Robustness of Magic and Symmetries of the Stabiliser Polytope

Markus Heinrich and David Gross

Institute for Theoretical Physics, University of Cologne, 50937 Cologne, Germany

April 5, 2019

We give a new algorithm for computing the *robustness of magic*—a measure of the utility of quantum states as a computational resource. Our work is motivated by the *magic state model* of fault-tolerant quantum computation. In this model, all unitaries belong to the Clifford group. Non-Clifford operations are effected by injecting non-stabiliser states, which are referred to as *magic states* in this context. The *robustness of magic* measures the complexity of simulating such a circuit using a classical Monte Carlo algorithm. It is closely related to the degree negativity that slows down Monte Carlo simulations through the infamous *sign problem*. Surprisingly, the robustness of magic is *submultiplicative*. This implies that the classical simulation overhead scales subexponentially with the number of injected magic states—better than a naive analysis would suggest. However, determining the robustness of n copies of a magic state is difficult, as its definition involves a convex optimisation problem in a 4^n -dimensional space. In this paper, we make use of inherent symmetries to reduce the problem to n dimensions. The total run-time of our algorithm, while still exponential in n , is super-polynomially faster than previously published methods. We provide a computer implementation and give the robustness of up to 10 copies of the most commonly used magic states. Guided by the exact results, we find a finite hierarchy of approximate solutions where each level can be evaluated in polynomial time and yields rigorous upper bounds to the robustness. Technically, we use symmetries of the stabiliser polytope to connect the robustness of magic to the geometry of a low-dimensional convex polytope generated by certain *signed quantum weight enumerators*. As a by-product, we characterised the automorphism group of the stabiliser polytope, and, more generally, of projections onto complex projective 3-designs.

1 Introduction

In fault-tolerant quantum computation (for a recent review, see Ref. [8]), each logical qubit is encoded in a non-local subspace of a number of physical qubits. There are several ways of effecting a unitary transformation of logical qubits. In the simplest case, logical unitaries can be implemented *transversally*, i.e. by local gates acting on the physical qubits. Unfortunately, a no-go theorem by Eastin and Knill [13] states that there are no quantum codes that allow for a *universal* set of transversal gates.

In the *magic state model* [5], the logical gate set is chosen to be the Clifford group, which can be implemented transversally in various quantum codes using their physical counterparts. Any logical non-Clifford gate would promote the Clifford group to universality. This remaining problem is solved by providing an auxiliary qubit in a non-stabiliser state. Using a circuit gadget (which only requires Clifford operations), one can turn this auxiliary state into a non-Clifford gate (Fig. 1). The auxiliary qubit state is consumed in the process, so that one such input needs to be injected for each non-Clifford gate. These inputs are the *magic states* from which the protocol derives its name.

Markus Heinrich: markus.heinrich@uni-koeln.de

Figure 1: Use of magic state injection to perform a T gate on some input state $|\psi\rangle$. The state injection circuit can be rewritten as a swap circuit followed by T gate.

Figure 2: Magic state distillation turns a supply of mixed states ρ into a pure magic state, e.g. $|H\rangle$ using only Clifford operations.

A common choice for a non-Clifford gate is the T -gate $T = \text{diag}(1, e^{i\pi/4})$, which is realised by the following magic state

$$|H\rangle := T|+\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + e^{i\pi/4} |1\rangle \right). \quad (1)$$

Moreover, there is a second magic state, $|T\rangle$, which realises the non-Clifford gate $\text{diag}(1, e^{i\pi/6})$. Their Bloch representation is shown in Fig. 5. Interestingly, it has been found that even certain mixed states can “supply the magic” to promote a Clifford circuit to universality. Indeed, a process called *magic state distillation* (Fig. 2) can turn many copies of some mixed state ρ into a pure magic state using Clifford unitaries and computational basis measurements [5, 34].

Magic state distillation motivates the search for quantitative measures of the “computational utility” of auxiliary states. This analysis turns out to be slightly simpler for quantum systems with odd-dimensional Hilbert spaces [27, 36, 37], as the theory of stabiliser states is somewhat better-behaved in this case, and there is a better-developed toolbox of “phase space methods” available in this case (see e.g. Refs. [15, 24, 42]). However, as qubits are the paradigmatic systems for quantum computation, quantitative resource theories for multi-qubit magic states have since been developed [6, 23].

The starting point of these theories is the Gottesman-Knill Theorem [30]. It states that quantum circuits consisting only of preparations of stabiliser states, Clifford unitaries, and computational basis measurements can be efficiently simulated on a classical computer. Therefore, if the auxiliary states are stabilisers, there can be no quantum computational advantage. Next, assume that an auxiliary n -qubit state ρ is an element of the *stabiliser polytope* SP_n , i.e.

$$\rho = \sum_i p_i s_i,$$

where $(p_i)_i$ is a probability distribution and the $s_i = |\psi_i\rangle\langle\psi_i|$ are stabiliser states. This readily gives rise to an efficient classical randomised algorithm that will draw outcomes from the same distribution as a quantum computer would [39], provided that one can sample efficiently from the probability distribution $(p_i)_i$: Indeed, draw s_i with probability p_i , and then continue to simulate the further time evolution using Gottesman-Knill. Thus, density matrices contained in the convex hull of stabiliser states are equally useless as computational resource states in the magic state model (Fig. 3).

Figure 3: Bloch representation of the two most commonly considered magic states $|H\rangle$ and $|T\rangle$. These states lie outside of the octahedron spanned by 1-qubit stabiliser states having a Bloch vector orthogonal to an edge ($|H\rangle$) or a facet ($|T\rangle$) of the stabiliser octahedron. The intersection of their Bloch vector with the facet or edge is marked with a blue dot. Certain mixed states can be used to distil these pure states using Clifford unitaries and measurements. However, states lying inside the stabiliser polytope are useless as a resource state.

Since the stabiliser states $\{s_i\}_i$ span the space of Hermitian operators, any auxiliary state can be expanded as $\rho = \sum_i x_i s_i$, with coefficients x_i that are not necessarily non-negative. However, taking traces on both sides shows that the expansion is *affine*, i.e. $\sum_i x_i = 1$. It is well-known in the theory of Quantum Monte Carlo methods [17] that the probabilistic algorithm sketched above can be extended to the more general scenario. However, the runtime will increase with the total amount of “negativity” in the expansion coefficients x_i . This is the dreaded *sign problem*. A precise theory of the simulation runtime in the context of quantum computation has been developed in Ref. [31] and applied to the magic state model in Ref. [23]. More precisely, they define the *robustness of magic* (RoM) as

$$\mathcal{R}(\rho) := \min \left\{ \|x\|_1 \mid x \in \mathbb{R}^N : \rho = \sum_{i=1}^N x_i s_i \right\}, \quad (2)$$

where the sum ranges over stabiliser states $\{s_1, \dots, s_N\}$ and the ℓ_1 -norm

$$\|x\|_1 = \sum_{i=1}^N |x_i| = 1 + 2 \sum_{i: x_i \leq 0} |x_i|$$

measures the “amount of negativity” in the affine combination. Then, the number of samples which have to be taken in the Monte Carlo simulation scales as $O(\mathcal{R}(\rho)^2)$ [23, 31].

In addition to measuring the “computational utility” in the above precise sense, the RoM has further interpretations. For example, it can be used to systematically lower-bound the number of non-Clifford gates required to synthesise certain unitaries, namely those that allow for a magic state realisation [23]. Lastly, the RoM derives its name from the fact that it quantifies the robustness of a state’s computational utility against noise processes. A precise account of this point of view is given in Section 2.

Interestingly, the RoM is *submultiplicative*, i.e. $\mathcal{R}(\rho^{\otimes 2}) \leq \mathcal{R}(\rho)^2$, where the inequality is usually strict [23]. That means that the simulation effort of a magic state circuit grows subexponentially with the number of injected magic states—an intriguing phenomenon. Therefore, a quantity of interest is the *regularised RoM*:

$$\mathcal{R}_{\text{reg}}(\rho) := \lim_{n \rightarrow \infty} \mathcal{R}(\rho^{\otimes n})^{1/n}.$$

Unfortunately, computing $\mathcal{R}(\rho^{\otimes n})$ seems to be a difficult task. For ρ being a single-qubit state, the tensor power $\rho^{\otimes n}$ lives in an 4^n -dimensional space, and the sum over the s_i in the definition (2) of the RoM has to range over the $2^{O(n^2)}$ stabiliser states defined for n -qubit systems. Any direct implementation of the optimisation problem (2) will thus quickly become computationally intractable—and, indeed, Howard and Campbell [23] could carry it out only up to $n = 5$.

The starting point of this work is the observation that there is a large symmetry group shared by $\rho^{\otimes n}$ and the stabiliser polytope. Thus, we formulate the optimisation

Figure 4: Projected n -qubit stabiliser polytopes with respect to the symmetry group of the magic state $|H\rangle^{\otimes n}$ and $n = 2, 3$. We use a Bloch-like representation in the basis constructed in Sec. 3.3. The origin O corresponds to the maximally mixed state $\mathbb{1}/2^n$ and lies inside the polytope. The complexity of the polytopes is significantly reduced compared to the full 15-dimensional (respectively 63-dimensional) stabiliser polytopes. Visual inspection suggests that no joint symmetries of $|H\rangle^{\otimes n}$ and the projected polytope remain.

in a space where the joint symmetries have been “modded out”. The space of operators invariant under the joint symmetry group turns out to have a dimension mildly polynomial in n . For the especially interesting cases where the state is $|H\rangle^{\otimes n}$ or $|T\rangle^{\otimes n}$, the dimension reduces further to exactly n . While the projection of the stabiliser polytope to this invariant space (Fig. 4) still has exponentially many vertices, it turns out that formulating the optimisation problem in this symmetry-reduced way leads to a super-polynomially faster algorithm.

Equipped with the knowledge of the exact solution to Eq. (2) for the commonly used magic states $|H\rangle^{\otimes n}$ and $|T\rangle^{\otimes n}$ and $n \leq 10$ qubits, we formulate a relaxation of the RoM problem for these states which yields an upper bound for the exact RoM. These approximations are in excellent agreement with the exact data for $n \leq 10$ and can be carried out for up to 26 qubits. What is more, we can not only compute the RoM bounds for these approximations, but also find the corresponding affine decompositions $\rho^{\otimes n} = \sum_i x_i s_i$, which can directly be used in Monte Carlo simulations. Furthermore, we find a hierarchy of such RoM approximations by restricting to k -partite entangled stabiliser states which converges to the exact RoM. Interestingly, every level of the hierarchy can be computed in polynomial time.

Finally, both the exact and approximate results imply a runtime of $O(2^{0.737t})$ for simulating a circuit with t T gates using the RoM algorithm. Moreover, our analysis suggests that this runtime is the optimal one that can be achieved using a RoM algorithm. Our work improves on the previously known runtime of $O(2^{0.753t})$ derived in Ref. [23]. Note that the RoM algorithm is able to simulate noisy circuits and mixed states. This is in contrast to simulation algorithms based on the so-called *stabiliser rank* which can achieve a runtime of $O(2^{0.48t})$ for pure states [4, 6, 7].

This paper is organised as follows. Section 2 is devoted to a short discussion of the Robustness of Magic, giving an alternative definition to the one in the previous section and stating the properties of this resource monotone. Next, a series of techniques is presented which use the symmetries in the definition of the monotone to simplify the computation significantly. To this end, the symmetry group of the stabiliser polytope is characterised in Sec. 3.2 and certain classes of states are singled out in Sec. 3.3 which profit from a high degree of symmetry. For these states, we explicitly derive the symmetry-reduced problem by constructing a suitable basis for the invariant subspace in Sec. 3.3, followed by enumerating equivalence classes of stabiliser states up to symmetry in Sec. 3.4. The numerical solutions for the constructed problems are presented and discussed in Section 4. Based on this, we prove a polytime relaxation of the RoM problem in Sec. 4.3. Our results are summarised in Sec. 5.

2 Robustness of Magic

The resource theory of magic states can be developed in analogy to the more-established resource theory of entanglement and the *robustness of entanglement* [38] studied in this context. There, the robustness of a state can be interpreted as a measure for the worst-case separable noise that renders the state separable. However, its construction can be generalised to any resource theory as follows: Given a convex set S of free resources, the robustness of a relative to $b \in S$ is defined as

$$R(a||b) := \inf \left\{ s \geq 0 \mid \frac{1}{1+s} (a + sb) \in S \right\}. \quad (3)$$

Depending on the choice of b , the robustness might be infinite. If it is finite, we can express a as a pseudo-mixture

$$a = (1+s)b^+ - sb^-, \quad \text{with } b^\pm \in S. \quad (4)$$

Following Vidal and Tarrach [38], one can define the so-called *total robustness* by minimising over the set of free resources:

$$R(a) := \inf_{b \in S} R(a||b). \quad (5)$$

In the following, we choose $S = \text{SP}_n$ to be the convex polytope spanned by the n -qubit stabiliser states. More precisely, $\text{SP}_n = \text{conv stab}(n)$, where $\text{stab}(n) = \{s_1, \dots, s_N\}$ is the set of all n -qubit stabiliser states. Here, and in the following, by a “quantum state”, we will always mean the density matrix representing it. In the case of pure states $s_i = |\psi_i\rangle\langle\psi_i|$, the associated vector $|\psi_i\rangle$ will be referred to as a *state vector*. The polytope SP_n is a subset of the real vector space of $(D \times D)$ -dimensional Hermitian matrices H_D where $D = 2^n$ is the overall dimension of Hilbert space. More specifically, quantum states lie in the $(D^2 - 1)$ -dimensional affine subspace given by $\text{tr } \rho = 1$. Within this affine hyperplane, SP_n is full-dimensional and we usually consider it as the ambient space of SP_n .

Howard and Campbell [23] work with an equivalent robustness measure: the *robustness of magic* (RoM) introduced in Eq. (2). A straightforward calculation (c.f. Appendix A) shows that the two measures are related by a simple affine transformation:

$$\mathcal{R}(\rho) = 1 + 2R(\rho). \quad (6)$$

The robustness of magic provides a proper resource monotone with the following properties:

Proposition 1 (Properties of Robustness of Magic [23]). *The robustness of magic has the following properties:*

1. Faithfulness: $\mathcal{R}(\rho) = 1$ iff $\rho \in \text{SP}_n$
2. Monotonicity: $\mathcal{R}(\mathcal{X}(\rho)) \leq \mathcal{R}(\rho)$ for all stabiliser operations $\mathcal{X}$ with equality if $\mathcal{X}$ is unitary.
3. Convexity: $\mathcal{R}((1-t)\rho + t\sigma) \leq (1-t)\mathcal{R}(\rho) + t\mathcal{R}(\sigma)$ for $0 \leq t \leq 1$.
4. Submultiplicativity: $\mathcal{R}(\rho \otimes \sigma) \leq \mathcal{R}(\rho)\mathcal{R}(\sigma)$.

