

# New techniques for bounding stabilizer rank

Benjamin Lovitz<sup>1</sup> and Vincent Steffan<sup>2</sup>

<sup>1</sup>Institute for Quantum Computing and Department of Applied Mathematics, University of Waterloo, 200 University Ave W, Waterloo, ON, Canada

<sup>2</sup>QMATH, Department of Mathematical Sciences, University of Copenhagen, Universitetsparken 5, 2100 Copenhagen, Denmark

In this work, we present number-theoretic and algebraic-geometric techniques for bounding the stabilizer rank of quantum states. First, we refine a number-theoretic theorem of Moulton to exhibit an explicit sequence of product states with exponential stabilizer rank but constant approximate stabilizer rank, and provide alternate (and simplified) proofs of the best-known asymptotic lower bounds on stabilizer rank and approximate stabilizer rank, up to a log factor. Second, we find the first non-trivial examples of quantum states with multiplicative stabilizer rank under the tensor product. Third, we introduce and study the generic stabilizer rank using algebraic-geometric techniques.

## 1 Introduction

It is of great practical importance to determine the classical simulation cost of quantum computations. Indeed, lower bounds on the simulation cost indicate quantum speedups, while upper bounds can help us to understand the limitations of quantum computation. The *stabilizer rank* is a useful barometer for the computational cost of classically simulating quantum circuits under the stabilizer formalism [1]. A *stabilizer state* is a quantum state in the orbit of a computational basis state under the action of the Clifford group (which is defined in Section 2). For a (pure) quantum state  $\psi$ , we define its *stabilizer rank*, denoted  $\chi(\psi)$ , to be the smallest integer  $r$  for which  $\psi$  can be written as a superposition of  $r$  stabilizer states. The stabilizer rank is motivated by the fact that the classical simulation cost of applying Clifford gates and computational basis measurements to  $\psi$  under current state-of-the-art simulation protocols scales polynomially in the number of Clifford gates and  $\chi(\psi)$  (see Appendix A, and [1, 2, 3, 4]). For a real number  $\delta > 0$ , the  $\delta$ -*approximate stabilizer rank*,  $\chi_\delta(\psi)$ , is defined as the minimum stabilizer rank over all quantum states that are  $\delta$ -close to  $\psi$ , and similarly quantifies the classical simulation cost of approximating the application of Clifford gates and computational basis measurements to  $\psi$  under the stabilizer formalism.

The *T-count* of a quantum state  $\psi$  is the number of *T*-gates needed to prepare  $\psi$  using a circuit consisting only of Clifford+*T*-gates and post-selective computational basis measurements (we define the *T*-gate in Appendix A). It is known that if  $\psi$  has *T*-count  $n$ , then  $\chi(\psi) \leq \chi(T^{\otimes n})$ , where  $T = \frac{1}{\sqrt{2}}(e_0 + e^{i\pi/4}e_1)$  is the so-called *T-state*, and  $e_0, e_1$  are

---

Benjamin Lovitz: [benjamin.lovitz@gmail.com](mailto:benjamin.lovitz@gmail.com)

Vincent Steffan: [sv@math.ku.dk](mailto:sv@math.ku.dk)

the computational basis vectors in  $\mathbb{C}^2$  [1]. It is therefore of particular interest to determine  $\chi(T^{\otimes n})$  and  $\chi_\delta(T^{\otimes n})$ .

Despite the practical importance of the stabilizer rank, few techniques are known for bounding this quantity. In this work, we introduce techniques from number theory and algebraic geometry for bounding the stabilizer rank. In particular, we:

1. Refine a theorem of Moulton on subset-sum representations of exponentially increasing sequences, and use this refinement to prove lower bounds on exact and approximate stabilizer rank. In particular, we:
  - Prove that for any non-stabilizer qubit state  $\psi$ , it holds that  $\chi(\psi^{\otimes n}) = \Omega(n/\log_2 n)$ , and in particular,  $\chi(T^{\otimes n}) \geq \frac{n+1}{4\log_2(n+1)}$ . Our asymptotic scaling matches the best-known lower bound  $\chi(T^{\otimes n}) \geq n/100$  up to a log factor [5].
  - Prove that for any non-stabilizer qubit state  $\psi$ , there exists a constant  $\delta > 0$  for which  $\chi_\delta(\psi^{\otimes n}) \geq \sqrt{n}/(2\log_2 n)$  for all  $n \geq 2$ . In particular, our asymptotic scaling for the  $T$ -state matches the best-known lower bound  $\chi_\delta(T^{\otimes n}) = \Omega(\sqrt{n}/\log_2 n)$  [5].
  - Exhibit, for any fixed  $\delta > 0$ , an explicit sequence of  $n$ -qubit product states of stabilizer rank  $2^n$  (the largest possible) and  $\delta$ -approximate stabilizer rank 1 (the smallest possible).
2. Explicitly construct the first non-trivial examples of quantum states with multiplicative stabilizer rank under the tensor product.
3. Introduce and study the *generic stabilizer rank*, which upper bounds  $\chi(T^{\otimes n})$ , using algebraic-geometric techniques.

In the remainder of this introduction, we expand on points 1, 2, and 3, and identify directions for future work. In Section 2 we review some mathematical preliminaries for this work. In Sections 3, 4, and 5 we prove the results introduced in points 1, 2, and 3, respectively. In Appendix A we review motivation for the stabilizer rank as a measure of the computational cost of classical simulations of quantum circuits.

## 1.1 Lower bounds on stabilizer rank and approximate stabilizer rank

In Section 3, we refine a number-theoretic theorem of Moulton to prove lower bounds on stabilizer rank and approximate stabilizer rank [6]. Let  $[n] = \{1, \dots, n\}$  when  $n$  is a positive integer. For integers  $q \geq 2$  and  $r \geq 1$ , and tuples of non-zero complex numbers

$$\begin{aligned}\alpha &= (\alpha_1, \dots, \alpha_q) \in \mathbb{C}^q \\ \beta &= (\beta_1, \dots, \beta_r) \in \mathbb{C}^r,\end{aligned}$$

we say that  $\beta$  is a *subset-sum representation* of  $\alpha$  if for all  $i \in [q]$  there exists a subset  $R_i \subseteq [r]$  for which  $\sum_{j \in R_i} \beta_j = \alpha_i$ . We refer to the integer  $r$  as the *length* of the subset-sum representation  $\beta \in \mathbb{C}^r$ . For an integer  $2 \leq p \leq q$ , we say that  $\alpha \in \mathbb{C}^q$  has an *exponentially increasing subsequence* of length  $p$  if there exists  $i_1, \dots, i_p \in [q]$  for which

$$|\alpha_{i_{j+1}}| \geq 2|\alpha_{i_j}| \quad \text{for all } j \in [p].$$

Moulton's theorem states that any subset-sum representation of a  $q$ -tuple containing the subsequence  $(1, 2, 4, \dots, 2^{p-1})$  has length at least  $p/\log_2 p$  [6]. We refine this result to

prove that the same bound holds for any  $q$ -tuple that contains an exponentially increasing subsequence of length  $p$  (Theorem 3.1).

Since stabilizer states have coordinates in  $\{0, \pm 1, \pm i\}$  in the computational basis (see Section 2), any decomposition of a state  $\psi$  into a superposition of  $r$  stabilizer states can be converted into a length- $4r$ -subset-sum representation of the coordinates of  $\psi$ . It follows that if the coordinates of  $\psi$  contain an exponentially increasing subsequence of length  $p$ , then  $\chi(\psi) \geq p/(4 \log_2 p)$  (Theorem 3.2). In particular, since  $T$  is Clifford-equivalent to the  $H$ -state  $H \propto e_0 + \frac{1}{\sqrt{2-1}}e_1$ , and the coordinates of  $H^{\otimes n}$  contain an exponentially increasing subsequence of length  $n+1$ , we obtain  $\chi(T^{\otimes n}) \geq \frac{n+1}{4 \log_2(n+1)}$ . By a similar argument, we prove that  $\chi(\psi^{\otimes n}) = \Omega(n/\log_2 n)$  for any non-stabilizer qubit state  $\psi$  (Theorem 3.2).

We further use Theorem 3.1, along with standard concentration inequalities for the binomial distribution, to prove that for any non-stabilizer qubit state  $\psi$  there exists a constant  $\delta > 0$  for which it holds that  $\chi_\delta(\psi^{\otimes n}) \geq \sqrt{n}/(2 \log_2 n)$  for all  $n \geq 2$  (Theorem 3.4).

Very recently, Peleg et al. obtained similar results: They proved that  $\chi(T^{\otimes n}) \geq n/100$ , and that there exists  $\delta > 0$  for which  $\chi_\delta(T^{\otimes n}) = \Omega(\sqrt{n}/\log_2 n)$  [5]. Asymptotically, our bounds match theirs up to a log factor, and we suggest that our proof technique is much simpler. While both of our bounds follow quite quickly from our refinement of Moulton's theorem mentioned above, the two bounds of Peleg et al. use two different approaches from the analysis of boolean functions and complexity theory: For their lower bound on  $\chi(T^{\otimes n})$ , they analyze directional derivatives of quadratic polynomials, and for their lower bound on  $\chi_\delta(T^{\otimes n})$ , they use Razborov-Smolensky low-degree polynomial approximations and correlation bounds against the majority function [7, 8, 9]. It is interesting that the vastly different approaches of ours and Peleg et al. yield such similar results.

As a further application of our refinement of Moulton's theorem, we explicitly construct a sequence of  $n$ -qubit product states  $\psi^{\otimes n}$  for which it holds that  $\chi(\psi^{\otimes n}) \geq \frac{2^n}{4n}$  and  $\chi_\delta(\psi^{\otimes n}) = \mathcal{O}(1)$  for any  $\delta > 0$ , simply by writing down a product state with exponentially increasing coordinate amplitudes. Using different techniques, in Proposition 3.7 we construct a sequence of  $n$ -qubit product states  $\psi^{\otimes n}$  for which  $\chi(\psi^{\otimes n}) = 2^n$  (the largest possible) and  $\chi_\delta(\psi^{\otimes n}) = 1$  (the smallest possible). These results lie in contrast to the situation for other notions of rank, in which it is a difficult open problem to explicitly construct sequences of states of near-maximal rank. For example, the maximum *border rank*, a relevant notion of rank in classical complexity theory, of a quantum state in three local spaces of (affine) dimensions  $d$ , is  $\lceil \frac{d^3}{3d-2} \rceil$  for all  $d \neq 3$ , whereas the largest border rank of any known explicit sequence of states in this space is only linear in  $d$  (see [10] for the largest known border rank and [11] for a general introduction to the topic).

