right)^{-t} \tag{46}$$

which recovers the desired result in Eq. (26)

$$\delta_t \geq \frac{\sqrt{2}}{6} \left(\frac{1}{\sqrt{2}} - \frac{1}{2}\right)^{t} \tag{47}$$

D Sampling the stabilizer group from Bell measurements

Lemma 1. *Given a quantum state $|\omega\rangle$ on q-qubits, there exist a Pauli operator $\bar{P}$ such that $|\langle\omega|\bar{P}|\omega^*\rangle| \geq 2^{-q}$.*

Proof. To show this, let us assume the contrapositive, i.e. $\forall P \in \mathbb{P}_q$ then $|\langle\omega|P|\omega^*\rangle| < 2^{-q}$. First of all, notice that it always holds

$$\sum_{P\in\mathbb{P}_q} |\langle\omega|P|\omega^*\rangle|^2 = \sum_{P\in\mathbb{P}_q} \mathrm{tr}(\omega P \omega^* P) = 2^q \tag{48}$$

However, sticking to the hypothesis, if we sum up the squares we get

$$\sum_{P\in\mathbb{P}_q} |\langle\omega|P|\omega^*\rangle|^2 < 2^{-q} \sum_{P\in\mathbb{P}_q} < 2^q \tag{49}$$

and this is a contradiction. □

In this section, we shall show that given $P, P' \sim \widetilde{\Xi}_{\psi_t}$ drawn from $\widetilde{\Xi}_{\psi_t}$, then their product PP' belongs to the stabilizer group G_{ψ_t} with probability greater than 2^{-6t}. Formally

$$\Pr_{P,P'\sim\widetilde{\Xi}_{\psi_t}} (PP' \in G_{\psi_t}) \geq \frac{1}{2^{6t}} \tag{50}$$

First of all, let us refresh some basis about stabilizer states. Consider a stabilizer state $|\sigma\rangle$ and its conjugate state in the computational basis $|\sigma^*\rangle$. In Ref. [10], it has been shown that there exist a Pauli operator P_σ such that

$$P_\sigma |\sigma\rangle = |\sigma^*\rangle \tag{51}$$

which can be understood at the level of the stabilizer group in the following way. Let $G_\sigma = \langle g_1, \ldots, g_n\rangle$ the stabilizer group of $|\sigma\rangle$. The stabilizer group of $|\sigma^*\rangle$ is, of course, given by $G_{\sigma^*} = \langle g_1^*, \ldots, g_n^*\rangle$. Therefore, thanks to Eq. (51), there exist P_σ such that

$$P_\sigma g_i P_\sigma = g_i^*, \quad \forall g_i \in G_\sigma \tag{52}$$

Consider now the projector $\Pi_{\psi_t} := \prod_{i=1}^m \frac{\mathbb{1}+\phi_{g_j} g_j}{2}$ onto the stabilizer group G_{ψ_t}. Since G_{ψ_t} can be completed to a maximal stabilizer group $\widetilde{G_{\psi_t}}$, i.e. $|\widetilde{G_{\psi_t}}| = d$, there exists P_{ψ_t} such that

$$P_{\psi_t} \Pi_{\psi_t} P_{\psi_t} = \Pi_{\psi_t}^* \tag{53}$$

where $\Pi_{\psi_t}^* = \prod_{i=1}^m \left(\frac{\mathbb{1}+\phi_{g_j} g_j^*}{2}\right)$. On the state vector level, the action of P_{ψ_t} on $|\psi_t^*\rangle$ results in $|\psi_t^{*\prime}\rangle = P_{\psi_t} |\psi_t^*\rangle$ with a density matrix representation equal to

$$|\psi_t^{*\prime}\rangle\langle\psi_t^{*\prime}| = \left(\frac{1}{2^t} \sum_{i=0}^{k} \mathrm{tr}(h_i \psi_t^*) h_i\right) \Pi_{\psi_t} \tag{54}$$

i.e. having the same projector Π_{ψ_t} of $|\psi_t\rangle$. To demonstrate the validity of Eq. (54), is sufficient to compute the overlap $\mathrm{tr}(\Pi_{\psi_t} P_{\psi_t} \psi_t^* P_{\psi_t}) = 1$. Thanks to Eq. (54), given $\mathcal{D}_{\psi_t}$ being the diagonalizer associated to $|\psi_t\rangle$, one has that

$$\mathcal{D}_{\psi_t} |\psi_t^{*\prime}\rangle = |0\rangle^{\otimes m} \otimes |\phi^*\rangle \tag{55}$$

The last step before proving the statement comes from the result of Lemma 1 that ensures the existence of a Pauli operator $\bar{P}$ such that $|\langle\phi|\bar{P}|\phi^*\rangle| \geq 2^{-(n-m)}$. Therefore, let us prove the statement, i.e. that the probability that Bell measurements sample a Pauli P such that $PP_{\psi_t}\mathcal{D}^\dagger\bar{P}\mathcal{D} \in G_{\psi_t}$ is greater than $d^{-1}8^{-t}$. Starting Eq. (10), we have

$$\begin{aligned} |\langle\psi_t|P|\psi_t^*\rangle| &= |\langle\psi_t|PP_{\psi_t}|\psi_t^{*\prime}\rangle| \\ &= |\langle 0^m\otimes\phi|\mathcal{D}PP_{\psi_t}\mathcal{D}^\dagger|0^m\otimes\phi^*\rangle| \\ &= |\langle 0^m\otimes\phi|\mathcal{D}PP_{\psi_t}\mathcal{D}^\dagger\bar{P}\bar{P}|0^m\otimes\phi^*\rangle| \end{aligned}$$

Let us impose $PP_{\psi_t}\mathcal{D}^\dagger\bar{P}\mathcal{D} \in G_{\psi_t}$; therefore, we have the following bound:

$$\begin{aligned} |\langle\psi_t|P|\psi_t^*\rangle| &= |\langle 0^m\otimes\phi|\bar{P}|0^m\otimes\phi^*\rangle| \\ &= |\langle\phi|\bar{P}|\phi^*\rangle| \geq 2^{-(n-m)} \end{aligned} \tag{56}$$

And therefore, we can formally write

$$\Pr(PP_{\psi_t}\mathcal{D}^\dagger\bar{P}\mathcal{D} \in G_{\psi_t}) \geq \frac{|G_{\psi_t}|}{d}\frac{1}{2^{2(n-m)}} \geq \frac{1}{8^t} \tag{57}$$

For fixed P_{ψ_t} and $\bar{P}$, one has that the probability that two samples Pauli operators P, P' obeys the property in Eq. (57) is $\frac{1}{2^{6t}}$, and one has that the probability that the product $PP' \in G_{\psi_t}$ is, by a simple shift for $P_{\psi_t}\mathcal{D}^\dagger\bar{P}\mathcal{D}$, is the one in Eq. (50).