3 Exploiting stabiliser symmetries

3.1 Definition of the RoM problem.

The Robustness of Magic is defined as the following optimisation problem.

Problem 1 (Robustness of Magic). Let $\text{stab}(n) = \{s_1, \dots, s_N\}$ be the set of stabiliser states. Given a state ρ , solve the following problem:

$$\begin{aligned} \min \quad & \|x\|_1 \quad \text{over } x \in \mathbb{R}^N \\ \text{s. t.} \quad & \rho = \sum_{i=1}^N x_i s_i. \end{aligned}$$

Using standard techniques, this problem can be reformulated as a linear program (LP) with $D^2 + 2N$ constraints and $2N$ variables [3]. Although the time complexity of LPs is linear in the product of number of constraints and variables, these numbers themselves grow super-exponentially with the number of qubits n . Concretely, $N = 2^{O(n^2)}$ and $D^2 = 4^n$. Moreover, the LP needs access to an oracle which provides the N stabiliser states. The implementation of such an oracle would necessarily have super-exponential time complexity itself. However, even if an efficient oracle were provided, the storage of the states would quickly exceed the memory capacity of any computer. In practice, this limits the evaluation of the problem to $n \leq 5$ on normal computers and renders it infeasible, even on supercomputers, for $n \geq 8$.¹

A standard method in the analysis of optimisation problems is dualising the problem. Clearly, by Slater's condition, strong duality holds and thus the dual problem is an equivalent definition for the Robustness of Magic. In Appendix B, we state the dual problem and derive a lower bound from a feasible solution. However, this bound matches the one that was already found in Ref. [23].

3.2 Symmetry reduction

The complexity of the RoM problem can be significantly reduced by exploiting the symmetries of the problem, a procedure that we will call *symmetry reduction* and is well-known in convex optimisation theory, see e.g. [2]. Here, we will explain the basic ideas and refer the interested reader to App. E for a mathematical review.

By *stabiliser symmetries* $\text{Aut}(\text{SP}_n)$, we mean the linear symmetry group of the stabiliser polytope. This is the group of linear maps $H_D \rightarrow H_D$ that leave SP_n invariant. These maps necessarily have to preserve the set of vertices, i.e. the set of stabiliser states $\text{stab}(n)$. Clearly, the group of n -qubit Clifford unitaries $\mathcal{C}_n$ induces such symmetry transformations by conjugation. Another obvious symmetry of the set of stabilisers is the *transposition*:

$$s_i = |\psi_i\rangle \langle \psi_i| \mapsto s_i^T = \mathcal{C} |\psi_i\rangle \langle \psi_i| \mathcal{C},$$

where $\mathcal{C}$ is the (anti-unitary) operation of complex conjugation in the computational basis. The group of unitary and anti-unitary operations generated by Clifford unitaries and complex conjugation is known as the *extended Clifford group* EC_n [1]. Our first result states that any stabiliser symmetry is induced by the action of an element of the extended Clifford group on the Hilbert space. This is a corollary of the more general Thm. 1 on symmetries of 3-designs and is proven in App. C.

Corollary 1. *The group of stabiliser symmetries $\text{Aut}(\text{SP}_n)$ is given by the adjoint representation of the extended Clifford group EC_n .*

We emphasise that this is a non-trivial result which is in general wrong for the case of odd-dimensional qudits where it is possible to construct explicit counter-examples. This turns out to be related to the fact that stabiliser states fail to form 3-designs in odd dimensions [25, 40, 41].

Note that anti-unitary symmetries in EC_n act in the adjoint representation as $\text{Ad}(C) \circ T$, where $C \in \mathcal{C}_n$ and T is the transposition map. Hence, there are only *global* antiunitary symmetries. Every tensor product of local antiunitary symmetries

¹Already the storage of $\text{stab}(7)$ would require around 77 TiB of memory. For $n = 8$, this number increases to around 76 PiB which exceeds the state-of-the-art by a factor of 7.

would involve a partial transposition and such a map could not preserve the set of *entangled* stabiliser states.

Let $G_\rho < \text{EC}_n$ be a (not necessarily maximal) subgroup fixing ρ . The projection onto the subspace of G_ρ -fixed points $V^{G_\rho} \subset H_D$, see App. E, is given by

$$\Pi_{G_\rho}(\sigma) = \frac{1}{|G_\rho|} \sum_{U \in G_\rho} U \sigma U^\dagger. \quad (7)$$

Note that Π_{G_ρ} is trace-preserving, hence the image of quantum states will again lie in the affine subspace $\text{tr}^{-1}(\{1\}) \cap V^{G_\rho}$.

Recall that we can express the robustness of ρ as a minimisation over $t \geq 0$ and (mixed) stabiliser states $\sigma^\pm \in \text{SP}_n$ such that

$$\rho = (1+t)\sigma^+ - t\sigma^-. \quad (8)$$

Since Π_{G_ρ} preserves SP_n , every such decomposition yields a decomposition in terms of G_ρ -invariant mixed stabiliser states:

$$\rho = \Pi_{G_\rho}(\rho) = (1+t)\Pi_{G_\rho}(\sigma^+) - t\Pi_{G_\rho}(\sigma^-), \quad (9)$$

In particular, if the decomposition was optimal in the first place, the projected decomposition is also optimal.

This shows that there is always G_ρ -invariant optimal solution for the problem. Hence, instead of optimising over the whole set of stabiliser states, we only have to optimise over G_ρ -invariant mixed stabiliser states $\overline{\text{SP}}_n := \text{SP}_n \cap V^{G_\rho}$. By Lemma 3 in App. E, these are exactly given by $\overline{\text{SP}}_n = \Pi_{G_\rho}(\text{SP}_n)$ and can thus be computed by evaluating the projections $\text{stab}(n) := \Pi_{G_\rho}(\text{stab}(n))$. Since $\Pi_{G_\rho}(UsU^\dagger) = \Pi_{G_\rho}(s)$ for all $U \in G_\rho$ and $s \in \text{stab}(n)$, it is sufficient to compute the projections on representatives of $\text{stab}(n)/G_\rho$. Finally, we remark that a majority of the projected states $\text{stab}(n)$ are not extremal points of the projected polytope $\overline{\text{SP}}_n$. Given an extremal subset $\mathcal{V}_n = \{v_1, \dots, v_M\} \subset \text{stab}(n)$, the symmetry-reduced version of Prob. 1 is given by substituting $\text{stab}(n) \mapsto \mathcal{V}_n$ and $N \mapsto M$.

3.3 Identification of symmetries

The first step towards the explicit symmetry-reduced problem is to identify the group G_ρ that fixes the state ρ of interest. Motivated by magic state distillation and the submultiplicativity problem, we are especially interested in the case $\rho = |\psi\rangle\langle\psi|^{\otimes n}$ with $|\psi\rangle$ being a m -qubit state. A large part of the analysis does not depend on the choice of $|\psi\rangle$, so we keep the discussion as general as possible and specialise later to $m = 1$ and particular choices of $|\psi\rangle$. The symmetries of $|\psi\rangle^{\otimes n}$ can be classified as follows:

Permutation symmetry Clearly, $|\psi\rangle^{\otimes n}$ is invariant under permutations of the n tensor factors. Such permutations also preserve the stabiliser polytope. Thus, the symmetric group S_n is contained in the symmetry group of the problem.

Local symmetries By local symmetries of $|\psi\rangle^{\otimes n}$ we mean products of m -qubit stabiliser symmetries of $|\psi\rangle$. By Corollary 1, this class contains only local Clifford operations. Let $(\mathcal{C}_m)_\psi$ be the stabiliser of $|\psi\rangle$ within the m -qubit Clifford group $\mathcal{C}_m$, then the local symmetry group is given by $(\mathcal{C}_m)_\psi^{\otimes n}$.

Global symmetries We refer to all other symmetries as global. The global symmetry group contains e.g. the transposition $\rho \mapsto \rho^T$.

The maximal symmetry group for $\rho = |\psi\rangle\langle\psi|^{\otimes n}$ is given by the subgroup $\mathcal{C}_\rho$ that stabilises ρ within EC_n . Here, we focus on the subgroup of $\mathcal{C}_\rho$ which is given by local symmetries and permutations:

$$G_\rho := (\mathcal{C}_m)_\psi^{\otimes n} \rtimes S_n. \quad (10)$$

The following analysis suggests that for our choices of ρ , G_ρ actually coincides with $\mathcal{C}_\rho$, meaning that there are no further global symmetries. However, since the study of symmetries in EC_n can be quite involved [16], we can not exclude the possibility that we missed some of the symmetries.

For the rest of this paper, we will consider the case $m = 1$. Note that $\mathcal{C}_1$ acts by rotating about the symmetry axes of the stabiliser polytope. It is easy to see that states $|\psi\rangle$ with non-trivial stabilisers $(\mathcal{C}_1)_\psi$ fall into three classes: Stabiliser states (with trivial robustness), and magic states that lie on the Clifford orbit of $|H\rangle$ or $|T\rangle$. Since the RoM is Clifford-invariant, we can pick the following states for concreteness:

$$|H\rangle\langle H| = \frac{1}{2} \left(\mathbb{1} + \frac{1}{\sqrt{2}}(X + Y) \right), \quad |T\rangle\langle T| = \frac{1}{2} \left(\mathbb{1} + \frac{1}{\sqrt{3}}(X + Y + Z) \right). \quad (11)$$

Figure 5 shows the two states and their stabiliser symmetries. The respective unitary symmetries correspond to a two-fold rotation symmetry about the $|H\rangle$ -axis and three-fold rotation symmetry about the $|T\rangle$ -axis. In terms of Clifford operations, these stabiliser groups are represented by

$$(\mathcal{C}_1)_H = \langle SX \rangle, \quad (\mathcal{C}_1)_T = \langle SH \rangle. \quad (12)$$

Recall that these should be understood in the adjoint representation and thus the order of these groups is indeed $|(\mathcal{C}_1)_H| = 2$ and $|(\mathcal{C}_1)_T| = 3$.

Furthermore, there are antiunitary stabiliser symmetries

$$\mathcal{A}: X \mapsto X, \quad \mathcal{B}: X \mapsto Y, \quad \mathcal{C}: X \mapsto Z, \quad (13)$$

$$Y \mapsto Y, \quad Y \mapsto X, \quad Y \mapsto Y, \quad (14)$$

$$Z \mapsto -Z, \quad Z \mapsto Z, \quad Z \mapsto X, \quad (15)$$

such that $|H\rangle$ is fixed by $\mathcal{A}$ and $\mathcal{B}$ and $|T\rangle$ is fixed by $\mathcal{B}$ and $\mathcal{C}$. Recall that these can only contribute global symmetries such as $\mathcal{A}^{\otimes n}$. However, the common $+1$ eigenspace of $\mathcal{A}^{\otimes n}$ and $\mathcal{B}^{\otimes n}$ coincides with that of $SX^{\otimes n}$ and thus adding these symmetries to the symmetry group will not further reduce the invariant subspace. A similar argument holds also for the antiunitary symmetries of $|T\rangle$.

Figure 5: Stabiliser symmetries of the magic states $|H\rangle$ and $|T\rangle$ and the octahedron of stabiliser states. $|H\rangle$ is fixed by the antiunitary reflections $\mathcal{A}$, $\mathcal{B}$ and unitary π rotations around its axis. $|T\rangle$ is fixed by the antiunitary reflections $\mathcal{B}$, $\mathcal{C}$ and unitary $\pi/3$ rotations around its axis.

Hence, the considered symmetry groups are as follows:

$$G_H := \langle SX \rangle^{\otimes n} \rtimes S_n, \quad G_T := \langle SH \rangle^{\otimes n} \rtimes S_n. \quad (16)$$

Since the symmetric group S_n is always a subgroup of the symmetry group, the fixed point subspace V^{G_ρ} is always a subspace of the totally symmetric subspace $\text{Sym}(H_D)$. Let us first consider a generic state ρ with no further symmetries. Then, V^{G_ρ} coincides with $\text{Sym}(H_D)$. Thus, the trace 1 subspace has dimension $\frac{1}{6}(n+3)(n+2)(n+1) - 1$ and is thus exponentially smaller than the full space. A basis for the symmetric subspace

is given by a Fock-style “occupation number basis” constructed from the Pauli basis $\mathbb{1}, X, Y, Z$ as follows

$$N_{i,j,k} = \text{Sym} \left(X^{\otimes i} \otimes Y^{\otimes j} \otimes Z^{\otimes k} \otimes \mathbb{1}^{\otimes (n-i-j-k)} \right),$$

$$\text{for } i, j, k \in \{0, \dots, n\} \text{ such that } i + j + k \leq n. \quad (17)$$

Here, the symmetrisation operator $\text{Sym} \equiv \Pi_{S_n}$ is given by averaging over all permutations of the tensor factors. The trace one subspace can be obtained as the span of all basis elements with the $N_{0,0,0} = \mathbb{1}$ component set to $1/D$.

Due to linearity, the symmetrisation map is completely determined by its action on the Pauli basis. Given a Pauli operator g , there is a permutation $\pi \in S_n$ such that $\pi(g) = X^{\otimes i} \otimes Y^{\otimes j} \otimes Z^{\otimes k} \otimes \mathbb{1}^{\otimes (n-i-j-k)}$. The appearing exponents $i = \text{wt}_X(g)$, $j = \text{wt}_Y(g)$ and $k = \text{wt}_Z(g)$ are exactly the *weights* of g , i.e. the number of X , Y , Z factors, respectively. By the invariance of Sym under permutations, we thus get $\text{Sym}(g) = \text{Sym}(\pi(g)) = N_{i,j,k}$. We define *weight indicator functions*,

$$A_{i,j,k}(g) := \begin{cases} 1 & \text{if } \text{wt}_X = i, \text{wt}_Y = j, \text{wt}_Z = k, \\ 0 & \text{else,} \end{cases} \quad (18)$$

such that we can write the S_n -projection of a Pauli operator g as

$$\text{Sym}(g) = \sum_{i,j,k} A_{i,j,k}(g) N_{i,j,k}. \quad (19)$$

By extending the functions $A_{i,j,k}$ linearly to H_D , we thus get exactly the coefficients of the projection in the number basis.