## 1.2 States with multiplicative stabilizer rank under the tensor product

It is a standard fact that the stabilizer rank is *sub-multiplicative* under the tensor product, i.e.  $\chi(\psi \otimes \psi) \leq \chi(\psi)^2$  for any quantum state  $\psi$  [12, Section 2.1.3]. In [12, Section 4.4] it was remarked that there are no known examples of quantum states  $\psi$  of stabilizer rank greater than one for which equality holds. In Section 4, we explicitly construct two-qubit states  $\psi$  for which  $\chi(\psi) = 2$  and  $\chi(\psi \otimes \psi) = 4$ . This is the smallest possible example of such a state, since for any single-qubit state  $\phi$  it holds that  $\chi(\phi \otimes \phi) \leq 3$ .

## 1.3 Generic stabilizer rank

For any positive integer  $n$ , all but finitely many qubit states  $\psi$  (up to phase) maximize  $\chi(\psi^{\otimes n})$  (Fact 5.1). This motivates us to define the  $n$ -th *generic stabilizer rank*, denoted  $\chi_n$ , to be the maximum stabilizer rank of any state of the form  $\psi^{\otimes n}$ . In Section 5, we

prove new bounds on  $\chi_n$ , along with some useful reductions for studying this quantity. In Proposition 5.2 we modestly improve the best-known upper bound on  $\chi_n$ , recently obtained by Qassim et al., from  $\mathcal{O}((n+1)2^{n/2})$  to  $\mathcal{O}(2^{n/2})$  [4, Theorem 2]. In Propositions 5.3 and 5.4 we prove two useful reductions for studying  $\chi_n$ , namely, that there must exist a single set of  $\chi_n$  stabilizer states that span the symmetric subspace, and that it suffices to work over the real numbers. In Proposition 5.5 we introduce a technique for upper bounding  $\chi_n$  when upper bounds on  $\chi(\psi^{\otimes n})$  are known for sufficiently many (linear in  $n$ ) pairwise non-collinear qubit states  $\psi$ . In Proposition 5.6 we compute an upper bound on the (finite) number of qubit states  $\psi$  (up to phase) for which  $\chi(\psi^{\otimes n}) < \chi_n$ .

## 1.4 Directions for future work

We believe that our work opens the door for new approaches on questions related to the stabilizer rank. Here, we present two of the most promising ones.

### 1.4.1 Lower bounds on stabilizer rank via the $T$ -count

Recall that for any quantum state  $\psi_n$  of  $T$ -count  $n$ , it holds that  $\chi(T^{\otimes n}) \geq \chi(\psi_n)$  [1]. Also note that, from the proof of Theorem 3.2, if the smallest subset-sum representation of  $\psi_n$  has size at least  $a_n \in \mathbb{N}$ , then  $\chi(\psi_n) \geq \frac{1}{4}a_n$ . This suggests the following technique for obtaining lower bounds on  $\chi(T^{\otimes n})$  (based on a technique introduced in [1]): Find a sequence of states  $\psi_n$  of  $T$ -count  $n$  with no subset-sum representation of size less than  $a_n$ , where  $a_n$  grows suitably quickly in  $n$ . Indeed, this is the technique we use to obtain our linear lower bound in Theorem 3.2: We find a sequence of states  $\psi_n \propto (e_0 + \frac{i}{\sqrt{2-1}}e_1)^{\otimes n}$  of  $T$ -count  $n$  and no subset-sum representation of size less than  $\frac{n+1}{\log_2(n+1)}$ , where the latter property is ensured from the fact that  $\psi_n$  contains an exponentially increasing sequence of length  $n+1$  (see Theorem 3.1). It would be interesting to see if this technique can be used to obtain super-linear lower bounds on  $\chi(T^{\otimes n})$ . Unfortunately, by [13, Proposition 5.8], any state of  $T$ -count  $n$  can have an exponentially increasing sequence of length at most  $O(n)$ , so one would need to find another way to lower bound the size of a subset-sum representation.

### 1.4.2 Bounds on generic stabilizer rank

In Section 5 we prove several reductions for studying the generic stabilizer rank  $\chi_n$ , but only manage to modestly improve the best-known bounds on this quantity. We ask whether stronger bounds can be obtained from our reductions.

## Acknowledgments

We thank the second referee for the key ideas in the proof of Proposition 3.7. We thank Gerry Myerson for pointing us to the work of Moulton [6]. BL thanks Kieran Mastel and William Slofstra for helpful discussions. VS thanks Daniel Stilck França and Matthias Christandl for helpful discussions. BL acknowledges financial support from the University of Waterloo and the Government of Ontario through an Ontario Graduate Scholarship. VS acknowledges financial support from VILLUM FONDEN via the QMATH Centre of Excellence (Grant No. 10059).

## 2 Background

For a complex vector space  $\mathcal{V}$ , let  $\mathcal{S}(\mathcal{V})$  be the set of unit vectors in  $\mathcal{V}$  (with respect to the Euclidean norm), let  $U(\mathcal{V})$  be the set of unitary operators on  $\mathcal{V}$ , and let  $\mathbb{P}(\mathcal{V})$  be the set of one-dimensional linear subspaces of  $\mathcal{V}$ . In precise terms, a pure quantum state is a unit vector modulo phase, i.e. an element of  $\mathcal{S}(\mathcal{V})/U(\mathbb{C})$ . However, to match historical notation in quantum information, we will define a (*pure, quantum*) *state* to be an element of  $\mathcal{S}(\mathcal{V})$ , and define a (*pure, quantum*) *state mod phase* to be an element of  $\mathcal{S}(\mathcal{V})/U(\mathbb{C})$ . Under the canonical identification between this quotient and  $\mathbb{P}(\mathcal{V})$ , which sends a unit vector to its span, we also refer to elements of  $\mathbb{P}(\mathcal{V})$  as states mod phase. This endows the set of states mod phase (and relevant subsets) with the structure of an algebraic variety. We will use this structure in Section 5 to study the generic stabilizer rank.

For a vector  $\psi \in \mathcal{V}$ , let  $[\psi] \in \mathbb{P}(\mathcal{V})$  be the subspace spanned by  $\psi$  (not to be confused with  $[n] := \{1, \dots, n\}$  when  $n$  is a positive integer). We say that two non-zero vectors  $\psi, \phi \in \mathcal{V}$  are *collinear* if  $[\psi] = [\phi]$ . For a subset  $X \subseteq \mathbb{P}\mathcal{V}$ , let  $\hat{X} \subseteq \mathcal{V}$  be the affine cone over  $X$ , i.e.  $\hat{X} = \{\psi \in \mathcal{V} : [\psi] \in X\} \cup \{0\}$ . For a positive integer  $n$ , let  $\mathbb{P}^n = \mathbb{P}(\mathbb{C}^{n+1})$  and  $\mathcal{V}_n = (\mathbb{C}^2)^{\otimes n}$ . We refer to the individual copies of  $\mathbb{C}^2$  that make up  $\mathcal{V}_n$  as *subsystems*. We refer to elements of  $\mathcal{V}_n$  as *tensors* to emphasize the multipartite structure of  $\mathcal{V}_n$ . Let  $S^n(\mathbb{C}^2) \subseteq \mathcal{V}_n$  be the *symmetric subspace*: the linear subspace of tensors that are invariant under permutation of the subsystems. Note that  $\mathbb{P}(\mathcal{V}_n) = \mathbb{P}^{2^n-1}$ .

For a positive integer  $n$ , let  $\text{Pauli}_n \subseteq U(\mathcal{V}_n)$  be the *Pauli group*, the group generated by all  $n$ -fold tensor products of elements of the set  $\{X, Z, i\mathbb{1}_2\} \subseteq U(\mathbb{C}^2)$ , where

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

and  $\mathbb{1}_k$  is the identity matrix in  $U(\mathbb{C}^k)$  for any positive integer  $k$ . The *Clifford group*, denoted  $\text{Cliff}_n \subseteq U(\mathcal{V}_n)$ , is the normalizer of the Pauli group in  $U(\mathcal{V}_n)$ . The Clifford group is generated by all tensor products of elements of the set  $\{H, S, CNOT\}$ , along with global phase gates in  $U(\mathbb{C})$ , where

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad \text{and} \quad CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

A quantum state  $\psi \in \mathcal{S}(\mathcal{V})$  is called a *stabilizer state* if  $\psi = Ue_0^{\otimes n}$  for some  $U \in \text{Cliff}_n$ . Let  $\text{Stab}_n = \text{Cliff}_n e_0^{\otimes n}$  be the set of stabilizer states, and let  $\check{\text{Stab}}_n = \{[\psi] : \psi \in \text{Stab}_n\} \subseteq \mathbb{P}^{2^n-1}$  be the set of stabilizer states mod phase. It is well known that a state  $\psi \in \mathcal{S}(\mathcal{V}_n)$  is a stabilizer state if and only if

$$\psi \propto \sum_{x \in A} i^{l(x)} \cdot (-1)^{q(x)} \cdot e_x \tag{1}$$

for some affine linear subspace  $A \subseteq \mathbb{F}_2^n$ , linear form  $l: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ , and quadratic form  $q: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$  [14, 15]. Here and throughout, we define  $e_x := e_{x_1} \otimes \dots \otimes e_{x_n}$  when  $x \in \mathbb{F}_2^n$ .

The *stabilizer rank* of a state  $\psi \in \mathcal{S}(\mathcal{V}_n)$ , denoted  $\chi(\psi)$ , is the smallest integer  $r$  for which

$$\psi = \sum_{i=1}^r c_i \sigma_i$$

for some complex numbers  $c_i \in \mathbb{C}$  and stabilizer states  $\sigma_i \in \text{Stab}_n$ . We denote the set of states mod phase of stabilizer rank at most  $r$  by  $\Sigma_r(\check{\text{Stab}}_n) \subseteq \mathbb{P}^{2^n-1}$  ( $\Sigma_r(\cdot)$  denotes

the  $r$ -th secant variety, see [16, Example 8.5]). Note that  $\check{\text{Stab}}_n$  is *non-degenerate*, i.e.  $\text{span}(\check{\text{Stab}}_n) = \mathbb{P}^{2^n-1}$ .

We also have an approximate version of stabilizer rank. For a positive real number  $\delta > 0$  and state  $\psi \in \mathcal{S}(\mathcal{V}_n)$ , we define the  $\delta$ -approximate stabilizer rank of  $\psi$ , denoted  $\chi_\delta(\psi)$ , as

$$\chi_\delta(\psi) = \min_{\phi \in \mathcal{S}(\mathcal{V}_n)} \{ \chi(\phi) : \|\phi - \psi\| \leq \delta \}.$$

We say a quantum state  $\psi \in \mathcal{S}(\mathcal{V}_n)$  is *real* if  $\psi$  is proportional to a state with only real coordinates in the computational basis. A quantum state  $\psi$  is a real stabilizer state if and only if it can be written in the form (1) with  $l = 0$ . The set of real stabilizer states in  $\mathcal{S}(\mathcal{V}_n)$ , which we denote by  $\text{Stab}_n^{\mathbb{R}}$ , is precisely the orbit of  $e_0^{\otimes n}$  under the group generated by  $U(\mathbb{C})$ ,  $H$  and  $CNOT$  [14]. We denote by  $\check{\text{Stab}}_n^{\mathbb{R}}$  the set of real stabilizer states mod phase. For a quantum state  $\psi \in \mathcal{S}(\mathcal{V}_n)$ , we define the *real stabilizer rank* of  $\psi$ , denoted  $\chi^{\mathbb{R}}(\psi)$ , to be the smallest integer  $r$  for which  $\psi$  can be written as a (complex) superposition of  $r$  real stabilizer states.

We close this section by computing the number of stabilizer states and real stabilizer states mod phase, which we will use in Section 5 to upper bound the number of states mod phase of sub-generic rank. It is a standard fact that there are  $\binom{n}{k}_2$  distinct  $k$ -dimensional linear subspaces of  $\mathbb{F}_2^n$ , where

$$\binom{n}{k}_2 = \prod_{i=0}^{k-1} \frac{2^{n-i} - 1}{2^{k-i} - 1}$$

is the *Gaussian binomial coefficient* (see e.g. [17]). Since there are  $2^{n-k}$  distinct affine translations of a  $k$ -dimensional linear subspace of  $\mathbb{F}_2^n$ , it follows that there are  $\binom{n}{k}_2 2^{n-k}$  distinct affine linear subspaces of dimension  $k$ . For each index  $k \in [n]$  and each  $k$ -dimensional affine subspace  $A \subseteq \mathbb{F}_2^n$ , there are  $2^{k(k+1)/2}$  distinct quadratic forms on  $A$  and  $2^k$  distinct linear functions on  $A$ . It follows that

$$\begin{aligned} |\check{\text{Stab}}_n| &= 2^n \sum_{k=1}^n \binom{n}{k}_2 2^{k(k+1)/2} \\ &= 2^n \prod_{k=1}^n (2^k + 1), \end{aligned}$$

where the second line follows from the Gaussian binomial theorem (see e.g. [17]). Similarly,

$$|\check{\text{Stab}}_n^{\mathbb{R}}| = 2^n \sum_{k=1}^n \binom{n}{k}_2.$$

The quantity  $|\check{\text{Stab}}_n|$  was previously computed in [18, Corollary 21] using a different proof technique.

### 3 Lower bounds on stabilizer rank and approximate stabilizer rank

In this section, we refine a number-theoretic theorem of Moulton, and use this to prove lower bounds on the stabilizer rank and approximate stabilizer rank. Recall the definitions of exponentially increasing subsequences and subset-sum representations given in Section 1.1. Moulton proved that any subset-sum representation of a  $q$ -tuple containing the subsequence  $(1, 2, 4, \dots, 2^{p-1})$  has length at least  $p/\log_2 p$  [6]. In Section 3.1, we refine this result to

prove that the same bound holds for any  $q$ -tuple containing an exponentially increasing subsequence of length  $p$  (Theorem 3.1). In Section 3.2 we use our refinement to prove that any quantum state whose coordinates contain an exponentially increasing subsequence of length  $p$  has stabilizer rank at least  $p/(4\log_2 p)$  (Theorem 3.2). We then use this result to explicitly construct a sequence of product states of exponential stabilizer rank, to prove that  $\chi(T^{\otimes n}) \geq \frac{n+1}{4\log_2(n+1)}$ , and to prove that  $\chi(\psi^{\otimes n}) = \Omega(n/\log_2 n)$  for any non-stabilizer qubit state  $\psi$ . In Section 3.3 we use our refinement of Moulton's theorem to prove that, for any non-stabilizer qubit state  $\psi$ , there exists  $\delta > 0$  for which  $\chi_\delta(\psi^{\otimes n}) \geq \sqrt{n}/(2\log_2 n)$  for all  $n \in \mathbb{N}$ . In Section 3.4 we use our refinement of Moulton's theorem, as well as independent field-theoretic techniques, to construct explicit sequences of product states of exponential stabilizer rank but constant approximate stabilizer rank.

### 3.1 A refinement of Moulton's theorem

**Theorem 3.1** (Refinement of Theorem 1 in [6]). *Let  $2 \leq p \leq q$  be integers, and let  $\alpha \in \mathbb{C}^q$  be a  $q$ -tuple of non-zero complex numbers. If  $\alpha$  contains an exponentially increasing subsequence of length  $p$ , then any subset-sum representation of  $\alpha$  has length at least  $p/\log_2(p)$ .*

*Proof.* It suffices to consider the case  $p = q$  and  $2|\alpha_i| \leq |\alpha_{i+1}|$  for all  $i \in [q-1]$ . Let  $\beta \in \mathbb{C}^r$  be a subset-sum representation of  $\alpha$ . Then for each  $i \in [q]$ , there exists  $c_i \in \{0, 1\}^r$  such that  $\alpha_i = \beta^T c_i$ . Suppose that, for some  $u_1, \dots, u_q, v_1, \dots, v_q \in \{0, 1\}$ , we have

$$\sum_{i=1}^q u_i c_i = \sum_{i=1}^q v_i c_i.$$

Applying  $\beta^T$  to both sides gives

$$\sum_{i=1}^q u_i \alpha_i = \sum_{i=1}^q v_i \alpha_i.$$

It follows that  $u_i = v_i$  for all  $i \in [q]$ . Indeed, it suffices to prove that  $|\alpha_{i+1}| > |\alpha_1 + \dots + \alpha_i|$  for all  $i \in [q-1]$ , which in turn can be easily verified by an inductive argument. By assumption,  $|\alpha_2| > |\alpha_1|$ , and by induction,

$$|\alpha_1 + \dots + \alpha_i| \leq |\alpha_1 + \dots + \alpha_{i-1}| + |\alpha_i| < 2|\alpha_i| \leq |\alpha_{i+1}|.$$

The remainder of the proof is identical to that of [6]. There are at most  $2^q - 1$  choices of  $u_1, \dots, u_q \in \{0, 1\}$ , excluding the case  $u_1 = \dots = u_q = 1$ . For each of these choices, the sum  $\sum_{i=1}^q u_i c_i$  can take one of  $q^r - 1$  possible choices in  $\{0, 1, \dots, q-1\}^{\times r}$  (the choice  $(q-1, q-1, \dots, q-1)^T$  is excluded since the  $u_i$  are not all equal to 1). Since each choice of  $u_1, \dots, u_q$  yields a different vector, we must have  $q^r - 1 \geq 2^q - 1$ , i.e.  $r \geq q/\log_2(q)$ .  $\square$

### 3.2 Lower bounds on stabilizer rank

In this subsection we use Theorem 3.1 to prove lower bounds on stabilizer rank.

**Theorem 3.2.** *Let  $p \geq 2$  be an integer, and let  $\psi \in \mathcal{S}(\mathcal{V}_n)$  be a quantum state. If the coordinates of  $\psi$  contain an exponentially increasing subsequence of length  $p$ , then  $\chi(\psi) \geq p/(4\log_2 p)$ .*

*Proof.* Let  $r = \chi(\psi)$ , let  $x_1, \dots, x_p \in \mathbb{F}_2^n$  be such that  $|\psi_{x_i}| \leq 2|\psi_{x_{i+1}}|$  for all  $i \in [p-1]$ , and let  $\alpha = (\psi_{x_1}, \dots, \psi_{x_p}) \in \mathbb{C}^p$ . Without loss of generality, there exist complex numbers  $\{c_i : i \in [r]\} \subseteq \mathbb{C}$  and stabilizer states  $\{\sigma_i : i \in [r]\} \subseteq \text{Stab}_n$  such that for all  $i \in [r]$ , every coordinate of  $\sigma_i$  is an element of  $\{0, \pm 1, \pm i\}$ , and  $\psi = \sum_{i=1}^r c_i \sigma_i$ . Let

$$S = (\sigma_1, \dots, \sigma_r) \in \{0, \pm 1, \pm i\}^{\{0,1\}^n \times r}$$

and

$$c = (c_1, \dots, c_r) \in \mathbb{C}^r,$$

so that  $Sc = \psi$ . In particular, there exists a  $p \times r$  submatrix  $T$  of  $S$  for which  $Tc = \alpha$ . Let  $T_1, T_2, T_3, T_4 \in \{0, 1\}^{p \times r}$  be such that

$$T = T_1 - T_2 + i(T_3 - T_4).$$

Then

$$(T_1, T_2, T_3, T_4)(c, -c, ic, -ic)^T = Tc = \alpha,$$

so  $(c, -c, ic, -ic)$  is a subset-sum representation of  $\alpha$ . It follows from Theorem 3.1 that  $4r \geq p/(\log_2 p)$ . This completes the proof.  $\square$

Theorem 3.2 also implies the following lower bound on  $\chi(T^{\otimes n})$ , and more generally, on  $\chi(\psi^{\otimes n})$  for any non-stabilizer qubit state  $\psi$ .