Let $S < \mathcal{P}_n$ be a stabiliser group stabilising a state s . The projection of this state is

$$\begin{aligned} \text{Sym}(s) &= \frac{1}{2^n} \sum_{g \in S} \text{sgn}(g) \text{Sym}(g) \\ &= \frac{1}{2^n} \sum_{i,j,k} \left(\sum_{g \in S} \text{sgn}(g) A_{i,j,k}(g) \right) N_{i,j,k} \\ &= \frac{1}{2^n} \sum_{i,j,k} A_{i,j,k}^{\pm}(S) N_{i,j,k}. \end{aligned} \quad (20)$$

The $A_{i,j,k}^{\pm}(S)$ are the coefficients of the *complete signed quantum weight enumerators* of the stabiliser code S . Recall that for a classical code $C \subset \mathbb{F}_d^n$, the *complete weight enumerator* is the degree- n polynomial in d variables given by

$$\sum_{c \in C} x_0^{\text{wt}_0(c)} \dots x_{d-1}^{\text{wt}_{d-1}(c)} =: \sum_{i_1, \dots, i_{d-1}} A_{i_1, \dots, i_{d-1}}(C) x_0^{n-(i_1+\dots+i_{d-1})} x_1^{i_1} \dots x_{d-1}^{i_{d-1}},$$

where $\text{wt}_i(c)$ gives the number of times $i \in \mathbb{F}_d$ appears in c [26]. The analogy should be clear. *Unsigned* weight enumerators for quantum codes have been studied since the early days of quantum coding theory [28, Ch. 13]. Much less seems to be known about their signed counterparts, with Refs. [32, 33] being the only related references we are aware of. There it is shown that, as their classical analogues, signed quantum weight enumerators are NP-hard to compute.

Finally, we want to return to the cases $|\psi\rangle = |H\rangle$ and $|\psi\rangle = |T\rangle$ and discuss the invariant subspaces $V^{H,T} := V^{G_{H,T}}$ for these states. Let us rotate the Pauli basis such that the first basis vector corresponds to the Bloch representation of $|H\rangle$ and $|T\rangle$,

respectively:

$$E_1^H := \frac{1}{\sqrt{2}}(X + Y), \quad E_1^T := \frac{1}{\sqrt{3}}(X + Y + Z), \quad (21)$$

$$E_2^H := \frac{1}{\sqrt{2}}(X - Y), \quad E_2^T := \frac{1}{\sqrt{6}}(X - 2Y + Z) \quad (22)$$

$$E_3^H := Z, \quad E_3^T := \frac{1}{\sqrt{2}}(X - Z). \quad (23)$$

Note that this choice of basis is such that the orthogonal decompositions of state space $H_2 = \langle \mathbb{1} \rangle \oplus \langle E_1^H \rangle \oplus \langle E_2^H \rangle \oplus \langle E_3^H \rangle = \langle \mathbb{1} \rangle \oplus \langle E_1^T \rangle \oplus \langle E_2^T, E_3^T \rangle$ correspond to (real) irreps of the respective Clifford stabilisers $(\mathcal{C}_1)_{H,T}$, as can be seen from the matrix representation of the generators in the rotated basis:

$$SX \simeq \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \quad SH \simeq \frac{1}{2} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & -1 & \sqrt{3} \\ 0 & 0 & -\sqrt{3} & -1 \end{pmatrix}. \quad (24)$$

In general, a basis for the trivial representation of $(\mathcal{C}_1)_{H,T}^{\otimes n}$ in the n -qubit state space H_{2^n} is given by $\mathcal{B}^{H,T} := \{\mathbb{1}, E_1^{H,T}\}^{\otimes n}$. To construct a basis for the full invariant subspace, we have to symmetrise $\mathcal{B}^{H,T}$ resulting in $\{N_{i,0,0}^{H,T} =: N_i^{H,T} \mid i = 0, \dots, n\}$. Here, $N_{i,j,k}^{H,T}$ is the occupation number basis associated to the rotated basis $\{\mathbb{1}, E_1^{H,T}, E_2^{H,T}, E_3^{H,T}\}$ and is constructed analogously to before.

In general, the components of stabiliser states in the rotated bases can be written in terms of weight enumerators by computing the induced basis transformations on $\text{Sym}(H_D)$ from $N_{i,j,k}$ to $N_{i,j,k}^{H,T}$. However, we are only interested in the projection onto $j = k = 0$ which simplifies this computation. First, let us rewrite the n -qubit Pauli operators in the H -basis. Note that every operator with non-vanishing Z -weight is already in the orthocomplement of V^H .

$$\begin{aligned} X^{\otimes i} \otimes Y^{\otimes j} &= \left(\frac{1}{\sqrt{2}}\right)^{i+j} (E_1^H + E_2^H)^{\otimes i} \otimes (E_1^H - E_2^H)^{\otimes j} \\ &= \left(\frac{1}{\sqrt{2}}\right)^{i+j} (E_1^H)^{\otimes(i+j)} + \text{orth. terms} \end{aligned} \quad (25)$$

Here, we left out possible identity factors and all orthogonal terms on the RHS, i. e. those containing E_2^H . This result implies that we can write the projection of a stabiliser state s as

$$\Pi_H(s) = \frac{1}{2^n} \sum_{i=0}^n \left(\sum_{j=0}^i A_{i-j,j,0}^{\pm}(S) \right) \frac{N_i^H}{2^{i/2}} =: \frac{1}{2^n} \sum_{i=0}^n B_i^{\pm}(S) \frac{N_i^H}{2^{i/2}}. \quad (26)$$

We call the numbers $B_i^{\pm}(S)$ the *partial signed quantum weight enumerators* of S . The analysis works the same way for the T -projection:

$$\begin{aligned} X^{\otimes i} \otimes Y^{\otimes j} \otimes Z^{\otimes k} &= \left(\frac{E_1^T}{\sqrt{3}} + \frac{E_2^T}{\sqrt{6}} + \frac{E_3^T}{\sqrt{2}} \right)^{\otimes i} \otimes \left(\frac{E_1^T}{\sqrt{3}} - \sqrt{\frac{2}{3}} E_2^T \right)^{\otimes j} \otimes \\ &\quad \otimes \left(\frac{E_1^T}{\sqrt{3}} + \frac{E_2^T}{\sqrt{6}} - \frac{E_3^T}{\sqrt{2}} \right)^{\otimes k} \\ &= \left(\frac{1}{\sqrt{3}} \right)^{i+j+k} (E_1^T)^{\otimes(i+j+k)} + \text{orth. terms} \end{aligned} \quad (27)$$

In this case, the T -projection of a stabiliser state s with stabiliser group S involves *total signed quantum weight enumerators* $C_i^{\pm}(S)$ as follows:

$$\Pi_T(s) = \frac{1}{2^n} \sum_{i=0}^n \left(\sum_{j=0}^i \sum_{k=0}^{i-j} A_{i-j-k,j,k}^{\pm}(S) \right) \frac{N_i^T}{3^{i/2}} =: \frac{1}{2^n} \sum_{i=0}^n C_i^{\pm}(S) \frac{N_i^T}{3^{i/2}}. \quad (28)$$

Note that all projections $\text{Sym} \equiv \Pi_{S_n}$, Π_H and Π_T can be computed from the complete signed weight enumerators of the stabiliser codes which themselves are functions of the weight distributions. For numerical purposes, it is convenient to absorb all appearing factors in the bases such that the coefficients of stabiliser states are given by the integer weight enumerators.

Finally, we want to give expressions for the states $|H\rangle^{\otimes n}$ and $|T\rangle^{\otimes n}$ in the respective bases:

$$|H\rangle \langle H|^{\otimes n} = \frac{1}{2^n} (\mathbb{1} + E_1^H)^{\otimes n} = \frac{1}{2^n} \sum_{i=0}^n \binom{n}{i} N_i^H, \quad (29)$$

$$|T\rangle \langle T|^{\otimes n} = \frac{1}{2^n} (\mathbb{1} + E_1^T)^{\otimes n} = \frac{1}{2^n} \sum_{i=0}^n \binom{n}{i} N_i^T. \quad (30)$$

In general, we are not aware of any method which can predict whether the projection of a stabiliser state will be extremal within the projected polytope. However, the following lemma gives a necessary condition on the extremality of products $s \otimes s'$ of stabiliser states which will be useful later.

Lemma 1 (Projection of product states). *The following is true for $\Pi = \text{Sym}, \Pi_H, \Pi_T$: If the projection $\Pi(s)$ of an arbitrary stabiliser state s is non-extremal, so is $\Pi(s \otimes s')$ for any other stabiliser state s' .*

Proof. We prove the statement by showing it on the level of the complete signed weight enumerators $A_{i,j,k}^\pm$. This proves the claim directly for $\Pi = \text{Sym}$ and the other cases follow since the partial and total signed weight enumerators are linear functions of the complete ones.

Note that the Pauli X, Y, Z weights are additive under tensor products, e. g. $\text{wt}_X(g \otimes g') = \text{wt}_X(g) + \text{wt}_X(g')$. This implies that we can write the indicator function as $A_{i,j,k}(g \otimes g') = A_{i',j',k'}(g) A_{i-i',j-j',k-k'}(g')$ for i', j', k' being the weights of g . However, since $A_{i',j',k'}(g)$ is zero if i', j', k' are not the weights of g , we can instead sum over all possible decompositions on the right hand side. Hence, for any two stabiliser codes S, S' we get

$$\begin{aligned} A_{i,j,k}^\pm(S \times S') &= \sum_{g \in S, g' \in S'} \text{sgn}(g \otimes g') A_{i,j,k}(g \otimes g') \\ &= \sum_{i'=0}^i \sum_{j'=0}^j \sum_{k'=0}^k \sum_{g \in S} \sum_{g' \in S'} \text{sgn}(g) \text{sgn}(g') A_{i',j',k'}(g) A_{i-i',j-j',k-k'}(g') \quad (31) \\ &= \sum_{i'=0}^i \sum_{j'=0}^j \sum_{k'=0}^k A_{i',j',k'}^\pm(S) A_{i-i',j-j',k-k'}^\pm(S'). \end{aligned}$$

Suppose S is the stabiliser of a state s and $\text{Sym}(s)$ can be written as convex combination,

$$\text{Sym}(s) = \sum_{l=1}^M \lambda_l \text{Sym}(s_l) \quad \Leftrightarrow \quad A_{i,j,k}^\pm(S) = \sum_{l=1}^M \lambda_l A_{i,j,k}^\pm(S_l), \quad (32)$$

with stabiliser states s_l , stabilised by the groups S_l . Let s' be stabilised by S' , then we find by Eq. (31),

$$A_{i,j,k}^\pm(S \times S') = \sum_{i',j',k'} \sum_{l=1}^M \lambda_l A_{i',j',k'}^\pm(S_l) A_{i-i',j-j',k-k'}^\pm(S') = \sum_{l=1}^M \lambda_l A_{i,j,k}^\pm(S_l \times S'), \quad (33)$$

and hence the projection of the product state $s \otimes s'$ is non-extremal. $\square$

Note that Eq. (31) allows us to compute the projection of products $\Pi(s \otimes s')$ from $\Pi(s)$ and $\Pi(s')$ via the signed quantum weight enumerators using $\text{poly}(n)$ operations. This is an important improvement over computing $\Pi(s)$ for a general (fully entangled) stabiliser state s which requires $O(2^n)$ operations.

3.4 Representatives of inequivalent stabiliser states

Computing the projected polytope involves the computation of the signed quantum weight enumerators for all stabiliser states. However, from the previous discussions we know that we can restrict the computations to the orbits $\text{stab}(n)/G_\rho$ with respect to the symmetry group G_ρ . In this section we will construct representatives for these orbits.

Our approach is based on a subset of the set of stabiliser states, the so-called *graph states* $\text{graph}(n)$. For every simple, i. e. self-loop free, graph G of n vertices, there is a state vector $|G\rangle$ that is stabilised by operators of the form

$$K_j = X_j \prod_{k=1}^n Z_k^{\theta_{jk}}, \quad (j = 1, \dots, n), \quad (34)$$

where X_j, Z_j are the Pauli operators on the j -th qubit and θ is the adjacency matrix of the graph G . Graph states play a fundamental role in the studies of stabiliser states since Schlingemann [35] proved that every stabiliser state is equivalent to a graph state under the action of the local Clifford group $LC_n = \mathcal{C}_1^{\otimes n}$:

$$\text{stab}(n) = LC_n \cdot \text{graph}(n). \quad (35)$$

This result can be used to label every stabiliser state vector $|C, G\rangle$ by a local Clifford unitary $C \in LC_n$ and a graph state $|G\rangle \in \text{graph}(n)$ such that $|C, G\rangle = C|G\rangle$. However, LC_n -equivalent graph states generate the same LC_n -orbit and are equally well suited to represent a stabiliser state. Hein, Eisert, and Briegel [19] and Nest, Dehaene, and De Moor [29] discovered that two graph states are LC_n -equivalent if and only if the underlying graphs are related by a graph theoretic transformation called *local complementation* (LC). Thus, it is sufficient to consider graphs up to local complementation.

Furthermore, the symmetry group G_ρ induces additional equivalence relations on the graph state representation. Let us again begin the discussion with the case of a generic state with S_n -symmetry. This already allows us to restrict the representation to non-isomorphic graphs, i. e. graphs up to permutation of their vertices, since for any graph state $|G\rangle$ and a permuted version $|\pi G\rangle \equiv \pi|G\rangle$ the LC_n -orbits are isomorphic: $\pi C|G\rangle = C_\pi|\pi G\rangle$ with the permuted local Clifford unitary $C_\pi = \pi C \pi^\dagger \in LC_n$. Moreover, it is straightforward to show that the composition of graph isomorphism and local complementation is symmetric and thus a equivalence relation $\sim_{LC, S_n}$ on graphs whose equivalence classes are isomorphic to $\text{graph}(n)/\sim_{LC, S_n}$. These equivalence classes have been studied in the context of graph codes and entanglement in graph states [11, 20] and were enumerated by Danielsen [10]. However, different local Clifford unitaries can still result in equivalent states. To see this, pick some symmetry $\pi \in \text{Aut}(G)$ of the graph, i. e. $\pi G = G$, then the actions of C and C_π yield isomorphic states. Hence, it is enough to act with $LC_n/\text{Aut}(G)$ on the graph state $|G\rangle$.

For the computation of the LC_n -orbits it is enough to consider $LC_n/\mathcal{P}_n$, since Pauli operators will only change the possible 2^n signs of the final generators which are better added by hand. It is well known that the quotient $\mathcal{C}_n/\mathcal{P}_n$ is isomorphic to the binary symplectic group $\text{Sp}(2n, \mathbb{Z}_2)$ which is the foundation of the phase space formalism. We make use of this formalism to compute the LC_n -orbits of graph states G by evaluating the orbits of the local symplectic group $\text{Sp}(2, \mathbb{Z}_2)^{\times n}$ up to the stabiliser of G and $\text{Aut}(G)$.

The additional symmetries in the case of the $|H\rangle$ and $|T\rangle$ state can be taken into account by restricting the allowed symplectic transformations using the symplectic maps $\hat{S}$ and $\hat{S}\hat{H}$ induced by the generators SX and SH , respectively. The corresponding cosets are given by the representatives $\text{Sp}(2, \mathbb{Z}_2)/\langle\hat{S}\rangle \simeq \{\mathbb{1}, \hat{H}, \hat{H}\hat{S}\}$ and $\text{Sp}(2, \mathbb{Z}_2)/\langle\hat{S}\hat{H}\rangle \simeq \{\mathbb{1}, \hat{S}\}$, respectively.

However, the described generation procedure will quickly become computationally expensive. Moreover, most of the projected stabiliser states are non-extremal points for the projected polytope and thus redundant. Unfortunately, there is no simple way

Figure 6: Vertices of the projected stabiliser polytope for the $|H\rangle$ symmetry group G_H . These states are represented as decorated graph states compatible with Refs. [14, 35], c.f. the description in the text. The convex hull of these vertices is shown in Fig. 4.

of deciding whether a state will be extremal after projection or not. However, Lemma 1 states at least a criterion for product states which allows us to restrict to projecting only *fully entangled stabiliser states*. To this end, we only have to iterate over *connected* graph representatives with respect to $\sim_{LC, S_n}$ and compute the projections of product states directly from lower-dimensional vertices using the appropriate version of Eq. (31).

4 Computing the robustness of magic

Using the enumeration procedure of the last section, we generated the set of H - and T -projections of *fully entangled* stabiliser states $\overline{\text{stab}}_c^{H/T}(n) = \Pi_{H/T}(\text{stab}_c(n))$ and the set of projected product states from lower-dimensional vertices. In an additional step, we removed non-extremal points from the set of projected states, resulting in vertex sets $\mathcal{V}_n^{H/T}$ of the projected stabiliser polytopes for $n \leq 9$ and $n \leq 10$, respectively. As described in the last section, we are labelling the vertices by certain stabiliser representatives. To this end, we use a notation in terms of “decorated graph states” compatible with Refs. [14, 35]: A graph is decorated by symbols which indicate the action of local Clifford operations on the respective graph state. Nodes with signs indicate a sign change of the respective stabiliser generator, or alternatively, the action of Z on the respective qubit prior the any other gates. A hollow node in the graph denotes a Hadamard gate acting on the respective qubit and self-loops correspond to the action of phase gates (prior to possible Hadamard gates). Figure 6 shows the vertex sets $\mathcal{V}_n^H$ for $n = 1, 2, 3$. Since the dimension of the polytope is exactly n , it can be easily visualised for $n \leq 3$, see also Fig. 4 in Sec. 2.

The database of vertices and the program code can be found on the arXiv [21]. For a discussion of the algorithmic details see App. D.

Table 1 shows the number of vertices of the projected polytopes in comparison with the original number of stabiliser states. We see that the number of states N that have to be used in the ℓ_1 -minimisation is reduced drastically from $2^{O(n^2)}$ to a scaling which is approximately 2^n . Additionally, the dimension d of the ambient space is reduced exponentially from $4^n - 1$ to exactly n . As discussed in Sec. 3.2, the required ℓ_1 -minimisation for RoM is computed via a linear program with $2N + d$ constraints and $2N$ variables and has a runtime that is linear in its size $(2N + d)(2N) = 4N^2 + 2Nd$.

n	$ \text{stab}(n) $	$ \overline{\text{stab}}_c^H(n) + \text{prod.}$	$ \mathcal{V}_n^H $	$ \overline{\text{stab}}_c^T(n) + \text{prod.}$	$ \mathcal{V}_n^T $
1	6	3+0	2	2+0	2
2	60	5+3	4	4+3	4
3	1080	11+8	8	4+8	6
4	36720	48+18	13	18+14	12
5	2423520	252+38	32	61+26	22
6	315057600	1881+86	60	256+57	42
7	81284860800	20378+208	144	2151+116	66
8	41780418451200	331794+510	304	21475+226	131
9	42866709330931200	8410183+1270	804	329712+462	238
10	—	—	—	5964000+991	371

Table 1: Number of stabiliser states $|\text{stab}(n)|$ in comparison with the number of projections of fully entangled stabiliser states $|\overline{\text{stab}}_c(n)|$, projected product states and vertices $|\mathcal{V}_n|$ of the projected stabiliser polytope as a function of the number of qubits n .

The runtime is thus reduced as

$$2^{O(n^2)} \longrightarrow 2^{O(n)}, \quad (36)$$

leading to a super-polynomial speed-up in the ℓ_1 -minimisation. Although both time and space complexity of the ℓ_1 -minimisation are exponential in n , it is in principle feasible for moderate n . Here, the limiting factor is the implementation of the oracle providing the projected states with runtime which is still super-exponential in n .

4.1 Robustness of the $|H\rangle^{\otimes n}$ and $|T\rangle^{\otimes n}$ states

Figure 7 shows the Robustness of Magic of $|H\rangle^{\otimes n}$ for $n = 1, \dots, 9$, computed from the vertices $\mathcal{V}_n^H$ of the projected stabiliser polytope. Note that the data for $n \leq 5$ is in perfect agreement with the so-far computed values in Ref. [23]. We are particularly interested in the submultiplicative behaviour of $\mathcal{R}$. Here, the new data for $n > 5$ turns out to be helpful: We can observe that the data points quickly approach an apparent exponential scaling with n . More precisely, submultiplicativity is clearly observable for $1 \leq n \leq 4$, but the scaling becomes effectively multiplicative for larger n . We quantified this using an exponential fit of the data range $3 \leq n \leq 9$ (shown in blue in Fig. 7) resulting in $(1.059 \pm 0.015) \times (1.283 \pm 0.002)^n$. From previous works it is known that the *regularised* robustness $\mathcal{R}_{\text{reg}}(|H\rangle)$ is bounded from below by 1.207. Our work, however, indicates that it converges from above to a constant which is given by the fit as (1.283 ± 0.002) .

The previously known time complexity for simulating a circuit with t T gates using the RoM algorithm is $O(2^{0.753t})$ [23]. Our findings improve this to $O(\mathcal{R}(|H\rangle^{\otimes 9})^{\frac{2t}{9}}) = O(1.667^t) = O(2^{0.737t})$. Moreover, since we already explored an effectively multiplicative regime of the RoM, solving the problem for higher $n > 9$ will not much reduce the runtime. From our estimate for the asymptotic regularised robustness, we can estimate the best possible scaling to be $2^{0.719t}$.

Furthermore, we applied the same procedure to compute the robustness of the magic state $|T\rangle^{\otimes n}$. Since the T -symmetry group is larger than in the previous case, we were able to compute $\mathcal{R}(|T\rangle^{\otimes n})$ for up to 10 qubits, see Fig. 8. Qualitatively, the results agree very well with those of the last section. Quantitatively, the robustness of the T state is considerably higher than the one of the H state. Using again an exponential fit, we find the scaling $(1.169 \pm 0.011) \times (1.3865 \pm 0.0014)^n$ which predicts a regularised robustness of $(1.3865 \pm 0.0014)^n$. By the RoM construction, the 10-qubit solution gives rise to a simulation algorithm with runtime $O(1.984^m) = O(2^{0.988m})$ where m is the total number of $|T\rangle$ magic states used, or equivalently, the number of $\pi/12$ Z -rotation gates.

Figure 7: Robustness (blue) and regularised robustness (green) of the magic state $|H\rangle^{\otimes n}$ as a function of the number of qubits n . The blue line is the exponential fit $(1.059 \pm 0.015) \times (1.283 \pm 0.002)^n$ of the data.

Figure 8: Robustness (blue) and regularised robustness (green) of the magic state $|T\rangle^{\otimes n}$ as a function of the number of qubits n . The blue line is the exponential fit $(1.169 \pm 0.011) \times (1.386 \pm 0.0014)^n$ of the data.

4.2 Analysis of the optimal solutions

Additionally, we studied the optimal solutions of the ℓ_1 -minimisation for the previously discussed cases of $|H\rangle^{\otimes n}$ and $|T\rangle^{\otimes n}$. For this purpose, it is instructive to use the original formulation of the robustness of a state ρ in terms of an optimal affine combination of two (mixed) stabiliser states $\sigma^\pm \in \overline{\text{SP}}_n^{H,T}$, cp. Eq. (5):

$$\rho = \frac{1}{2} [(\mathcal{R}(\rho) + 1)\sigma^+ - (\mathcal{R}(\rho) - 1)\sigma^-]. \quad (37)$$

The states $\sigma^\pm$ can be obtained from the optimal solution of the ℓ_1 -minimisation $\rho = \sum_i x_i^* v_i$ as follows:

$$\sigma^+ = \frac{2}{\mathcal{R}(\rho) + 1} \sum_{i: x_i^* > 0} x_i^* v_i, \quad \sigma^- = -\frac{2}{\mathcal{R}(\rho) - 1} \sum_{i: x_i^* < 0} x_i^* v_i. \quad (38)$$

Recall from the discussion in Sec. 3.2 that replacing every vertex v_i in the optimal solution by a stabiliser representative in its preimage $\Pi_{H,T}^{-1}(v_i)$ yields an optimal solution for the original problem. Hence, we simply identify the vertices of the projected polytope by their stabiliser representatives constructed in Sec. 3.3. Surprisingly, these states seem to have a rather simple structure, especially the positive contributions σ^+ . We will discuss the solutions in the following for the H and T case separately.

Figure 9: Positive contributions to the optimal affine combination for $|H\rangle^{\otimes n}$, written as convex combinations of stabiliser states. These states are represented as decorated graph states where hollow nodes indicate Hadamard action on the respective nodes and signs represent the respective sign of the stabiliser generator. Note that these states have only $\lfloor \log_2 n \rfloor$ contributions which themselves are products of $|+\rangle$ and Bell states.

Optimal solutions for the $|H\rangle^{\otimes n}$ state The positive contributions σ^+ to the $|H\rangle^{\otimes n}$ state for $n = 1, 2, 3$ are simply given by the graph state $|+\rangle^{\otimes n}$. Figure 9 shows the remaining states for $n = 4, \dots, 8$. Note that these states have to lie on a facet of the polytope to minimise the robustness. But instead of the generic n contributions, they can be written using only $\lfloor \log_2 n \rfloor$ terms. The vertices themselves are products of $|+\rangle$ and the Bell state $|\Psi^+\rangle$.

In contrast, the negative contributions σ^- , shown in Fig. 10, have less structure and seem to be partially irregular. Of course, σ^- has a non-unique convex combination and thus part of structure could be shadowed by the non-uniqueness. Nevertheless, since the dominant part of the contributions consists of products of $|\pm\rangle$ and the Bell states $|\Psi^\pm\rangle$, it is reasonable to assume that the σ^- can be approximated by Bell states. We suspect that this approximation is quite good, at least for a moderate number of qubits, due to the apparent suppression of vertices with more complex structure.

Motivated by these observations, we define the following polytope:

$$Q_n^H = \text{conv } \Pi_H \left(\left\{ \text{all } n \text{ qubits states that are products of } |\pm\rangle \text{ and } |\Psi^\pm\rangle \right\} \right). \quad (39)$$

By Eq. (31), we can compute these states efficiently from the signed weight enumerators of $|\pm\rangle$ and $|\Psi^\pm\rangle$. Note that the projection of $|+\rangle \otimes |-\rangle$ is a convex combination of the projected Bell states and thus only states with “all plus” or “all minus” contributions are extremal in Q_n^H . Let $\mathcal{W}_n^H$ be the set of vertices of Q_n^H and $m = \lfloor n/2 \rfloor$. We can explicitly enumerate its elements by tuples $(i, j, k) \in \{0, \dots, m\}^3$ such that $i + j + k = m$. Every such tuple corresponds to a product of i $|\Psi^+\rangle$, j $|\Psi^-\rangle$ and $(2k + n - 2m)$ $|\pm\rangle$ states. Hence, the number of vertices is

$$K := |\mathcal{W}_n^H| = 2 \sum_{i=0}^m (m+1-i) = (m+1)(m+2). \quad (40)$$

We define the approximate robustness of $|H\rangle^{\otimes n}$ as the robustness with respect to the

Figure 10: Negative contributions to the optimal affine combination for $|H\rangle^{\otimes n}$, written as convex combinations of stabiliser states. Note that these states have more contributions compared to the positive terms and seem partially irregular.

polytope Q_n^H :

$$r_n^H := \min \left\{ \|x\|_1 \mid x \in \mathbb{R}^K : \rho = \sum_{i=1}^K x_i w_i \text{ with } w_i \in \mathcal{W}_n^H \right\}. \quad (41)$$

Since the optimisation is over a subset of all projected stabiliser states, r_n^H is an upper bound for $\mathcal{R}(|H\rangle^{\otimes n})$. Moreover, it can be efficiently evaluated since both the complexity of computing $\mathcal{W}_n^H$ and of the ℓ_1 -minimisation is $O(n^4)$. Figure 11 shows a comparison of r_n^H with the exact robustness. From the previous analysis it is clear that the approximation is exact for $n \leq 4$. The deviation from the exact data for $4 < n \leq 9$ is at most 0.06% and thus negligible. However, we expect that the deviation becomes larger the higher n is, since it is likely that the importance of multipartite entangled contributions increases. Nevertheless, the approximation seems to be surprisingly good. The approximate data again follows an exponential increase with n , predicting an asymptotic regularised robustness of about (1.2829 ± 0.0017) which is compatible with the prediction (1.283 ± 0.002) from the exact data.

However, this approach is limited to $n \leq 26$. For larger n , the ℓ_1 -minimisation lacks a feasible solution, which can only be the case if $|H\rangle^{\otimes n}$ is not in the affine span of the product states $\mathcal{W}_n^H$. This indicates that the dimension of the subpolytope Q_n^H becomes too small. A solution to these infeasibility problems will be discussed in Sec. 4.3.

Figure 11: Exact (blue, orange) and approximate (purple, green) robustness and regularised robustness of the magic state $|H\rangle^{\otimes n}$ as a function of the number of qubits n .