**Corollary 3.3.** *For any state  $\psi \in \mathcal{S}(\mathbb{C}^2)$  that is not a stabilizer state,  $\chi(\psi^{\otimes n}) = \Omega(n/\log_2 n)$ . In particular,*

$$\chi(T^{\otimes n}) \geq \frac{n+1}{4\log_2(n+1)}.$$

*Proof.* Since  $\psi$  is not a stabilizer state, there exists  $\alpha \in \mathbb{C}$  with  $|\alpha| > 1$  for which  $\tau := \frac{1}{\sqrt{1+|\alpha|^2}}(e_0 + \alpha e_1)$  is in the Cliff<sub>1</sub>-orbit of  $\psi$ . Indeed, by adjusting the global phase of  $\psi$  we may assume  $\psi = \frac{1}{\sqrt{1+|\beta|^2}}(e_0 + \beta e_1)$  for some complex number  $\beta \in \mathbb{C}^\times \setminus \{0, \pm 1, \pm i\}$ , because  $\psi$  is not a stabilizer state. If  $|\beta| > 1$  we are done, and if  $|\beta| < 1$  then let  $\tau = X\psi$ . If  $|\beta| = 1$  then either  $H\psi$  or  $XH\psi$  must have the desired form. When  $\psi = T$ , we can take  $\tau = XH\psi \propto e_0 + \frac{i}{\sqrt{2-1}}e_1$ .

Since  $|\alpha| > 1$ , there exists  $k \in \mathbb{N}$  for which  $|\alpha|^k \geq 2$ . (When  $\psi = T$ , we can take  $k = 1$ .) Now observe that the complex numbers  $1, \alpha^k, \alpha^{2k}, \dots, \alpha^{\lfloor n/k \rfloor k}$  all appear as coordinates of  $\psi^{\otimes n}$ . By Theorem 3.2, it follows that

$$\chi(\psi^{\otimes n}) \geq \frac{\lfloor n/k \rfloor + 1}{4\log_2(\lfloor n/k \rfloor + 1)}.$$

This completes the proof.  $\square$

### 3.3 Lower bounds on approximate stabilizer rank

In this subsection, we use Theorem 3.1 to prove that, for any non-stabilizer qubit state  $\psi$ , there exists a constant  $\delta > 0$  for which  $\chi_\delta(\psi^{\otimes n}) \geq \sqrt{n}/(2\log_2 n)$ .

**Theorem 3.4.** *For any non-stabilizer qubit state  $\psi \in \mathcal{S}(\mathbb{C}^2)$ , there exists a constant  $\delta > 0$  such that, for every integer  $n \geq 2$ ,*

$$\chi_\delta(\psi^{\otimes n}) \geq \frac{\sqrt{n}}{2 \log_2 n}.$$

*Proof.* As in the proof of Corollary 3.3, since  $\psi$  is not a stabilizer state, there exists  $\alpha \in \mathbb{C}$  with  $|\alpha| > 1$  for which  $\tau := \frac{1}{\sqrt{1+|\alpha|^2}}(\mathbf{e}_0 + \alpha \mathbf{e}_1) \in \text{Cliff}_1(\psi)$ . Let  $\beta = \frac{1}{\sqrt{1+|\alpha|^2}}$  and  $\gamma = \frac{\alpha}{\sqrt{1+|\alpha|^2}}$ , so  $\tau = \beta \mathbf{e}_0 + \gamma \mathbf{e}_1$ . Since the (approximate) stabilizer rank is unchanged under  $\text{Cliff}_n$ , it suffices to lower bound the approximate stabilizer rank of  $\tau^{\otimes n}$ .

Let  $k \in \mathbb{N}$  be the smallest integer for which  $|\alpha|^k > 2$ , and let  $\lambda = \frac{2}{|\alpha|^k}$ . If  $\psi = T$ , then we can take  $\alpha = \frac{1}{\sqrt{2-1}}$  and  $k = 1$ . Let  $\phi \in \mathcal{S}(\mathcal{V}_n)$  be a state, and let  $S \subseteq [n]$  be the set of integers  $p \in [n]$  that satisfy the following two properties:

1.  $|\gamma|^{2n} - k \lceil \sqrt{n} \rceil \leq p \leq |\gamma|^{2n} + k \lceil \sqrt{n} \rceil$ .
2. For all  $x \in \mathbb{F}_2^n$  of Hamming weight  $|x| = p$ ,

$$|\tau_x^{\otimes n} - \phi_x| \geq \left( \frac{1-\lambda}{1+\lambda} \right) |\beta|^{n-p} |\gamma|^p.$$

By the De Moivre-Laplace Theorem, there exists a constant  $\tilde{c} > 0$  (which may depend on  $|\alpha|$ , but does not depend on  $n$ ) for which

$$\binom{n}{p} |\beta^{n-p} \gamma^p|^2 \geq \tilde{c} / \sqrt{n}$$

for all  $p \in [n]$  that satisfy property 1 (see [19, Section VII, Theorem 1] or [5, Claim 4.6]). Let

$$c = \left( \frac{1-\lambda}{1+\lambda} \right)^2 \tilde{c},$$

so that

$$\left( \frac{1-\lambda}{1+\lambda} \right)^2 \binom{n}{p} |\beta^{n-p} \gamma^p|^2 \geq c / \sqrt{n}$$

for all  $p \in S$ . It follows that

$$\|\tau^{\otimes n} - \phi\|^2 \geq \sum_{p \in S} \left( \frac{1-\lambda}{1+\lambda} \right)^2 \binom{n}{p} |\beta^{n-p} \gamma^p|^2 \geq |S| \frac{c}{\sqrt{n}}.$$

Let  $\delta = \sqrt{ck}$ , and suppose that  $\|\tau^{\otimes n} - \phi\| \leq \delta$ . Then  $|S| \leq k\sqrt{n}$ . Let  $P \subseteq [n]$  be the set of integers  $p \in [n]$  that satisfy property 1 but do not satisfy property 2. Observe that  $|P| \geq k \lceil \sqrt{n} \rceil$ , because there are at least  $2k \lceil \sqrt{n} \rceil$  integers that satisfy property 1, and  $|S| \leq k\sqrt{n}$ . By our definition of  $P$ , for each  $p \in P$  there exists  $x_p \in \mathbb{F}_2^n$  with  $|x_p| = p$  and

$$|\tau_{x_p}^{\otimes n} - \phi_{x_p}| \leq \left( \frac{1-\lambda}{1+\lambda} \right) |\beta|^{n-p} |\gamma|^p. \quad (2)$$

For any  $p, q \in P$  with  $p < q$ , it holds that

$$\begin{aligned}
\frac{|\phi_{x_q}|}{|\phi_{x_p}|} &= \frac{|\phi_{x_q} - \tau_{x_q}^{\otimes n} + \tau_{x_q}^{\otimes n}|}{|\phi_{x_p} - \tau_{x_p}^{\otimes n} + \tau_{x_p}^{\otimes n}|} \\
&\geq \frac{|\tau_{x_q}^{\otimes n}| - |\phi_{x_q} - \tau_{x_q}^{\otimes n}|}{|\tau_{x_p}^{\otimes n}| + |\phi_{x_p} - \tau_{x_p}^{\otimes n}|} \\
&\geq \frac{(1 - \frac{1-\lambda}{1+\lambda})|\beta^{n-q}\gamma^q|}{(1 + \frac{1-\lambda}{1+\lambda})|\beta^{n-p}\gamma^p|} \\
&= \lambda|\alpha|^{q-p},
\end{aligned}$$

where the first line is trivial, the second is the triangle inequality, the third follows from (2) and the fact that  $|\tau_x^{\otimes n}| = |\beta^{n-|x|}\gamma^{|x|}|$  for all  $x \in \mathbb{F}_2^n$ , and the fifth is obvious. In particular, if  $q - p \geq k$ , then  $\frac{|\phi_{x_q}|}{|\phi_{x_p}|} \geq 2$ . Since  $|P| \geq k\lceil\sqrt{n}\rceil$ , there exists a subset  $Q \subseteq P$  of size  $|Q| \geq \sqrt{n}$  for which  $p - q \geq k$  for all  $p, q \in Q$  with  $p < q$ . By Theorem 3.2,

$$\chi(\phi) \geq \frac{\sqrt{n}}{2 \log_2(n)}.$$

This completes the proof.  $\square$

We note that, using [19, Section VII, Theorem 1] and a similar proof as above, slight improvements to the above bound can be obtained if  $\delta$  is allowed to decay in  $n$ .

### 3.4 Product states with exponential stabilizer rank and constant approximate stabilizer rank

It is not difficult to prove that for any  $\delta > 0$ , there exist product states  $\psi_n \in \mathcal{S}(\mathcal{V}_n)$  with  $\chi(\psi_n) = 2^n$  (the largest possible) and  $\chi_\delta(\psi_n) = 1$  (the smallest possible). Indeed, generic product states have stabilizer rank  $2^n$  (see the discussion following Proposition 5.3), so a  $\delta$ -ball around any product stabilizer state (e.g.  $e_0^{\otimes n}$ ) will contain (many) product states of stabilizer rank  $2^n$ . In this subsection, we will explicitly construct examples of such product states. In Corollary 3.5 we use Theorem 3.2 to provide a simple proof that a particular sequence of product states has stabilizer rank at least  $\frac{2^n}{4n}$  and  $\delta$ -approximate stabilizer rank  $\mathcal{O}(1)$ . In Proposition 3.7, we use independent, field-theoretic techniques to construct a different sequence of product states of stabilizer rank  $2^n$  and  $\delta$ -approximate stabilizer rank 1. The following lemma will allow us to upper-bound the  $\delta$ -approximate stabilizer rank of product states with exponentially increasing coordinates.

**Lemma 3.5.** *Let  $\delta > 0$  be a positive real number. For a complex number  $\theta \in \mathbb{C}$  and natural number  $n \in \mathbb{N}$ , let*

$$\psi_n^\theta = \sqrt{\frac{|\theta|^2 - 1}{|\theta|^{2^{n+1}} - 1}} \bigotimes_{i=1}^n (e_0 + \theta^{2^{i-1}} e_1) \in \mathcal{S}(\mathcal{V}_n).$$

*If  $|\theta| > 1$ , then  $\chi_\delta(\psi_n^\theta) = \mathcal{O}(1)$ . Furthermore, there exists a positive real number  $\lambda_\delta > 0$  such that for any  $\theta \in \mathbb{C}$  with  $|\theta| > \lambda_\delta$ , it holds that  $\chi_\delta(\psi_n^\theta) = 1$  for all  $n \in \mathbb{N}$ .*

*Proof.* For each  $i \in \{0, 1, \dots, 2^n - 1\}$ , let

$$c_i = \sum_{j=0}^i |\theta|^{2j} = \frac{|\theta|^{2i+2} - 1}{|\theta|^2 - 1},$$

and observe that for any positive integer  $k$ , the tensor  $\phi_{n,k}^\theta \in \mathcal{V}_n$  obtained by setting all but the  $k$  largest coordinates of  $\psi_n^\theta$  to zero satisfies

$$\begin{aligned}
\left\| \psi_n^\theta - \frac{\phi_{n,k}^\theta}{\|\phi_{n,k}^\theta\|} \right\|^2 &= \left\| \frac{1}{\sqrt{c_{2^n-1}}} \sum_{i=0}^{2^n-1} \theta^i e_i - \frac{1}{\sqrt{c_{2^n-1} - c_{2^n-k-1}}} \sum_{i=2^n-k}^{2^n-1} \theta^i e_i \right\|^2 \\
&= \frac{c_{2^n-k-1}}{c_{2^n-1}} + \left( \frac{1}{\sqrt{c_{2^n-1}}} - \frac{1}{\sqrt{c_{2^n-1} - c_{2^n-k-1}}} \right)^2 (c_{2^n-1} - c_{2^n-k-1}) \\
&= \frac{c_{2^n-k-1}}{c_{2^n-1}} + \left[ \sqrt{1 - \frac{c_{2^n-k-1}}{c_{2^n-1}}} - 1 \right]^2, \\
&= \frac{|\theta|^{-2k} - |\theta|^{-2^{n+1}}}{1 - |\theta|^{-2^{n+1}}} + \left[ \sqrt{\frac{1 - |\theta|^{-2k}}{1 - |\theta|^{-2^{n+1}}}} - 1 \right]^2, \tag{3}
\end{aligned}$$

where we have re-indexed the computational basis of  $\mathcal{V}_n$  as  $e_0, \dots, e_{2^n-1}$  for clarity in this proof. Since  $|\theta| > 1$ , the quantity (3) can be set to less than  $\delta^2$  by appropriate choice of  $k = \mathcal{O}(1)$ . Since  $\chi(\phi_{n,k}^\theta) \leq k$ , this shows that  $\chi_\delta(\psi_n^\theta) = \mathcal{O}(1)$ . It is clear that we can set  $k = 1$  if  $|\theta|$  is large enough. This completes the proof.  $\square$

Note that, using Theorem 3.2 and Lemma 3.5, we can easily find a sequence of product states of stabilizer rank at least  $\frac{2^n}{4n}$  and  $\delta$ -approximate stabilizer rank  $\mathcal{O}(1)$ .

**Corollary 3.6.** *For any  $n \in \mathbb{N}$ , let*

$$\psi_n = \sqrt{\frac{3}{4^{2^n} - 1}} \bigotimes_{i=1}^n (e_0 + 2^{2^{i-1}} e_1) \in \mathcal{S}(\mathcal{V}_n)$$

*be a quantum state. Then  $\chi(\psi_n) \geq \frac{2^n}{4n}$  and for any constant  $\delta > 0$ ,  $\chi_\delta(\psi_n) = \mathcal{O}(1)$ .*

*Proof.* For each  $n$ , the coordinates of  $\psi_n$  form an exponentially increasing sequence of length  $2^n$ . It follows from Theorem 3.2 that  $\chi(\psi_n) \geq \frac{2^n}{4n}$ . The bound  $\chi_\delta(\psi_n) = \mathcal{O}(1)$  follows from Lemma 3.5.  $\square$

We now use field-theoretic techniques to construct a sequence of product states of stabilizer rank  $2^n$  and  $\delta$ -approximate stabilizer rank 1.

**Proposition 3.7.** *Let  $\delta > 0$  be a positive real number. If  $\theta \in \mathbb{C}$  is a complex number of degree at least  $2^n$  over  $\mathbb{Q}(i)$ , then the state*

$$\psi_n^\theta = \sqrt{\frac{|\theta|^2 - 1}{|\theta|^{2^{n+1}} - 1}} \bigotimes_{i=1}^n (e_0 + \theta^{2^{i-1}} e_1) \in \mathcal{S}(\mathcal{V}_n)$$

*has stabilizer rank  $\chi(\psi_n^\theta) = 2^n$ . If it furthermore holds that  $|\theta| > 1$ , then  $\chi_\delta(\psi_n^\theta) = \mathcal{O}(1)$ . Finally, there exists a positive real number  $\lambda_\delta$  such that for every  $\theta \in \mathbb{C}$  of degree at least  $2^n$  over  $\mathbb{Q}(i)$  for which  $|\theta| > \lambda_\delta$ , it holds that  $\chi(\psi_n^\theta) = 2^n$  and  $\chi_\delta(\psi_n^\theta) = 1$ .*

For example, to obtain a product state with stabilizer rank  $2^n$  and approximate stabilizer rank  $\mathcal{O}(1)$ , one can choose any transcendental number  $\theta \in \mathbb{C}$ , e.g. the circumference-to-diameter ratio  $\pi$ . Note also that there are  $\theta \in \mathbb{C}$  with  $|\theta| = 1$  such that Proposition 3.7 applies. It is worth mentioning that in this case, the coordinates of  $\psi_n^\theta$  contain no exponentially increasing sequence, that is, Theorem 3.2 does not yield an immediate lower bound on  $\chi(\psi_n^\theta)$ .

*Proof.* Note that the coordinates of  $\psi_n^\theta$  are (up to the normalization factor)  $1, \theta, \dots, \theta^{2^n-1}$ . By the degree assumption on  $\theta$ , the coordinates of  $\psi_n^\theta$  are linearly independent over  $\mathbb{Q}(i)$ . Let  $\psi_n^\theta = \sum_{i=1}^r c_i \sigma_i$  be a stabilizer decomposition of  $\psi_n^\theta$ , where  $\sigma_i \in \text{Stab}_n$  and  $c_i \in \mathbb{C}$  for each  $i \in [r]$ . Since the coordinates of each  $\sigma_i$  are contained in  $\mathbb{Q}(i)$ , it follows that

$$\text{span}_{\mathbb{Q}(i)}\{c_1, \dots, c_r\} \supseteq \{1, \theta, \dots, \theta^{2^n-1}\},$$

so  $r \geq 2^n$ . This completes the proof that  $\chi(\psi_n^\theta) = 2^n$ . The remaining statements follow from Lemma 3.5.  $\square$

## 4 States with multiplicative stabilizer rank under the tensor product

It is a standard fact that the stabilizer rank is *sub-multiplicative* under the tensor product, i.e.  $\chi(\psi \otimes \psi) \leq \chi(\psi)^2$  for any quantum state  $\psi$  [12, Section 2.1.3]. In [12, Section 4.4] it was remarked that there are no known examples of quantum states  $\psi$  of stabilizer rank greater than one for which equality holds. In this section, we explicitly construct two-qubit states  $\psi$  for which  $\chi(\psi) = 2$  and  $\chi(\psi \otimes \psi) = 4$ . Note that this is the smallest non-trivial example of multiplicative stabilizer rank that one can hope for, since for any single-qubit state  $\psi \propto e_0 + \alpha e_1$ , it holds that  $\psi^{\otimes 2} \propto e_{00} + \alpha(e_{01} + e_{10}) + \alpha^2 e_{11}$ , which has stabilizer rank at most 3.

**Theorem 4.1.** *Let*

$$\psi_\alpha = \frac{1}{\sqrt{1+2|\alpha|^2}}(e_{00} + \alpha(e_{01} + e_{10})) \in \mathcal{S}((\mathbb{C}^2)^{\otimes 2})$$

*when  $\alpha \in \mathbb{C}^\times$  is a non-zero complex number. Then  $\chi(\psi_\alpha) = 2$ , and for all but finitely many  $\alpha$  it holds that  $\chi(\psi_\alpha^{\otimes 2}) = 4$ . In particular,  $\chi(\psi_\alpha^{\otimes 2}) = 4$  for any  $\alpha$  that is transcendental over  $\mathbb{Q}$ .*

*Proof.* The fact that  $\chi(\psi_\alpha) = 2$  is obvious, so it suffices to prove that  $\chi(\psi_\alpha^{\otimes 2}) = 4$ . Note that, since the imaginary unit  $i$  is algebraic over  $\mathbb{Q}$ ,  $\alpha$  is transcendental over  $\mathbb{Q}$  if and only if it is transcendental over  $\mathbb{Q}(i)$ . Since there are only finitely many stabilizer states mod phase, it suffices to prove that for any set of three stabilizer states  $\{\sigma_1, \sigma_2, \sigma_3\} \subseteq \text{Stab}_2$ , there are at most finitely many  $\alpha$  (and no  $\alpha$  which are transcendental over  $\mathbb{Q}$ ) for which

$$\psi_\alpha^{\otimes 2} \in \text{span}\{\sigma_1, \sigma_2, \sigma_3\}. \quad (4)$$

For each  $j \in [3]$ , we may assume that

$$\sigma_j = \frac{1}{\sqrt{|A_j|}} \sum_{x \in A_j} i^{l_j(x)} \cdot (-1)^{q_j(x)} \cdot e_x$$

for some affine linear subspace  $A_j \subseteq \mathbb{F}_2^2$ , linear functional  $l_j$ , and quadratic form  $q_j$ , as in (1). Let  $S = (\sigma_1, \sigma_2, \sigma_3) \in \mathbb{Q}(i)^{\{0,1\}^2 \times 3}$ . For every  $\alpha$  that satisfies (4), there exist complex numbers  $\beta_\alpha, \gamma_\alpha, \lambda_\alpha \in \mathbb{C}$  for which  $\psi_\alpha^{\otimes 2} = \beta_\alpha \sigma_1 + \gamma_\alpha \sigma_2 + \lambda_\alpha \sigma_3$ , and a  $3 \times 3$  submatrix  $T$  of  $S$  for which

$$\left[ T \mid -\mathbb{1}_3 \right] \begin{bmatrix} \beta_\alpha \\ \gamma_\alpha \\ \lambda_\alpha \\ 1 \\ \alpha \\ \alpha^2 \end{bmatrix} = 0. \quad (5)$$

Since there are only finitely many  $3 \times 3$  submatrices of  $S$ , it suffices to prove that for any choice of  $3 \times 3$  submatrix  $T$ , only finitely many  $\alpha$  (and no transcendental  $\alpha$ ) can satisfy (5).