Optimal solutions for the $|T\rangle^{\otimes n}$ state As in the previous case, the two connected vertices of the projected 2-qubit polytope constitute a dominant part in the optimal solutions. They are not projections of Bell states, so we will denote their representatives by $|\gamma^\pm\rangle$ and define them to be the states stabilised by $\{X_1 Z_2, Z_1 X_2\}$ and $\{-X_1 Z_2, -Z_1 Y_2\}$, respectively. The analysis of the optimal solutions shows that the σ^+ states are convex combinations of products of $|+\rangle$ and the maximally entangled state $|\gamma^+\rangle$. Moreover, they seem to be even more sparse than for the previous case, see Fig. 12. As in the case of $|H\rangle$, the σ^- state shows only partial structure, see Fig. 14.

The similarities suggest that the robustness for $|T\rangle^{\otimes n}$ can be well approximated using a similar procedure as in the last section. To this end, we define the polytope

$$Q_n^T = \text{conv } \Pi_T \left(\{ \text{all } n \text{ qubits states that are products of } |\pm\rangle \text{ and } |\gamma^\pm\rangle \} \right). \quad (42)$$

The approximate robustness r_n^T is again defined with respect to this polytope. The vertices $\mathcal{W}_n^T$ can be efficiently computed using the same procedure as in the $|H\rangle$ case and the approximation is exact for $n \leq 3$. Figure 13 shows the approximate robustness

Figure 12: Positive contributions to the optimal affine combination for $|T\rangle^{\otimes n}$ and $3 \leq n \leq 8$, written as convex combinations of stabiliser states. These states are again represented as decorated graph states, see Sec. 4. Note that these states have less than $\lfloor \log_2 n \rfloor$ contributions which themselves are product states made from $|+\rangle$ and Bell states.

Figure 13: Exact (blue, orange) and approximate (purple, green) robustness and regularised robustness of the magic state $|T\rangle^{\otimes n}$ as a function of the number of qubits n .

Figure 14: Negative contributions to the optimal affine combination for $|T\rangle^{\otimes n}$ and $3 \leq n \leq 8$, written as convex combinations of stabiliser states. These states are again represented as decorated graph states, see Sec. 4.

compared to the exact results. The approximation is again surprisingly good with a maximum deviation from the exact data of around 0.8%. Although this error is still small, it is an order of magnitude larger than for the $|H\rangle$ state. The approximation yields an asymptotic regularised robustness of (1.3916 ± 0.0014) which is slightly larger than the result from the exact data. Similar to the last section, the applicability of this approximation is limited to $n \leq 24$ due to the infeasibility of the optimisation problem for larger n . In the next section, we will show how to generalise this approximation to overcome the feasibility problems.

4.3 Finite hierarchy of RoM approximations

In general, the idea of restricting to at most k -partite entangled stabiliser states leads to a hierarchy of approximations with levels $1 \leq k \leq n$. Clearly, for $k = n$ the exact problem is recovered. The set of at most k -partite entangled n -qubit stabiliser states can be constructed by taking all possible tensor products of states in $\text{stab}(i)$ for $1 \leq i \leq k$ which result in n -qubit states. However, without the presence of additional symmetries, this will still result in an exponentially large set since already the set of fully separable stabiliser states ($k = 1$) has size 6^n .

Hence, we assume that we want to compute approximations to $\mathcal{R}(\rho)$ where ρ is a symmetric n -qubit state (not necessarily pure) such that the stabiliser symmetry group contains at least the symmetric group S_n . In particular, this applies to the magic states $|H\rangle^{\otimes n}$ and $|T\rangle^{\otimes n}$. In this case, we are able to give $\text{poly}(n)$ upper bounds on the runtime for every fixed level $k < n$.

Following Lemma 1 and Section 3.3, the set of S_n -projections of k -partite entangled n -qubit stabiliser states can be constructed from the vertices of the projected polytopes $\overline{\text{SP}}_i = \text{Sym}(\text{SP}_i)$ for $1 \leq i \leq k$ which have *fully entangled* representatives. Let us denote the sets of representatives by $V_i \subset \text{stab}(i)$. Since the order does not matter, the possible ways to take tensor products of these sets are exactly captured by (descending) partitions of n into parts with size at most k . We will denote such a partition by $\lambda \vdash_k n$. Then, we define the subpolytope of projected k -partite entangled states as

$$Q_{n,k} := \text{conv Sym} \left(\bigcup_{\lambda \vdash_k n} \bigotimes_{i \in \lambda} V_i \right), \quad (43)$$

and the k -th level of the RoM hierarchy by the relaxation of Prob. 1 to the subpolytope $Q_{n,k}$. Clearly, this defines an upper bound $r_{n,k}(\rho)$ to the exact RoM $\mathcal{R}(\rho)$.

To bound the runtime of the k -th level of the hierarchy, we have to count the vertices $\mathcal{W}_{n,k}$ of $Q_{n,k}$. An upper bound to this number is given by the number of tensor products appearing in Eq. (43) up to permutations. Thus, let λ be a (descending) partition of n into r parts, with no part larger than k :

$$n = \lambda_1 + \dots + \lambda_r, \quad k \geq \lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_r > 0. \quad (44)$$

This can be rewritten as

$$n = \sum_{i=1}^k m_i i, \quad (45)$$

where $0 \leq m_i \leq n$ is the *multiplicity* of i in the partition λ . Since the permutations of the partition itself were already considered, the number of product states corresponding to the partition λ is given, up to permutations, by

$$\prod_{i=1}^k |V_i^{m_i} / S_{m_i}| = \prod_{i=1}^k \binom{m_i + L_i - 1}{L_i - 1}, \quad L_i := |V_i|. \quad (46)$$

Using that the number of fully entangled vertices is increasing with i , we can bound this number by

$$\prod_{i=1}^k \binom{m_i + L_i - 1}{L_i - 1} \leq \prod_{i=1}^k m_i^{L_i} \leq n^{k L_k}. \quad (47)$$

Finally, the number of partitions of n with parts no greater than k coincides with the number of partitions of n into at most k parts and is denoted by $p_k(n)$. A standard result in number theory is that

$$p_k(n) = \frac{n^{k-1}}{k!(k-1)!} + O(n^{k-2}). \quad (48)$$

Thus, we can bound the number of vertices $\mathcal{W}_{n,k}$ to be

$$|\mathcal{W}_{n,k}| \leq p_k(n) n^{k L_k} = \frac{n^{k(L_k+1)-1}}{k!(k-1)!} + O(n^{k(L_k+1)-2}). \quad (49)$$

Since the dimension is $O(n^3)$, this implies that the runtime of the relaxation of Problem 1 is polynomial in n for a fixed k .

Finally, we remark that one has to know the vertex sets V_i up to k to run the k -th level of the hierarchy. Moreover, the bounds are very loose due to the fact we have not strictly bound the number of fully entangled vertices L_i which is beyond the scope of this paper. However, by using the actual numbers for L_i , one can obtain much better bounds on $|\mathcal{W}_{n,k}|$ by evaluating the binomial coefficients. Let us illustrate this for the case of $|H\rangle^{\otimes n}$ and $k = 2, 3$: Using that $p_2(n) = \lfloor \frac{n}{2} \rfloor + 1$, $p_3(n) = \lfloor \frac{(n+3)^3}{12} + \frac{1}{2} \rfloor$ and $L_1 = L_2 = L_3 = 2$, we find

$$|\mathcal{W}_{n,2}| \leq \left(\left\lfloor \frac{n}{2} \right\rfloor + 1 \right) \binom{n+2-1}{2-1}^2 = O(n^3), \quad (50)$$

$$|\mathcal{W}_{n,3}| \leq \left\lfloor \frac{(n+3)^3}{12} + \frac{1}{2} \right\rfloor n^3 = O(n^6). \quad (51)$$

Note that we derived $|\mathcal{W}_{n,2}| = O(n^2)$ in the previous section using further information about the extremality of products.

5 Conclusion & Outlook

In this work, we have studied the symmetries of the n -qubit stabiliser polytope and showed how to use these to greatly reduce the combinatorial complexity of computing the robustness of single-qubit magic states and to gain insight into the structure of the problem.

We have determined the symmetry groups for the two types of single-qubit magic states and have constructed explicit stabiliser state representatives of the symmetry orbits. This has allowed us to evaluate the robustness of $|H\rangle^{\otimes n}$ for $n \leq 9$ and $|T\rangle^{\otimes n}$ for $n \leq 10$ qubits. Using the structure of the solutions, we have proposed an approximation based on at most bipartite entangled states which is efficient in n and gives an upper bound on the exact robustness. Furthermore, the agreement with the exact data for $n \leq 10$ qubits is excellent. Since the RoM becomes effectively multiplicative for larger n , we expect that the approximation is still very good in the regime $n > 10$. Moreover, by restricting to k -partite entangled stabiliser states, we obtained a finite hierarchy of approximations which recovers the exact RoM for $k = n$. We showed that a fixed level $k < n$ of the hierarchy can be computed in $\text{poly}(n)$ time.

We feel that the most interesting task left open in this work is to explain why even two-body entangled states are sufficient to produce excellent bounds on the RoM. This may be insightful in a wider context. Indeed, sub-additivity of resource costs occurs in several areas of quantum information theory, most famously for the entanglement of formation [18]. The violations to additivity in [18] can be proven to exist for randomised constructions in high dimensions. This makes it hard to study the structure of the optimal solutions, or their behavior in a limit of many copies. The combinatorial nature of the stabiliser polytope, and the observation that only few-body entanglement is enough to find almost-optimal solutions, suggest that RoM may provide an instance where understanding submultiplicativity is feasible.

6 Acknowledgements

We thank Earl Campbell, Mateus Araújo, Felipe M. Mora, Felix Huber, Frank Valentin, Arne Heimendahl, and Huangjun Zhu for helpful discussions and comments. In particular, we want to thank Richard Kueng for productive discussions concerning the dual problem.

This work has been supported by the Excellence Initiative of the German Federal and State Governments (Grant ZUK 81), the German Research Foundation (DFG project B01 of CRC 183), and ARO under contract W911NF-14-1-0098 (Quantum Characterization, Verification, and Validation).

A Equivalence of the two robustness measures

The equivalence given in Eq. (6) is stated implicitly in [23]. Here, we give an explicit proof.

Vidal and Tarrach [38] defined the so-called *total robustness* which is given by

$$R(a) := \inf_{b \in S} R(a||b). \quad (52)$$

For S being a (compact) polytope, this can be rewritten as follows. Since S is compact, the minimum b^* is attained. Hence, $R(a) = R(a||b^*) =: s^*$ and

$$b^+ := \frac{1}{1 + s^*} (b^* + s^* a) \in S. \quad (53)$$

Let $\{v_1, \dots, v_N\}$ be the vertices of S and write $b^+, b^* \in S$ as convex combinations with coefficients λ_i and μ_i . It follows:

$$a = (1 + s^*)b^+ - s^*b^* = \sum_{i=1}^N \underbrace{((1 + s^*)\lambda_i - s^*\mu_i)}_{=: x(s^*)_i} v_i. \quad (54)$$

The last sum is an affine combination of the vertices since $\sum_i x(s^*)_i = 1$. In other words, $x(s^*)$ is a feasible solution for the following minimisation problem:

$$\mathcal{R}(a) := \min \left\{ \|x\|_1 \mid x \in \mathbb{R}^N : a = \sum_{i=1}^N x_i v_i \text{ and } 1 = \sum_{i=1}^N x_i \right\}. \quad (55)$$

Moreover, the optimal value can be bounded as follows:

$$\mathcal{R}(a) \leq \sum_{i=1}^N |x(s^*)_i| \leq (1 + s^*) \sum_{i=1}^N \lambda_i + s^* \sum_{i=1}^N \mu_i = 1 + 2s^* = 1 + 2R(a). \quad (56)$$

Assume x^* is the optimal solution for $\mathcal{R}(a)$. Then, we can rewrite $\mathcal{R}(a)$, using $\sum_i x_i = 1$, as follows:

$$\mathcal{R}(a) = \|x^*\|_1 = \sum_{i: x_i^* \geq 0} x_i^* - \sum_{i: x_i^* < 0} x_i^* = 1 + 2s(x^*), \quad \text{with } s(x^*) := - \sum_{i: x_i^* < 0} x_i^*. \quad (57)$$

Hence, the optimal affine combination for a becomes

$$a = \sum_{i: x_i^* \geq 0} x_i^* v_i - \sum_{i: x_i^* < 0} |x_i^*| v_i \quad (58)$$

$$= (1 + s(x^*)) \underbrace{\sum_{i: x_i^* \geq 0} \frac{x_i^*}{1 + s(x^*)} v_i}_{=: \beta^+} - s(x^*) \underbrace{\sum_{i: x_i^* < 0} \frac{|x_i^*|}{s(x^*)} v_i}_{=: \beta^-}. \quad (59)$$

Here, the renormalised modulus of the affine coefficients form a convex combination and hence $\beta^\pm \in S$. Thus, we found a pseudo-mixture for a and the parameter $s(x^*)$ can not be smaller than the total robustness of a :

$$R(a) \leq s(x^*) \Leftrightarrow \mathcal{R}(a) \geq 1 + 2R(a). \quad (60)$$

Combined with Eq. (56), this shows that the two measures are equivalent:

$$\mathcal{R}(a) = 1 + 2R(a). \quad (61)$$

Finally, let us remark that β^- constructed from the optimal affine combination for a is such that

$$R(a) = R(a||\beta^-). \quad (62)$$

B On the dual RoM problem

At this point, any analytical insight could be helpful in simplifying the problem. A standard method is dualising the problem. Clearly, by Slater's condition, strong duality holds and thus the dual problem is an equivalent definition for the Robustness of Magic. The dual problem is straightforwardly obtained as follows:

Problem 2 (Dualised Robustness of Magic). Let $\text{stab}(n) = \{s_1, \dots, s_N\}$ be the set of stabiliser states. Given a state ρ , solve the following problem:

$$\begin{aligned} \mathbf{max} \quad & \text{tr}(\rho Y) \quad \text{over } Y \in H_D, \\ \mathbf{s. t.} \quad & |\text{tr}(Y s_i)| \leq 1. \end{aligned}$$

This formulation of the RoM has a particularly nice form. Thus, it seems at first that the dual problem might be easier to solve. Indeed, one can guess the following feasible solution:

$$Y = \frac{1}{2^n} \sum_{i=1}^{4^n} \text{sgn}(\text{tr}(\rho w_i)) w_i. \quad (63)$$

Here, $\{w_1, \dots, w_{4^n}\}$ denote the n -qubit Pauli operators which generate the n -qubit Pauli group $\mathcal{P}_n$. Feasibility follows from the following calculation for a stabiliser state s with stabiliser group $S < \mathcal{P}_n$:

$$\begin{aligned} |\text{tr}(Ys)| &= \left| \frac{1}{2^n} \sum_{i=1}^{4^n} \text{sgn}(\text{tr}(\rho w_i)) \text{tr}(w_i s) \right| \\ &\leq \frac{1}{4^n} \sum_{i=1}^{4^n} |\text{sgn}(\text{tr}(\rho w_i))| \sum_{g \in S} |\text{tr}(w_i g)| \\ &= \frac{1}{2^n} \sum_{i=1}^{4^n} (\delta(w_i \in S) + \delta(-w_i \in S)) \\ &\leq \frac{1}{2^n} |S| = 1. \end{aligned} \quad (64)$$

The corresponding objective value is

$$\text{tr}(\rho Y) = \frac{1}{2^n} \sum_{i=1}^{4^n} \text{sgn}(\text{tr}(\rho w_i)) \text{tr}(\rho w_i) = \sum_{i=1}^{4^n} \left| \frac{\text{tr}(\rho w_i)}{2^n} \right| = \|p(\rho)\|_1, \quad (65)$$

where $p(\rho) \in \mathbb{R}^{D^2}$ is the coefficient vector of ρ in the Pauli basis, i.e. $p(\rho)_i = 2^{-n} \text{tr}(\rho w_i)$. The objective value yields a lower bound to the RoM of ρ . Note that this bound, also called *st-norm* $\|\rho\|_{\text{st}}$, was already found in [23] with different techniques and gives the following lower bound on the RoM of $|H\rangle^{\otimes n}$ and $|T\rangle^{\otimes n}$:

$$1.207^n \leq \mathcal{R}(|H\rangle^{\otimes n}), \quad 1.366^n \leq \mathcal{R}(|T\rangle^{\otimes n}). \quad (66)$$

C Symmetries of 3-designs

In this section, we characterise the symmetry group associated with the projectors of certain t -designs.