If  $T$  is singular, then there exists a non-trivial  $\mathbb{Q}(i)$ -linear combination of  $\{1, \alpha, \alpha^2\}$  that equals zero, which at most finitely many  $\alpha$  will satisfy (and in particular, no transcendental  $\alpha$  will satisfy).

If  $T$  is nonsingular, then by applying  $T^{-1}$  to both sides we can find polynomials  $f, g, h \in \mathbb{Q}(i)[x]$  for which  $\beta_\alpha = f(\alpha), \gamma_\alpha = g(\alpha)$ , and  $\lambda_\alpha = h(\alpha)$  for every choice of  $\alpha$  that satisfies (5).

Let  $R = \{00, 01, 10\}^{\times 2} \subseteq \mathbb{F}_2^4$  be the subset of bitstrings corresponding to non-zero coordinates of  $\psi_\alpha^{\otimes 2}$ . If there exists  $x \in A_i \setminus R$  for some  $i \in [3]$ , then there exists a non-trivial  $\mathbb{Q}(i)$ -linear combination of  $\{f, g, h\}$  which equals zero, which at most finitely many  $\alpha$  (and no transcendental  $\alpha$ ) will satisfy. So we may assume  $A_i \subseteq R$  for all  $i \in [3]$ .

Let  $R_0 = \{0000\}$ ,  $R_1 = \{0001, 0010, 0100, 1000\}$ , and  $R_2 = \{0101, 0110, 1001, 1010\}$ , so  $R = R_0 \cup R_1 \cup R_2$ . If there exists  $x \in A_1 \cap R_2$  and  $y \in R_2 \setminus A_1$ , then there exist linear combinations

$$\begin{aligned} \star f(\alpha) + \cdot g(\alpha) + \cdot h(\alpha) &= \alpha^2 \\ \cdot g(\alpha) + \cdot h(\alpha) &= \alpha^2, \end{aligned}$$

where each  $\cdot \in \mathbb{C}$  denotes an arbitrary complex number we do not bother to name, and  $\star \in \mathbb{C}^\times$  denotes an arbitrary non-zero complex number we do not bother to name. Subtracting these equations yields a non-trivial  $\mathbb{Q}(i)$ -linear combination of  $\{f, g, h\}$  that equals zero, which at most finitely many  $\alpha$  (and no transcendental  $\alpha$ ) will satisfy. By symmetry, for all  $i \in [3]$ , either  $R_2 \subseteq A_i$  or  $R_2 \cap A_i = \emptyset$ . If  $R_2 \subseteq A_i$ , then  $R_2 = A_i$  because this is the only affine linear subspace contained in  $R$  that contains  $R_2$ . Without loss of generality, we may assume  $A_1 = R_2$ . If  $A_2 = R_2$ , then  $A_3 = R_0 \cup R_1$ , which is not an affine linear subspace, a contradiction. Otherwise,  $A_2 \cup A_3 = R_0 \cup R_1$ , which is also a contradiction, as there are no affine linear subspaces of size greater than 2 contained in  $R_0 \cup R_1$ . This completes the proof.  $\square$

## 5 Generic stabilizer rank

**Fact 5.1.** *For any positive integer  $n$ , all but finitely many qubit states mod phase  $[\psi] \in \mathbb{P}^1$  maximize  $\chi(\psi^{\otimes n})$ . Similarly, all but finitely many qubit states mod phase  $[\psi] \in \mathbb{P}^1$  maximize  $\chi^{\mathbb{R}}(\psi^{\otimes n})$ .*

This fact, the proof of which we defer until after introducing this section, motivates us to define the  $n$ -th *generic stabilizer rank* as

$$\chi_n = \max_{\psi \in \mathcal{S}(\mathbb{C}^2)} \chi(\psi^{\otimes n}),$$

and the  $n$ -th *generic real stabilizer rank* as

$$\chi_n^{\mathbb{R}} = \max_{\psi \in \mathcal{S}(\mathbb{C}^2)} \chi^{\mathbb{R}}(\psi^{\otimes n}).$$

In Proposition 5.4 we prove that  $\chi_n$  and  $\chi_n^{\mathbb{R}}$  differ by at most a constant factor of two. This motivates the study of  $\chi_n^{\mathbb{R}}$ , since it has the same scaling as  $\chi_n$ , but may be easier to work with. Note that  $\chi_n$  upper bounds  $\chi(T^{\otimes n})$ .

In this section, we prove bounds on  $\chi_n$  and  $\chi_n^{\mathbb{R}}$ , and observe some useful reductions for studying these quantities. In Proposition 5.2 we use Fact 5.1 to obtain a modest

improvement of the best-known upper bound on  $\chi_n$ . In Proposition 5.3 we prove a useful reduction for studying  $\chi_n$  (respectively,  $\chi_n^{\mathbb{R}}$ ), namely, that there must exist a single set of  $\chi_n$  stabilizer states (resp.  $\chi_n^{\mathbb{R}}$  real stabilizer states) that span the symmetric subspace. In other words, there exists a single set of  $\chi_n$  stabilizer states (resp.  $\chi_n^{\mathbb{R}}$  real stabilizer states) such that, for every qubit state  $\psi$ , the state  $\psi^{\otimes n}$  lies in the span of the set. In Proposition 5.5 we introduce a technique for upper bounding  $\chi_n$  when upper bounds on  $\chi(\psi^{\otimes n})$  are known for sufficiently many (linear in  $n$ ) qubit states mod phase  $[\psi] \in \mathbb{P}^1$ , and obtain similar results for  $\chi_n^{\mathbb{R}}$ . In Proposition 5.6 we refine Fact 5.1 to obtain quantitative upper bounds on the (finite) number of states mod phase of sub-generic stabilizer rank and sub-generic real stabilizer rank.

Before proceeding, we prove Fact 5.1. We refer the reader to [16] for the basic algebraic-geometric definitions and arguments used in this proof, and elsewhere in this section. In this proof and in others in this section, we only prove the statement for  $\chi_n$ , as the proof for  $\chi_n^{\mathbb{R}}$  is essentially identical.

*Proof of Fact 5.1.* We prove only the statement for  $\chi_n$ . Let

$$\nu_n(\mathbb{P}^1) = \{[\phi^{\otimes n}] : [\phi] \in \mathbb{P}^1\} \subseteq \mathbb{P}^{2^n-1},$$

which happens to be the image of the  $n$ -th Veronese embedding of  $\mathbb{P}^1$ , embedded in  $\mathbb{P}^{2^n-1}$ . The set  $\nu_n(\mathbb{P}^1)$  forms a 1-dimensional irreducible projective variety, so its intersection with any other projective variety is either empty, zero-dimensional, or equal to  $\nu_n(\mathbb{P}^1)$ . Hence, for any positive integer  $r$ ,  $\Sigma_r(\check{\text{Stab}}_n) \cap \nu_n(\mathbb{P}^1)$  is either a finite set of points, or  $\Sigma_r(\check{\text{Stab}}_n) \supseteq \nu_n(\mathbb{P}^1)$ . This completes the proof.  $\square$

Fact 5.1 immediately implies the following slight improvement of the upper bound  $\chi_n = \mathcal{O}((n+1)2^{n/2})$  obtained in [4, Theorem 3]:

**Proposition 5.2.**  $\chi_n = \mathcal{O}(2^{n/2})$ .

*Proof.* This follows directly from our Fact 5.1 and [4, Theorem 2], which states that equatorial states (an infinite family of states mod phase) have stabilizer rank  $\mathcal{O}(2^{n/2})$ .  $\square$

We next prove that a single set of  $\chi_n$  stabilizer states (respectively,  $\chi_n^{\mathbb{R}}$  real stabilizer states) spans  $S^n(\mathbb{C}^2)$ .

**Proposition 5.3.** *For any positive integer  $n$ , there exists a set of stabilizer states  $\{\sigma_1, \dots, \sigma_{\chi_n}\} \subseteq \text{Stab}_n$  for which*

$$S^n(\mathbb{C}^2) \subseteq \text{span}\{\sigma_1, \dots, \sigma_{\chi_n}\}.$$

*Similarly, there exists a single set of real stabilizer states  $\{\sigma_1, \dots, \sigma_{\chi_n^{\mathbb{R}}}\} \subseteq \text{Stab}_n^{\mathbb{R}}$  for which*

$$S^n(\mathbb{C}^2) \subseteq \text{span}\{\sigma_1, \dots, \sigma_{\chi_n^{\mathbb{R}}}\}.$$

Since  $\dim(S^n(\mathbb{C}^2)) = n+1$ , it follows from Proposition 5.3 that  $\chi_n \geq n+1$ . We note that a similar proof as below can be used to show that a generic product state of the form  $\psi_1 \otimes \dots \otimes \psi_n$ , for qubit states  $\psi_i \in \mathcal{S}(\mathbb{C}^2)$ , has stabilizer rank  $2^n$ , where in this context we define *generic* in the same algebraic-geometric sense as in [20]. In Proposition 3.7 we have presented an explicit sequence of product states of stabilizer rank  $2^n$ , which is maximal.

*Proof of Proposition 5.3.* We prove only the statement for  $\chi_n$ . Let  $r = \chi_n$ , so  $\Sigma_r(\check{\text{Stab}}_n) \supseteq \nu_n(\mathbb{P}^1)$ , where  $\nu_n(\mathbb{P}^1)$  is defined in the proof of Fact 5.1. Since  $\nu_n(\mathbb{P}^1)$  is irreducible, and  $\Sigma_r(\check{\text{Stab}}_n)$  is reducible into a finite union of projective  $(r-1)$ -dimensional linear subspaces, one of these subspaces must contain  $\nu_n(\mathbb{P}^1)$ . To complete the proof, recall that the affine cone over  $\text{span}(\nu_n(\mathbb{P}^1))$  is  $S^n(\mathbb{C}^2)$ .  $\square$

The next proposition shows that  $\chi_n^{\mathbb{R}}$  and  $\chi_n$  differ by at most a constant factor of two, which motivates the study of  $\chi_n^{\mathbb{R}}$ .

**Proposition 5.4.** *For any positive integer  $n$ , it holds that  $\chi_n \leq \chi_n^{\mathbb{R}} \leq 2\chi_n$ .*

*Proof.* The first inequality is obvious, so it suffices to prove  $\chi_n^{\mathbb{R}} \leq 2\chi_n$ . Since the tensors  $\sum_{|x|=k} e_x$  for  $k \in [n]$  form a basis for  $S^n(\mathbb{C}^2)$ , then by Proposition 5.3,  $\chi_n$  is the minimum number for which there exists a set of stabilizer states  $\{\sigma_1, \dots, \sigma_{\chi_n}\} \subseteq \text{Stab}_n$  such that

$$\sum_{\substack{x \in \mathbb{F}_2^n \\ |x|=k}} e_x \in \text{span}\{\sigma_1, \dots, \sigma_{\chi_n}\} \quad (6)$$

for all  $k \in \{0, 1, \dots, n\}$ . Without loss of generality, for each  $j \in [\chi_n]$  it holds that

$$\sigma_j = \frac{1}{\sqrt{|A_j|}} \sum_{x \in A_j} i^{l_j(x)} \cdot (-1)^{q_j(x)} \cdot e_x$$

for some affine linear subspace  $A_j \subseteq \mathbb{F}_2^n$ , linear functional  $l_j$ , and quadratic form  $q_j$  (see (1)). For each  $j \in [\chi_n]$ , we define  $\rho_j$  to be the state

$$\rho_j = \frac{1}{\sqrt{|A_j|}} \sum_{x \in A_j} (-1)^{q_j(x) + l_j(x)} \cdot e_x,$$

and observe that for any real numbers  $a, b \in \mathbb{R}$ , it holds that

$$\text{Re}((a + ib)\sigma_j) = (a - b)\text{Re}(\sigma_j) + b\rho_j, \quad (7)$$

where  $\text{Re}(\cdot)$  is the real part with respect to the computational basis. For each  $k \in \{0, 1, \dots, n\}$ , there exist real numbers  $a_1, \dots, a_{\chi_n}, b_1, \dots, b_{\chi_n} \in \mathbb{R}$  for which

$$\begin{aligned} \sum_{|x|=k} e_x &= \sum_{j \in [\chi_n]} (a_j + ib_j)\sigma_j \\ &= \text{Re} \left( \sum_{j \in [\chi_n]} (a_j + ib_j)\sigma_j \right) \\ &= \sum_{j \in [\chi_n]} ((a_j - b_j)\text{Re}(\sigma_j) + b_j\rho_j), \end{aligned}$$

where the first line follows from (6), the second follows from the fact that the tensor is already real, and the third follows from (7). Hence,

$$S^n(\mathbb{C}^2) \in \text{span}_{\mathbb{C}}\{\text{Re}(\sigma_1), \dots, \text{Re}(\sigma_{\chi_n}), \rho_1, \dots, \rho_{\chi_n}\}.$$

Since  $\text{Re}(\sigma_j)$  and  $\rho_j$  are clearly proportional to real stabilizer states for all  $j \in [\chi_n]$ , it follows that  $\chi_n^{\mathbb{R}} \leq 2\chi_n$ .  $\square$

Using similar techniques as in the proof of Proposition 5.3, it is straightforward to show that  $\chi(\psi) \leq \chi^{\mathbb{R}}(\psi) \leq 2\chi(\psi)$  for any real quantum state  $\psi \in \mathcal{S}(\mathcal{V}_n)$ .

The next proposition tells us that upper bounds on the stabilizer ranks (respectively, real stabilizer ranks) of any set of  $n + 1$  pairwise non-collinear states of the form  $\psi^{\otimes n}$  implies an upper bound on  $\chi_n$  (resp.  $\chi_n^{\mathbb{R}}$ ).

**Proposition 5.5.** *Let  $r$  be a positive integer. If there exists a set of  $n + 1$  pairwise non-collinear qubit states  $\{\psi_1, \dots, \psi_{n+1}\} \subseteq \mathcal{S}(\mathbb{C}^2)$  with  $\chi(\psi_i^{\otimes n}) \leq r$  for all  $i \in [n + 1]$ , then  $\chi_n \leq r(n + 1)$ . Similarly, if there exists a set of  $n + 1$  pairwise non-collinear qubit states  $\{\psi_1, \dots, \psi_{n+1}\} \subseteq \mathcal{S}(\mathbb{C}^2)$  with  $\chi^{\mathbb{R}}(\psi_i^{\otimes n}) \leq r$  for all  $i \in [n + 1]$ , then  $\chi_n^{\mathbb{R}} \leq r(n + 1)$ .*

*Proof.* We prove only the statement for  $\chi_n$ . First note that  $\text{span}\{\psi_1^{\otimes n}, \dots, \psi_{n+1}^{\otimes n}\} = S^n(\mathbb{C}^2)$  by [21, Proposition 3.1] or [22, Corollary 18]. Since  $\chi(\psi_i^{\otimes n}) \leq r$  for all  $i \in [n + 1]$ , then any superposition of the states  $\psi_1^{\otimes n}, \dots, \psi_{n+1}^{\otimes n}$  has stabilizer rank at most  $r(n + 1)$ . It follows that  $\chi_n \leq r(n + 1)$ .  $\square$

We close this section by refining Fact 5.1 to give a quantitative upper bound on the number of states of sub-generic rank.

**Proposition 5.6.** *There are at most*

$$n \binom{|\check{\text{Stab}}_n|}{\chi_n - 1}$$

*states mod phase  $[\psi] \in \mathbb{P}^1$  for which  $\chi(\psi^{\otimes n}) < \chi_n$ . Similarly, there are at most*

$$n \binom{|\check{\text{Stab}}_n^{\mathbb{R}}|}{\chi_n^{\mathbb{R}} - 1}$$

*states mod phase  $[\psi] \in \mathbb{P}^1$  for which  $\chi^{\mathbb{R}}(\psi^{\otimes n}) < \chi_n^{\mathbb{R}}$ .*

We have computed the quantities  $|\check{\text{Stab}}_n|$  and  $|\check{\text{Stab}}_n^{\mathbb{R}}|$  at the end of Section 2.

*Proof.* We prove only the statement for  $\chi_n$ . Note that any set of  $n + 1$  pairwise non-collinear states in  $\hat{\nu}_1(\mathbb{P}^1)$  (i.e. states of the form  $\psi^{\otimes n}$ ) span  $S^n(\mathbb{C}^2)$  (see [21, Proposition 3.1] or [22, Corollary 18]), so any set of  $\chi_n - 1$  linearly independent stabilizer states can contain at most  $n$  distinct elements of  $\hat{\nu}_1(\mathbb{P}^1)$  in their span. Since there are at most

$$\binom{|\check{\text{Stab}}_n|}{\chi_n - 1}$$

distinct sets of  $\chi_n - 1$  linearly independent stabilizer states, the bound follows.  $\square$

## References

- [1] Sergey Bravyi, Graeme Smith, and John A. Smolin. “Trading classical and quantum computational resources”. *Physical Review X* **6**, 021043 (2016). doi: [10.1103/PhysRevX.6.021043](https://doi.org/10.1103/PhysRevX.6.021043).
- [2] Sergey Bravyi and David Gosset. “Improved classical simulation of quantum circuits dominated by Clifford gates”. *Physical Review Letters* **116**, 250501 (2016). doi: [10.1103/PhysRevLett.116.250501](https://doi.org/10.1103/PhysRevLett.116.250501).

- [3] Sergey Bravyi, Dan Browne, Padraic Calpin, Earl Campbell, David Gosset, and Mark Howard. “Simulation of quantum circuits by low-rank stabilizer decompositions”. *Quantum* **3**, 181 (2019). doi: [10.22331/q-2019-09-02-181](https://doi.org/10.22331/q-2019-09-02-181).
- [4] Hammam Qassim, Hakop Pashayan, and David Gosset. “Improved upper bounds on the stabilizer rank of magic states”. *Quantum* **5**, 606 (2021). doi: [10.22331/q-2021-12-20-606](https://doi.org/10.22331/q-2021-12-20-606).
- [5] Shir Peleg, Amir Shpilka, and Ben Lee Volk. “Lower Bounds on Stabilizer Rank”. *Quantum* **6**, 652 (2022). doi: [10.22331/q-2022-02-15-652](https://doi.org/10.22331/q-2022-02-15-652).
- [6] David Petrie Moulton. “Representing powers of numbers as subset sums of small sets”. *Journal of Number Theory* **89**, 193–211 (2001). doi: [10.1006/jnth.2000.2646](https://doi.org/10.1006/jnth.2000.2646).
- [7] A. A. Razborov. “Lower bounds on the size of bounded depth circuits over a complete basis with logical addition”. *Mathematical notes of the Academy of Sciences of the USSR* **41**, 333–338 (1987). doi: [10.1007/BF01137685](https://doi.org/10.1007/BF01137685).
- [8] R. Smolensky. “Algebraic methods in the theory of lower bounds for boolean circuit complexity”. In *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*. Pages 77–82. (1987). doi: [10.1145/28395.28404](https://doi.org/10.1145/28395.28404).
- [9] R. Smolensky. “On representations by low-degree polynomials”. In *Proceedings of the 1993 IEEE 34th Annual Foundations of Computer Science*. Pages 130–138. (1993). doi: [10.1109/SFCS.1993.366874](https://doi.org/10.1109/SFCS.1993.366874).
- [10] J. Landsberg and M. Michałek. “Towards finding hay in a haystack: explicit tensors of border rank greater than  $2.02m$  in  $\mathbb{C}^m \otimes \mathbb{C}^m \otimes \mathbb{C}^m$ .” (2019). [arXiv:1912.11927](https://arxiv.org/abs/1912.11927).
- [11] Joseph Landsberg. “Graduate studies in mathematics”. In *Tensors: Geometry and Applications*. Volume 128 of *Graduate Studies in Mathematics*. AMS (2011). doi: [10.1090/gsm/128](https://doi.org/10.1090/gsm/128).
- [12] Hammam Qassim. “Classical simulations of quantum systems using stabilizer decompositions”. PhD thesis. University of Waterloo. (2021).
- [13] Michael Beverland, Earl Campbell, Mark Howard, and Vadym Kliuchnikov. “Lower bounds on the non-clifford resources for quantum computations”. *Quantum Science and Technology* **5**, 035009 (2020). doi: [10.1088/2058-9565/ab8963](https://doi.org/10.1088/2058-9565/ab8963).
- [14] Jeroen Dehaene and Bart De Moor. “Clifford group, stabilizer states, and linear and quadratic operations over  $\text{GF}(2)$ ”. *Physical Review A* **68**, 042318 (2003). doi: [10.1103/PhysRevA.68.042318](https://doi.org/10.1103/PhysRevA.68.042318).
- [15] Maarten Van den Nest. “Classical simulation of quantum computation, the Gottesman-Knill theorem, and slightly beyond”. *Quantum Information and Computation* **10**, 258–271 (2010).
- [16] Joe Harris. “Algebraic geometry: A first course”. *Graduate Texts in Mathematics*. Springer New York. (2013). doi: [10.1007/978-1-4757-2189-8](https://doi.org/10.1007/978-1-4757-2189-8).
- [17] Jay Goldman and Gian-Carlo Rota. “On the foundations of combinatorial theory IV: Finite vector spaces and Eulerian generating functions.”. Technical report. Harvard University (1970).
- [18] David Gross. “Hudson’s theorem for finite-dimensional quantum systems”. *Journal of Mathematical Physics* **47**, 122107 (2006). doi: [10.1063/1.2393152](https://doi.org/10.1063/1.2393152).
- [19] William Feller. “An introduction to probability theory and its applications”. Volume 1. John Wiley and Sons. (1991). Third edition.
- [20] Benjamin Lovitz and Nathaniel Johnston. “Entangled subspaces and generic local state discrimination with pre-shared entanglement” (2020). [arXiv:2010.02876](https://arxiv.org/abs/2010.02876).
- [21] Kil-Chan Ha and Seung-Hyeok Kye. “Multi-partite separable states with unique decompositions and construction of three qubit entanglement with positive partial