A *complex projective t -design* is a finite family $(\psi_i)_{i=1}^N$ of unit vectors in $\mathbb{C}^d$ such that

$$\frac{1}{N} \sum_{i=1}^N |\psi_i\rangle \langle \psi_i|^{\otimes t} = \frac{\text{Sym}_{[t]}}{D_{[t]}}, \quad (67)$$

where

$$\text{Sym}_{[t]} : (\mathbb{C}^d)^{\otimes t} \longrightarrow (\mathbb{C}^d)^{\otimes t}, \quad \text{Sym}_{[t]} := \frac{1}{t!} \sum_{\pi \in S_t} \pi \quad (68)$$

is the orthogonal projection onto the totally symmetric subspace $\text{Sym}((\mathbb{C}^d)^{\otimes t})$. Furthermore, $D_{[t]} = \binom{d+t-1}{t}$ is its dimension and $\pi \in S_t$ acts by permuting the factors of the tensor product $(\mathbb{C}^d)^{\otimes t}$. Taking a partial trace of Eq. (67) shows that a t -design is also a $t-1$ design.

As in the main part of this paper, we denote by H_d the real vector space of Hermitian $d \times d$ matrices with the induced Hilbert-Schmidt inner product $(A, B) := \text{tr}(AB)$. With respect to this inner product, we denote by $L^\dagger$ the adjoint of a linear map $L : H_d \rightarrow H_d$ and call L orthogonal if it preserves the inner product, or equivalently, if $L^\dagger = L^{-1}$.

Theorem 1. *Let $(\psi_i)_{i=1}^N \subset \mathbb{C}^d$ be a set of unit vectors. Let $L \in \text{End}(H_d)$ be a linear map on Hermitian operators that permutes the projectors $(|\psi_i\rangle\langle\psi_i|)_{i=1}^N$.*

1. *If $(\psi_i)_{i=1}^N$ is a 1-design, then L is unital (i.e. $L(\mathbb{1}) = \mathbb{1}$).*
2. *If $(\psi_i)_{i=1}^N$ is a 2-design, then L is orthogonal and trace-preserving.*
3. *If $(\psi_i)_{i=1}^N$ is a 3-design, then L is of the form $L = U \cdot U^\dagger$, where U is either a unitary or an antiunitary operator on $\mathbb{C}^d$.*

Proof. Define $\rho_i := |\psi_i\rangle\langle\psi_i|$.

1.—Using $\text{Sym}_{[1]} = \mathbb{1}$, we get

$$L(\mathbb{1}) = \frac{d}{N} \sum_{i=1}^N L(\rho_i) = \frac{d}{N} \sum_{i=1}^N \rho_i = \mathbb{1}, \quad (69)$$

hence L is unital.

2.—Let us define the traceless operators $f_i := \rho_i - \mathbb{1}/d$. Using the fact that $\{\psi_i\}_i$ forms a 2-design, Eq. (68), and the “swap trick”

$$\text{tr}(AB) = \text{tr}(A \otimes B \pi) \quad (70)$$

valid for the non-trivial element π of S_2 , one verifies the following for any traceless Hermitian operator $A \in H_d^0$:

$$\begin{aligned} \frac{1}{N} \sum_{i=1}^N (f_i, A)^2 &= \frac{1}{N} \sum_{i=1}^N \left[\text{tr}(\rho_i A) - \frac{1}{d} \text{tr}(A) \right]^2 \\ &= \frac{1}{N} \sum_{i=1}^N \text{tr}(\rho_i^{\otimes 2} A^{\otimes 2}) \\ &= \frac{1}{D_{[2]}} \text{tr}(\text{Sym}_{[2]} A^{\otimes 2}) \\ &= \frac{1}{2D_{[2]}} (\text{tr}(A)^2 + \text{tr}(A^2)) \\ &= \frac{\|A\|_2^2}{2D_{[2]}}. \end{aligned} \quad (71)$$

In other words, the operators (f_i) form a tight frame for the subspace $H_d^0 \subset H_d$ of traceless Hermitian matrices. Moreover, setting $f_0 = c\mathbb{1}$ with $c^2 = \frac{N(1-d)}{d^2+d^3}$, a similar calculation shows that the set $\{f_0, \dots, f_N\}$ forms a tight frame for all of H_d .

By 1., L is unital and thus permutes the tight frame $\{f_0, \dots, f_N\}$. However, any map permuting the elements of a tight frame is orthogonal. Finally, orthogonal and unital maps preserve the trace:

$$\text{tr } L(A) = \text{tr } \mathbb{1} L(A) = \text{tr } L^\dagger(\mathbb{1}) A = \text{tr } L^{-1}(\mathbb{1}) A = \text{tr } \mathbb{1} A = \text{tr } A. \quad (72)$$

3.—Consider the following trilinear function on H_d :

$$F(A, B, C) := \frac{1}{N} \sum_{i=1}^N \text{tr}(A \otimes B \otimes C \rho_i^{\otimes 3}). \quad (73)$$

F is invariant under L since $L^\dagger = L^{-1}$ is also a symmetry of the projectors ρ_i :

$$\begin{aligned} F(L(A), L(B), L(C)) &= \frac{1}{N} \sum_{i=1}^N \text{tr}(L(A) \otimes L(B) \otimes L(C) \rho_i^{\otimes 3}) \\ &= \frac{1}{N} \sum_{i=1}^N \text{tr} A \otimes B \otimes C (L^\dagger(\rho_i))^{\otimes 3} \\ &= \frac{1}{N} \sum_{i=1}^N \text{tr} A \otimes B \otimes C \rho_i^{\otimes 3} \\ &= F(A, B, C). \end{aligned} \quad (74)$$

We can explicitly evaluate F by expanding $\text{Sym}_{[3]}$ in terms of permutations and arguing as in Eq. (70). This yields

$$\begin{aligned} F(A, B, C) &= \text{tr} \left(A \otimes B \otimes C \frac{1}{N} \sum_{i=1}^N \rho_i^{\otimes 3} \right) \\ &= \frac{1}{D_{[3]}} \text{tr} (A \otimes B \otimes C \text{Sym}_{[3]}) \\ &= \frac{1}{6D_{[3]}} \left(\text{tr}(A) \text{tr}(B) \text{tr}(C) + \text{tr}(A) \text{tr}(BC) + \right. \\ &\quad \left. + \text{tr}(AB) \text{tr}(C) + \text{tr}(AC) \text{tr}(B) + \text{tr}(ABC) + \text{tr}(BAC) \right). \end{aligned} \quad (75)$$

The first four terms are individually L -invariant since L preserves the trace and is orthogonal. Hence, the L -invariance of F implies

$$\begin{aligned} \text{tr}(ABC) + \text{tr}(BAC) &= \text{tr} L(A)L(B)L(C) + \text{tr} L(B)L(A)L(C) \\ &= \text{tr} L^\dagger(L(A)L(B))C + \text{tr} L^\dagger(L(B)L(A))C. \end{aligned} \quad (76)$$

Since this holds $\forall C \in H_d$, we get

$$\begin{aligned} AB + BA &= L^\dagger(L(A)L(B)) + L^\dagger(L(B)L(A)) \\ \Leftrightarrow L(AB + BA) &= L(A)L(B) + L(B)L(A) \\ \Leftrightarrow L(\{A, B\}) &= \{L(A), L(B)\}. \end{aligned} \quad (77)$$

A linear automorphism on a matrix algebra fulfilling (77) is called a *Jordan automorphism*. Our goal is to apply a known structure theorem that restricts that form of such maps [22]. For the theorem to be applicable, we have to extend L from a map on the real vector space of Hermitian matrices, to a map on the algebra $M_d(\mathbb{C})$ of all matrices. To this end, we use that every $A \in M_d(\mathbb{C})$ can be written uniquely as $A = A_1 + iA_2$ where $A_{1,2} \in H_d$, and set

$$\hat{L}(A) := L(A_1) + iL(A_2) \in M_d(\mathbb{C}). \quad (78)$$

Clearly, this continuation yields a linear automorphism on $M_d(\mathbb{C})$. Moreover, since the anticommutator $\{\cdot, \cdot\}$ is bilinear, we get $\forall A, B \in M_d(\mathbb{C})$:

$$\hat{L}(\{A, B\}) = \{\hat{L}(A), \hat{L}(B)\}, \quad (79)$$

i. e. the continuation $\hat{L}$ to $M_d(\mathbb{C})$ is a Jordan automorphism. It is also straightforward to check that orthogonality of L implies that $\hat{L}$ is unitary with respect to the trace inner product.

It is known that every Jordan automorphism is either an algebra automorphism or algebra anti-automorphism [22]. Since every algebra automorphism is inner and $\hat{L}$ is unitary, $\hat{L}$ (and thus also $L \equiv \hat{L}|_{H_d}$) can in the first case be written as $\hat{L} = U \cdot U^\dagger$ for some $U \in U(d)$. In the second case, we can write $\hat{L}$ as a composition $\hat{L} = \hat{L}' \circ T$, where $\hat{L}' = U \cdot U^\dagger$ is an algebra automorphism and T is the transposition map. For every Hermitian matrix, transposition coincides with complex conjugation as $A^T = (A^\dagger)^* = A^*$. Hence, we can write $L = UC \cdot CU^\dagger$, where $U \in U(d)$ and C is complex conjugation on $\mathbb{C}^d$. Hence, L is in this case given by conjugation with the anti-unitary operator UC . $\square$

Since the qubit stabiliser state vectors in Hilbert space form a complex projective 3-design [25, 40, 41], we get the following corollary:

Corollary 1. *The group of stabiliser symmetries $\text{Aut}(\text{SP}_n)$ is given by the adjoint representation of the extended Clifford group EC_n .*

Proof. Theorem 1 implies that every qubit stabiliser symmetry is given by conjugation with either an unitary or anti-unitary operator on the Hilbert space $\mathbb{C}^{2^n}$.

Theorem 2 in [9] implies that every unitary operator that preserves the set of stabiliser states is an element of the Clifford group, up to a global phase.

Furthermore, note that complex conjugation C preserves the set of stabiliser states. Thus, if A is an anti-unitary operator preserving this set, CA is a perserving unitary operator. Hence, up to a phase, CA is Clifford and thus A is anti-Clifford. Finally, this implies our claim that $\text{Aut}(\text{SP}_n) = \text{Ad}(\text{EC}_n)$ $\square$

We note that the result is in general wrong for stabiliser states on odd-dimensional qudits. This also means that the third conclusion of Thm. 1 is not in general true for 2-designs. Concretely, take $(\psi_i)_i$ to be the set of stabiliser state vectors for $\mathbb{C}^d$, with d a prime number larger than or equal to 5. Then $(\psi_i)_{i=1}^N$ is a 2-design, but the group of linear symmetries of $\{|\psi_i\rangle\langle\psi_i|\}_i$ contains maps that cannot be represented by a linear or anti-linear operator on $\mathbb{C}^d$.

Sketch of proof. We sketch the proof of this claim in the language of [15]. With each $a \in \mathbb{Z}_d^2$, one can associate a *phase space point operator* $A(a)$. The $\{A(a)\}_a$ form a basis for H_d . The finite general linear group $GL(\mathbb{Z}_d^2)$ acts on this basis by permuting the indices $gA(a) = A(ga)$. The expansion coefficients $W_\rho(a)$ of an operator ρ with respect to the phase space point basis are the *Wigner function* of the operator. The stabiliser state $\rho_i = |\psi_i\rangle\langle\psi_i|$ are exactly the set of Hermitian operators whose Wigner function is the indicator function of an affine line in $\mathbb{Z}_d^2$ [15]. Clearly, the $GL(\mathbb{Z}_d^2)$ -action introduced above preserves the set of affine lines and thus permutes the ρ_i . As argued in the proof of Corollary 1, the group of (anti-)linear operators acting on the state vectors ψ_i is the extended Clifford group EC_n . To each U in EC_n , one can associate a $g \in \mathbb{Z}_d^2$ such that $UA(a)U^{-1} = A(ga)$. But g 's that arise this way have determinant $\det g = 1 \pmod d$ (if U is unitary) or $\det g = -1 \pmod d$ (if U is anti-unitary) [1]. The claim follows, as for $d \geq 5$, there are elements $g \in GL(\mathbb{Z}_d^2)$ with determinant different from ± 1 . $\square$

D Numerical implementation

Based on the discussion in Sec. 3.3, we can construct a generic algorithm for generating projected stabiliser states by calling various oracles. `GRAPHREPRESENTATIVES( $n$ )` generates suitable representatives of graph states. Here, these are given by *connected* representatives of $\text{graph}(n)/\sim_{LC, S_n}$ which were classified by Danielsen and Parker [11] up to 12 qubits and can be found in Ref. [10]. `GENERATORMATRIX( $G$ )` computes the binary generator matrix of the graph state $|G\rangle$. Furthermore, `LOCALSYMPLECTIC( $n, G$ )` returns the set of local symplectic matrices, ideally up to the considered symmetry group. For the discussed cases in Sec. 3.3, this is either the set of direct sums of $\{\mathbb{1}, \hat{H}, \hat{H}\hat{S}\}$ or

Algorithm 1 Algorithm for generating vertices of the projected stabiliser polytope

Require: Maximum number of qubits $n_{\max} \geq 1$, set of vertices $\mathcal{V}_n$

```

for  $n = 1, \dots, n_{\max}$  do
  for  $G \in \text{GRAPHREPRESENTATIVES}(n)$  do
     $M \leftarrow \text{GENERATORMATRIX}(G)$ 
    for  $S \in \text{LOCALSYMPLECTIC}(n, G)$  do
       $M' \leftarrow S \cdot M$ 
      for  $s \in \{-1, 1\}^{\times n}$  do
        Add  $\text{PROJECTSTATE}(M', s)$  to  $\mathcal{V}_n$ 
      end for
    end for
  end for
  for  $(i_1, \dots, i_k) \in \text{PARTITIONS}(n)$  do
    for  $v_1 \in \mathcal{V}_{i_1}, \dots, v_k \in \mathcal{V}_{i_k}$  do
      Add  $\text{PRODUCTSTATE}(v_1, \dots, v_k)$  to  $\mathcal{V}_n$ .
    end for
  end for
end for

```

$\{\mathbb{1}, \hat{S}\}$ up to the symmetry of the graph G . Finally, $\text{PROJECTSTATE}(M', s)$ and $\text{PRODUCTSTATE}(v_1, \dots, v_k)$ basically evaluate the weight enumerator formulas (18) and (31).

Furthermore, we use a output-sensitive algorithm by Dulá and Helgason [12] to compute the extremal points of the projected stabiliser polytope. This algorithm has time complexity $O(dNm)$ where d is the dimension, N the input size and m the output size, i.e. the number of extremal points. It performs way better than a naive approach since the input size $N = O(2^{n^2})$ is much larger than the number of extremal points $m = O(2^n)$.

E Symmetry reduction of convex optimisation problems

E.1 Group projections

The central tool for performing a symmetry reduction with respect to some (finite) group G is the so-called *G-projection*. Suppose g is represented by $\rho : G \rightarrow \text{GL}(V)$ on a (real or complex) vector space V , we define a linear map $\Pi_G : V \rightarrow V$, the *G-projection*, by

$$\Pi_G := \frac{1}{|G|} \sum_{g \in G} \rho(g). \quad (80)$$

The *G-projection* is well known in the representation theory of finite groups. In the physics literature, it is often called a *twirl* or *twirling operation*. Thus, we will also sometimes refer to it as *G-twirl*. For reference, we state some elementary properties of these maps without proof.

Proposition 2 (Properties of *G-projections*). *Let $\Pi_G : V \rightarrow V$ be a *G-projection*. Then the following holds:*

1. Π_G is a projection operator. Its image is the subspace V^G of fixed points of G .
2. If V is an inner product space and ρ is an orthogonal/unitary representation, then the projection is orthogonal/unitary.
3. For all $x \in V$, it holds that

$$\Pi_G(x) = \frac{1}{|G \cdot x|} \sum_{y \in G \cdot x} y. \quad (81)$$

4. Π_G is constant on every orbit in V/G
5. If $G = N \rtimes H$, then $\Pi_G = \Pi_N \circ \Pi_H = \Pi_H \circ \Pi_N$.

E.2 Symmetries in convex optimisation

A convex optimisation is the problem of minimising a convex function F over a convex set $\mathcal{X}$. It can always be rewritten in standard form as follows: Let $F : \mathbb{R}^N \rightarrow \mathbb{R}$ be a convex function and $C : \mathbb{R}^N \rightarrow \mathbb{R}^K$ be a (generalised) convex function with respect to the component-wise partial order $\preceq$ on $\mathbb{R}^K$, i. e. every component of C is convex. Furthermore, let $A : \mathbb{R}^N \rightarrow \mathbb{R}^M$ be an affine function. The problem is defined as [3]

$$\begin{aligned} & \textbf{Minimise} && F(x), \quad \text{for } x \in \mathbb{R}^N \\ & \textbf{subject to} && A(x) = 0, \\ & && C(x) \preceq 0. \end{aligned} \tag{82}$$

Here, the function F is called the *objective function* and the functions C and A are the (in-)equality *constraints*. Depending on the convex set that is modelled, one distinguishes between many subclasses such as linear, conic or semi-definite programming.

We call G a symmetry of the problem (82), if it acts on $\mathbb{R}^N$ such that the feasible set

$$\mathcal{X} = \{x \in \mathbb{R}^N \mid A(x) = 0, C(x) \preceq 0\}, \tag{83}$$

and the objective function F are left invariant. In particular, this will be the case if G acts linearly on all vector spaces such that the objective function is G -invariant and the constraints are G -equivariant, i. e. for all $x \in \mathbb{R}^N$ and $g \in G$ it holds

$$\begin{aligned} F(g \cdot x) &= F(x), \\ A(g \cdot x) &= g \cdot A(x), \\ C(g \cdot x) &= g \cdot C(x). \end{aligned} \tag{84}$$

Again, note that the G -action is different on the left and right hand side. Additionally, for G to be a proper symmetry, we require that its representation on $\mathbb{R}^K$ is given by *order automorphisms*, i. e.

$$p \preceq q \iff g \cdot p \preceq g \cdot q \quad \forall p, q \in \mathbb{R}^K, g \in G \tag{85}$$

Consequently, both the inequality $C(g \cdot x) \preceq 0$ and the equality constraint $A(g \cdot x) = 0$ are fulfilled if and only if they hold for x . Hence, $x \in \mathbb{R}^N$ is a feasible solution of Eq. (82) iff its orbit is feasible. Moreover, the objective function is constant on every orbit and thus any optimal solution x^* will have an orbit of optimal solutions.

The key point for the simplification of the problem is that all functions are *convex* (A is even affine). Let us again slightly abuse notation and denote with

$$\Pi_G = \frac{1}{|G|} \sum_{g \in G} g, \tag{86}$$

all G -projections on the respective spaces. Using this, we will derive two important consequences of G -equivariance of A and C . First, we evaluate the affine function A :

$$A \circ \Pi_G(x) = \frac{1}{|G|} \sum_{g \in G} A \circ g(x) = \frac{1}{|G|} \sum_{g \in G} g \circ A(x) = \Pi_G \circ A(x). \tag{87}$$

Recall that C is convex w.r.t. to the component-wise order $\preceq$ and that every $g \in G$ preserves this order. Thus, Π_G preserves order, too, and it follows:

$$C \circ \Pi_G(x) \preceq \frac{1}{|G|} \sum_{g \in G} C \circ g(x) = \frac{1}{|G|} \sum_{g \in G} g \circ C(x) \preceq \Pi_G \circ C(x). \tag{88}$$

Suppose x is a feasible solution, then by these relations, its G -projection $x^G = \Pi_G(x)$ is feasible, too. Following the same argument as above, we get $F(x^G) \leq F(x)$. Finally, we find the following results:

Lemma 2. *Every G -symmetric convex optimisation problem has a G -invariant optimal solution.*

Proof. Be x^* a optimal solution, then $\Pi_G(x^*)$ is G -invariant, feasible and $F(\Pi_G(x^*)) \leq F(x^*)$. Hence, $\Pi_G(x^*)$ is optimal, too. $\square$

Theorem 2 (Symmetry reduction of convex optimisation problems). *The convex optimisation problem (82) with symmetry group G is equivalent to the following, symmetry-reduced convex optimisation problem:*

$$\begin{aligned} & \textbf{Minimise} && F^G(x), \quad \text{for } x \in X^G \\ & \textbf{subject to} && A^G(x) = 0, \\ & && C^G(x) \preceq 0. \end{aligned} \tag{89}$$

With $F^G : X^G \rightarrow \mathbb{R}$, $A^G : X^G \rightarrow Y^G$ and $C^G : X^G \rightarrow Z^G$ being functions such that

$$F^G \circ \Pi_G = F, \quad A^G \circ \Pi_G = \Pi_G \circ A, \quad C^G \circ \Pi_G = \Pi_G \circ C, \tag{90}$$

and X^G, Y^G, Z^G being the G -invariant subspace of $X = \mathbb{R}^N, Y = \mathbb{R}^M$ and $Z = \mathbb{R}^K$.

Proof. First, it should be clear that the functions F^G, A^G and C^G exist and are well-defined by Eq. (90). Moreover, we compute for $x, y \in X^G$ and $t \in [0, 1], s \in \mathbb{R}$:

$$\begin{aligned} F^G(tx + (1-t)y) &= F(tx + (1-t)y) \\ &\leq tF(x) + (1-t)F(y) \\ &= tF^G(x) + (1-t)F^G(y), \\ A^G(sx + (1-s)y) &= \Pi_G \circ A(sx + (1-s)y) \\ &= s\Pi_G \circ A(x) + (1-s)\Pi_G \circ A(y) \\ &= sA^G(x) + (1-s)A^G(y), \\ C^G(tx + (1-t)y) &= \Pi_G \circ C(tx + (1-t)y) \\ &\preceq t\Pi_G \circ C(x) + (1-t)\Pi_G \circ C(y) \\ &= tC^G(x) + (1-t)C^G(y). \end{aligned} \tag{91}$$

Hence, F^G and C^G are convex and A^G as an affine function.

Suppose $x \in \mathbb{R}^N$ is a feasible solution of the original problem (82) which can be assumed to be G -invariant, i.e. $x \in X^G$. It will be feasible for the reduced problem since

$$\begin{aligned} A^G(x) &= A^G \circ \Pi_G(x) = \Pi_G \circ A(x) = 0, \\ C^G(x) &= C^G \circ \Pi_G(x) = \Pi_G \circ C(x) \preceq 0, \end{aligned} \tag{92}$$

and $F^G(x) = F(x)$.

Next, suppose x^G is feasible for the reduced problem. By the same line of argumentation we get due to Eq. (87):

$$0 = A^G(x^G) = A^G \circ \Pi_G(x) = \Pi_G \circ A(x) = A \circ \Pi_G(x) = A(x). \tag{93}$$

In the same fashion, we compute using Eq. (88):

$$0 \succeq C^G(x^G) = C^G \circ \Pi_G(x) = \Pi_G \circ C(x) \succeq C \circ \Pi_G(x) = C(x). \tag{94}$$

Hence, x^G is feasible for the original problem and $F^G(x^G) = F^G \circ \Pi_G(x^G) = F(x^G)$.

Finally, this implies that the optimal objective values have to agree: Suppose x^* and x_*^G are (G -invariant) optimal solutions for the original and the reduced problem, respectively. Then, $F^G(x^*) = F(x^*)$ and $F(x_*^G) = F^G(x_*^G)$. But since both x^* and x_*^G are feasible for both problems, $F(x_*^G) \neq F(x^*)$ would be a contradiction to the optimality of the solutions. $\square$

E.3 Affine constraints and symmetries

In the remainder of this work, both A and C will be affine maps and originate from a set of points $\mathcal{V}$ that span a polytope $\mathcal{P}$. The symmetry group G leaves $\mathcal{P}$ invariant and hence introduces permutations on $\mathcal{V}$. This will lead naturally to G -equivariance of these functions, as we will see in the following.

To simplify the discussion, we will focus on the function A . We can write the affine function A as

$$A(x) = \sum_{i=1}^N x_i v_i + v_0 \quad (95)$$

Here, $\mathcal{V} := \{v_1, \dots, v_N\} \subset Y$ are the column vectors of the matrix representing the linear part of A and v_0 is its affine part. Suppose G is represented on Y such that it leaves the set $\mathcal{V}$ invariant and fixes v_0 ². Hence, it can be identified with the left action of some subgroup of the symmetric group S_N on the index set $[N] = \{1, \dots, N\}$ via $g \cdot y_i =: y_{\pi_g(i)}$ for some $\pi_g \in S_N$. We can associate a right action on X with this left action by $(x \cdot g)_i := x_{\pi_g^{-1}(i)}$. This action is clearly linear and such that for all $g \in G$:

$$\sum_{i=1}^N x_i (g \cdot v_i) = \sum_{i=1}^N x_i v_{\pi_g(i)} = \sum_{i=1}^N x_{\pi_g^{-1}(i)} v_i = \sum_{i=1}^N (x \cdot g)_i v_i. \quad (96)$$

In particular, the function A is G -equivariant:

$$g \cdot A(x) = \sum_{i=1}^N x_i (g \cdot v_i) + g \cdot v_0 = \sum_{i=1}^N (x \cdot g)_i v_i + v_0 = A(x \cdot g). \quad (97)$$

To make use of Thm. 2, we have to compute the function A^G . Note that Π_G is constant on the every orbit $O \in [N]/G$ and hence $\Pi_G(v_j) =: w_O$ for all $j \in O$:

$$\begin{aligned} \Pi_G \circ A(x) &= \sum_{i=1}^N x_i \Pi_G(v_i) + v_0 \\ &= \sum_{O \in [N]/G} \sum_{j \in O} x_j \Pi_G(v_j) + v_0 \\ &= \sum_{O \in [N]/G} \left(\sum_{j \in O} x_j \right) w_O + v_0 \\ &= \sum_{O \in [N]/G} y_O w_O + v_0, \end{aligned} \quad (98)$$

where in the last step we set $y_O = \sum_{j \in O} x_j$. Finally, we have to turn this into a map on X^G . Note that the right permutation action of G on $X = \mathbb{R}^N$ partitions the standard basis $\{e_1, \dots, e_N\}$ into L orbits $O_1, \dots, O_L$ corresponding to $[N]/G$. Next, the linear spans $X_j = \langle O_j \rangle$ of these orbits provide a decomposition of $X = \bigoplus_j X_j$ and G acts transitively on every orbit. Hence, $\Pi_G(X_j)$ is one-dimensional and $\Pi_G(X) = \bigoplus_j \Pi_G(X_j)$ due to linearity. This implies that $\dim X^G = L = |[N]/G|$. Hence, the y_O are the components of a vector $y \in X^G$ w.r.t. the basis $\tilde{e}_O = \sum_{j \in O} e_j$. Note that if we normalise that basis as $e_O = \frac{1}{|O|} \tilde{e}_O$, then the new components are $\bar{x}_O = \frac{1}{|O|} y_O$, which are exactly the components of $\Pi_G(x)$. Hence, the induced map on X^G is

$$A^G(x) = \sum_{j=1}^L x_j w_j + v_0. \quad (99)$$

²In general, G -equivariance requires that the action preserves the range of A which is a weaker condition.

As stated in the beginning of this subsection, the points $\mathcal{V}$ are the extremal points of a polytope $\mathcal{P}$ and G is as subgroup of the polytope symmetries $\text{Aut}(\mathcal{P})$. We saw that the symmetry reduction corresponds to projecting the vertices of the polytope, and hence the polytope itself, onto the G -invariant subspace. This is equivalent to taking its intersection with this subspace as the following lemma states:

Lemma 3 (Projection with Polytope Symmetries). *Be $G < \text{Aut}(\mathcal{P})$ a subgroup. Then, the G -projection of $\mathcal{P}$ is contained in $\mathcal{P}$, $\Pi_G(\mathcal{P}) \subset \mathcal{P}$. More precisely, $\Pi_G(\mathcal{P}) = \mathcal{P} \cap X^G$.*

Proof. For all $x \in \mathcal{P}$, we have $G \cdot x \subset \mathcal{P}$ and $\Pi_G(x)$ is a convex combination of points in $\mathcal{P}$, hence in $\mathcal{P}$ itself. Moreover, it holds $\mathcal{P} \cap X^G = \Pi_G(\mathcal{P} \cap X^G) \subset \Pi_G(\mathcal{P})$. The converse direction follows since $\Pi_G(\mathcal{P}) \subset X^G$ and $\Pi_G(\mathcal{P}) \subset \mathcal{P}$, thus $\Pi_G(\mathcal{P}) \subset \mathcal{P} \cap X^G$, which shows $\Pi_G(\mathcal{P}) = \mathcal{P} \cap X^G$. $\square$

Finally, we want to remark that for computing the projection of the vertices $\{v_1, \dots, v_M\}$, it is sufficient to compute $\Pi_G(w_O)$ for some representatives w_O of the orbits $O \in \mathcal{V}/G$ since the projection only depends on the orbit.

References

- [1] D. M. Appleby. “Symmetric informationally complete–positive operator valued measures and the extended Clifford group”. In: *Journal of Mathematical Physics* 46.5 (Apr. 19, 2005), p. 052107. DOI: [10.1063/1.1896384](https://doi.org/10.1063/1.1896384) (cit. on pp. 6, 28).
- [2] Christine Bachoc, Dion C. Gijswijt, Alexander Schrijver, and Frank Vallentin. “Invariant semidefinite programs”. In: *Handbook on Semidefinite, Conic and Polynomial Optimization*. Ed. by Miguel F. Anjos and Jean B. Lasserre. International Series in Operations Research & Management Science. Springer US, 2012. DOI: [10.1007/978-1-4614-0769-0](https://doi.org/10.1007/978-1-4614-0769-0) (cit. on p. 6).
- [3] Stephen Boyd and Lieven Vandenberghe. *Convex Optimization*. Seventh printing with corrections. Cambridge University Press, 2009. DOI: [10.1017/CBO9780511804441.007](https://doi.org/10.1017/CBO9780511804441.007) (cit. on pp. 6, 30).
- [4] Sergey Bravyi and David Gosset. “Improved Classical Simulation of Quantum Circuits Dominated by Clifford Gates”. In: *Physical Review Letters* 116.25 (June 20, 2016), p. 250501. DOI: [10.1103/PhysRevLett.116.250501](https://doi.org/10.1103/PhysRevLett.116.250501) (cit. on p. 4).
- [5] Sergey Bravyi and Alexei Kitaev. “Universal quantum computation with ideal Clifford gates and noisy ancillas”. In: *Physical Review A* 71.2 (Feb. 22, 2005), p. 022316. DOI: [10.1103/PhysRevA.71.022316](https://doi.org/10.1103/PhysRevA.71.022316) (cit. on pp. 1, 2).
- [6] Sergey Bravyi, Graeme Smith, and John A. Smolin. “Trading Classical and Quantum Computational Resources”. In: *Physical Review X* 6.2 (June 29, 2016), p. 021043. DOI: [10.1103/PhysRevX.6.021043](https://doi.org/10.1103/PhysRevX.6.021043) (cit. on pp. 2, 4).
- [7] Sergey Bravyi, Dan Browne, Pádraic Calpin, Earl Campbell, David Gosset, and Mark Howard. *Simulation of quantum circuits by low-rank stabilizer decompositions*. July 31, 2018. arXiv: [1808.00128](https://arxiv.org/abs/1808.00128) (cit. on p. 4).
- [8] Earl T. Campbell, Barbara M. Terhal, and Christophe Vuillot. “Roads towards fault-tolerant universal quantum computation”. In: *Nature* 549.7671 (Sept. 2017), pp. 172–179. DOI: [10.1038/nature23460](https://doi.org/10.1038/nature23460) (cit. on p. 1).
- [9] Cecilia Cormick, Ernesto F. Galvão, Daniel Gottesman, Juan Pablo Paz, and Arthur O. Pittenger. “Classicality in discrete Wigner functions”. In: *Physical Review A* 73.1 (Jan. 3, 2006), p. 012301. DOI: [10.1103/PhysRevA.73.012301](https://doi.org/10.1103/PhysRevA.73.012301) (cit. on p. 28).
- [10] Lars Eirik Danielsen. *Database of Self-Dual Quantum Codes*. URL: <http://www.ii.uib.no/~larsed/vncorbits/> (visited on 06/12/2018) (cit. on pp. 12, 28).

- [11] Lars Eirik Danielsen and Matthew G. Parker. “On the classification of all self-dual additive codes over $\text{GF}(4)$ of length up to 12”. In: *Journal of Combinatorial Theory, Series A* 113.7 (Oct. 1, 2006), pp. 1351–1367. DOI: [10.1016/j.jcta.2005.12.004](https://doi.org/10.1016/j.jcta.2005.12.004) (cit. on pp. 12, 28).
- [12] J. H. Dulá and R. V. Helgason. “A new procedure for identifying the frame of the convex hull of a finite collection of points in multidimensional space”. In: *European Journal of Operational Research* 92.2 (July 19, 1996), pp. 352–367. DOI: [10.1016/0377-2217\(94\)00366-1](https://doi.org/10.1016/0377-2217(94)00366-1) (cit. on p. 29).
- [13] Bryan Eastin and Emanuel Knill. “Restrictions on Transversal Encoded Quantum Gate Sets”. In: *Physical Review Letters* 102.11 (Mar. 18, 2009), p. 110502. DOI: [10.1103/PhysRevLett.102.110502](https://doi.org/10.1103/PhysRevLett.102.110502) (cit. on p. 1).
- [14] Matthew B. Elliott, Bryan Eastin, and Carlton M. Caves. “Graphical description of the action of Clifford operators on stabilizer states”. In: *Physical Review A* 77.4 (Apr. 8, 2008), p. 042307. DOI: [10.1103/PhysRevA.77.042307](https://doi.org/10.1103/PhysRevA.77.042307) (cit. on p. 13).
- [15] D. Gross. “Hudson’s theorem for finite-dimensional quantum systems”. In: *Journal of Mathematical Physics* 47.12 (Dec. 1, 2006), p. 122107. DOI: [10.1063/1.2393152](https://doi.org/10.1063/1.2393152) (cit. on pp. 2, 28).
- [16] 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*. Dec. 22, 2017. arXiv: [1712.08628](https://arxiv.org/abs/1712.08628) (cit. on p. 8).
- [17] J. Gubernatis, N. Kawashima, and P. Werner. *Quantum Monte Carlo Methods: Algorithms for Lattice Models*. Cambridge University Press, 2016. DOI: [10.1017/CBO9780511902581](https://doi.org/10.1017/CBO9780511902581) (cit. on p. 3).
- [18] Matthew B Hastings. “Superadditivity of communication capacity using entangled inputs”. In: *Nature Physics* 5.4 (2009), p. 255. DOI: [10.1038/nphys1224](https://doi.org/10.1038/nphys1224) (cit. on p. 22).
- [19] M. Hein, J. Eisert, and H. J. Briegel. “Multiparty entanglement in graph states”. In: *Physical Review A* 69.6 (June 9, 2004). DOI: [10.1103/PhysRevA.69.062311](https://doi.org/10.1103/PhysRevA.69.062311) (cit. on p. 12).
- [20] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, and H.-J. Briegel. *Entanglement in Graph States and its Applications*. Feb. 11, 2006. arXiv: [quant-ph/0602096](https://arxiv.org/abs/quant-ph/0602096) (cit. on p. 12).
- [21] Markus Heinrich and David Gross. *Robustness of Magic and Symmetries of the Stabiliser Polytope*. July 26, 2018. arXiv: [1807.10296](https://arxiv.org/abs/1807.10296) (cit. on p. 13).
- [22] Israel Nathan Herstein. “Jordan Homomorphisms”. In: *Transaction of the American Mathematical Society* 81.2 (1956), pp. 331–341. DOI: [10.2307/1992920](https://doi.org/10.2307/1992920) (cit. on pp. 27, 28).
- [23] Mark Howard and Earl Campbell. “Application of a Resource Theory for Magic States to Fault-Tolerant Quantum Computing”. In: *Physical Review Letters* 118.9 (Mar. 3, 2017), p. 090501. DOI: [10.1103/PhysRevLett.118.090501](https://doi.org/10.1103/PhysRevLett.118.090501) (cit. on pp. 2–6, 14, 24, 25).
- [24] Angela Karanjai, Joel J Wallman, and Stephen D Bartlett. *Contextuality bounds the efficiency of classical simulation of quantum processes*. Feb. 21, 2018. arXiv: [arXiv:1802.07744](https://arxiv.org/abs/1802.07744) (cit. on p. 2).
- [25] Richard Kueng and David Gross. *Qubit stabilizer states are complex projective 3-designs*. Oct. 9, 2015. arXiv: [1510.02767](https://arxiv.org/abs/1510.02767) (cit. on pp. 6, 28).
- [26] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North Holland, 1977. DOI: [0.1137/1022103](https://doi.org/10.1137/1022103) (cit. on p. 9).
- [27] A. Mari and J. Eisert. “Positive Wigner Functions Render Classical Simulation of Quantum Computation Efficient”. In: *Physical Review Letters* 109.23 (Dec. 4, 2012), p. 230503. DOI: [10.1103/PhysRevLett.109.230503](https://doi.org/10.1103/PhysRevLett.109.230503) (cit. on p. 2).

- [28] Gabriele Nebe, Eric M. Rains, and Neil J. A. Sloane. *Self-Dual Codes and Invariant Theory*. Springer Science & Business Media, May 20, 2006. 449 pp. DOI: [10.1007/3-540-30731-1](https://doi.org/10.1007/3-540-30731-1) (cit. on p. 9).
- [29] Maarten Van den Nest, Jeroen Dehaene, and Bart De Moor. “Graphical description of the action of local Clifford transformations on graph states”. In: *Physical Review A* 69.2 (Feb. 24, 2004). DOI: [10.1103/PhysRevA.69.022316](https://doi.org/10.1103/PhysRevA.69.022316) (cit. on p. 12).
- [30] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. 10th. New York, NY, USA: Cambridge University Press, 2011. DOI: [10.1017/CBO9780511976667](https://doi.org/10.1017/CBO9780511976667) (cit. on p. 2).
- [31] Hakop Pashayan, Joel J. Wallman, and Stephen D. Bartlett. “Estimating Outcome Probabilities of Quantum Circuits Using Quasiprobabilities”. In: *Physical Review Letters* 115.7 (Aug. 10, 2015), p. 070501. DOI: [10.1103/PhysRevLett.115.070501](https://doi.org/10.1103/PhysRevLett.115.070501) (cit. on p. 3).
- [32] Patrick Rall. *Fractal Properties of Magic State Distillation*. Aug. 30, 2017. arXiv: [1708.09256](https://arxiv.org/abs/1708.09256) (cit. on p. 9).
- [33] Patrick Rall. *Signed quantum weight enumerators characterize qubit magic state distillation*. Feb. 22, 2017. arXiv: [arXiv:1702.06990](https://arxiv.org/abs/1702.06990) (cit. on p. 9).
- [34] Ben W. Reichardt. *Quantum universality by state distillation*. Aug. 9, 2006. arXiv: [quant-ph/0608085](https://arxiv.org/abs/quant-ph/0608085) (cit. on p. 2).
- [35] D. Schlingemann. *Stabilizer codes can be realized as graph codes*. Nov. 14, 2001. arXiv: [quant-ph/0111080](https://arxiv.org/abs/quant-ph/0111080) (cit. on pp. 12, 13).
- [36] Victor Veitch, Christopher Ferrie, David Gross, and Joseph Emerson. “Negative quasi-probability as a resource for quantum computation”. In: *New Journal of Physics* 14.11 (2012), p. 113011. DOI: [10.1088/1367-2630/14/11/113011](https://doi.org/10.1088/1367-2630/14/11/113011) (cit. on p. 2).
- [37] Victor Veitch, S. A. Hamed Mousavian, Daniel Gottesman, and Joseph Emerson. “The resource theory of stabilizer quantum computation”. In: *New Journal of Physics* 16.1 (2014), p. 013009. DOI: [10.1088/1367-2630/16/1/013009](https://doi.org/10.1088/1367-2630/16/1/013009) (cit. on p. 2).
- [38] Guifré Vidal and Rolf Tarrach. “Robustness of entanglement”. In: *Physical Review A* 59.1 (Jan. 1, 1999), pp. 141–155. DOI: [10.1103/PhysRevA.59.141](https://doi.org/10.1103/PhysRevA.59.141) (cit. on pp. 5, 24).
- [39] S. Virmani, Susana F. Huelga, and Martin B. Plenio. “Classical simulability, entanglement breaking, and quantum computation thresholds”. In: *Physical Review A* 71.4 (Apr. 2005), p. 042328. DOI: [10.1103/PhysRevA.71.042328](https://doi.org/10.1103/PhysRevA.71.042328) (cit. on p. 2).
- [40] Zak Webb. “The Clifford Group Forms a Unitary 3-design”. In: *Quantum Info. Comput.* 16.15 (Nov. 2016), pp. 1379–1400. DOI: [10.26421/QIC16.15-16](https://doi.org/10.26421/QIC16.15-16) (cit. on pp. 6, 28).
- [41] Huangjun Zhu. “Multiqubit Clifford groups are unitary 3-designs”. In: *Physical Review A* 96.6 (Dec. 29, 2017), p. 062336. DOI: [10.1103/PhysRevA.96.062336](https://doi.org/10.1103/PhysRevA.96.062336) (cit. on pp. 6, 28).
- [42] Huangjun Zhu. “Permutation symmetry determines the discrete Wigner function”. In: *Physical Review Letters* 116.4 (2016-01-26), p. 040501. DOI: [10.1103/PhysRevLett.116.040501](https://doi.org/10.1103/PhysRevLett.116.040501) (cit. on p. 2).