- transpose”. *Journal of Physics A: Mathematical and Theoretical* **48**, 045303 (2015). doi: [10.1088/1751-8113/48/4/045303](https://doi.org/10.1088/1751-8113/48/4/045303).
- [22] Benjamin Lovitz and Fedor Petrov. “A generalization of Kruskal’s theorem on tensor decomposition” (2021). [arXiv:2103.15633](https://arxiv.org/abs/2103.15633).
- [23] Daniel Gottesman. “Stabilizer codes and quantum error correction”. PhD thesis. California Institute of Technology. (1997).
- [24] Michael A. Nielsen and Isaac L. Chuang. “Quantum computation and quantum information”. Cambridge University Press. (2000). doi: [10.1017/CBO9780511976667](https://doi.org/10.1017/CBO9780511976667).
- [25] Daniel Gottesman. “The Heisenberg representation of quantum computers”. In 22nd International Colloquium on Group Theoretical Methods in Physics. Pages 32–43. (1998). [arXiv:quant-ph/9807006](https://arxiv.org/abs/quant-ph/9807006).
- [26] P. Oscar Boykin, Tal Mor, Matthew Pulver, Vwani Roychowdhury, and Farrokh Vatan. “On universal and fault-tolerant quantum computing: A novel basis and a new constructive proof of universality for Shor’s basis”. In Proceedings of the 40th Annual Symposium on Foundations of Computer Science. (1999). doi: [10.1109/SF-FCS.1999.814621](https://doi.org/10.1109/SF-FCS.1999.814621).
- [27] Sergey Bravyi and Alexei Kitaev. “Universal quantum computation with ideal clifford gates and noisy ancillas”. *Physical Review A* **71**, 022316 (2005). doi: [10.1103/PhysRevA.71.022316](https://doi.org/10.1103/PhysRevA.71.022316).

## A Motivation behind stabilizer rank

In this Appendix we will motivate the definition of stabilizer rank in more depth, and explain how it relates to the simulation cost of quantum circuits. In particular, we will review in detail how the stabilizer rank of a quantum state quantifies the classical simulation cost of applying Clifford gates and computational basis measurements to that state, and review how the stabilizer rank of  $n$  copies of the so-called  $T$ -state quantifies the simulation cost of Clifford+ $T$  circuits utilizing  $n$   $T$ -gates. We use the standard graphical notation for quantum circuits: Fixing some natural numbers  $m \leq k$ , we depict with



a circuit applying a  $k$ -qubit unitary  $U$  to an input state  $\psi \in \mathcal{S}(\mathcal{V}_k)$  and measuring an output register consisting of  $m$  qubits in computational basis. Without loss of generality, we will always take the first  $m$  qubits as output register. In the following, the number of qubits in a circuit as in (8) will always be  $k$  and the number of measured qubits  $m$  unless specified differently.

Let us start by recalling some basic notions of simulation of quantum circuits. Simulating a quantum circuit as in (8) with a  $k$ -qubit input state  $\psi$  *weakly* means to draw  $m$  classical bits according to the output distribution of the circuit. Simulating the circuit *strongly* on the other hand means to be able to compute the probability of a bitstring  $x_1 \dots x_m$  being the output of the circuit. By Born’s rule, this probability is given by

$$P(x_1 \dots x_m) = \psi^* U^\dagger \left( \Pi_{x_1 \dots x_m} \otimes \mathbf{1}_2^{\otimes k-m} \right) U \psi$$

where  $\Pi_{x_1 \dots x_m}$  is the orthogonal projection onto  $\text{span}\{e_{x_1} \otimes \dots \otimes e_{x_m}\}$ .

Another standard notion of simulation is the so-called  $\epsilon$ -strong simulation. For a bitstring  $x_1 \dots x_m$ , the task is to approximate the output probability  $P(x_1 \dots x_m)$  up to relative error  $\epsilon$ . More precisely, fix a relative error  $\epsilon$ . Given a bitstring  $x_1 \dots x_m$ , we then want to get an output  $\xi$  such that

$$(1 - \epsilon)P(x_1 \dots x_m) \leq \xi \leq (1 + \epsilon)P(x_1 \dots x_m)$$

where  $P$  is the output distribution of the circuit.

Recall the (affine) Clifford gates  $H, S$ , and  $CNOT$  Section 2. We will later also need the controlled  $Z$  gate defined via

$$CZ = (\mathbb{1}_2 \otimes H)CNOT(\mathbb{1}_2 \otimes H) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

The Clifford unitaries  $U \in \text{Cliff}_k$  are exactly those unitaries composed from  $H, S, CNOT$ , and global phase gates only. As done in Section 2, one can equivalently define the group  $\text{Cliff}_k$  as the normalizer of the  $k$ -qubit Pauli group  $\text{Pauli}_k$  (also defined in Section 2): Conjugating a Pauli unitary with a Clifford unitary yields another Pauli unitary [23].

As a consequence of this fact, we can work very efficiently on certain quantum states using the *stabilizer formalism*, which was introduced in [23]. We will now briefly recall some basics about the stabilizer formalism and refer the reader to [24] for an in-depth discussion and detailed proofs. To start, note that  $e_0^{\otimes k}$  is, up to global phase, the unique quantum state invariant under applying (or *stabilized by*)  $Z_i$  for all  $i \in [k]$ , where  $Z_i$  is the tensor product of a Pauli  $Z$  on the  $i$ 'th qubit with identities on all other qubits. In fact, one can show that if  $P_1, \dots, P_k$  are independent Pauli unitaries (that is, none of them is a product of the others), and the group generated by them does not contain  $-\mathbb{1}_2^{\otimes k}$ , then there exists up to global phase a unique state  $\sigma$  stabilized by  $P_1, \dots, P_k$  (see [24, Chapter 10.5.1] for details).

It turns out that if a state  $\sigma$  can be uniquely specified as above, the same holds for the state resulting from applying a Clifford unitary  $U$  to  $\sigma$ : In fact, one can show that the Pauli unitaries  $UP_1U^\dagger, \dots, UP_kU^\dagger$  are independent again, do not generate  $-\mathbb{1}_2^{\otimes k}$  and it is easy to see that they stabilize  $U\sigma$  (see [24, Chapter 10.5.2] for details). Conversely, for every state of the form  $Ue_0^{\otimes k}$ , there are  $k$  independent Paulis stabilizing it, see [18] for a proof. Summarizing, we see that the states of the form  $\sigma = Ue_0^{\otimes k}$  for a Clifford unitary  $U$  are exactly the ones uniquely specified up to global phase by  $k$  independent Pauli operators stabilizing it. This explains why we defined a *stabilizer state* as a state of the form  $Ue_0^{\otimes k}$  where  $U$  is a Clifford unitary in Section 2.

The celebrated Gottesman-Knill theorem states that a circuit as in (8) where  $U$  is a Clifford unitary can be simulated efficiently if the input state is a stabilizer state  $\sigma \in \mathcal{S}(\mathcal{V}_k)$ .

**Theorem A.1** (Gottesman, Knill [25]). *Let  $\sigma$  be a  $k$ -qubit stabilizer state specified by  $k$  independent Paulis that stabilize it. A quantum circuit  $U$  composed only from Clifford gates acting on  $\sigma$  followed by measuring an output register consisting of  $m \leq k$  qubits in the computational basis can be efficiently simulated both strongly and weakly. More precisely, the complexity of simulating the quantum computation scales quadratically in the number of qubits and linearly in the number of Clifford gates and measurements that are applied.*

A proof of Theorem A.1 can be found in [24, Section 10.5.4]. We mention that one essentially has to update the Pauli stabilizers gate-by-gate, which yields  $k$  independent Paulis stabilizing  $U\sigma$ . One can read in detail in [24, Section 10.5.3] how one can then efficiently obtain the outcome probabilities from this. It is also worth mentioning that the theorem holds more generally if we measure any observable from the Pauli group, not only for measuring in the computational basis.

Note that if a quantum state  $\sigma \in \mathcal{S}(\mathcal{V}_k)$  is stabilized by a Pauli unitary  $P$ , all states of the form  $e^{i\theta}\sigma$  for  $\theta \in \mathbb{R}$  are also stabilized by  $P$ . While a global phase does not influence the outcome probabilities of computational basis measurements, it changes the amplitudes of the state. This means that Theorem A.1 as stated above does not let us calculate amplitudes but only outcome probabilities. In [3], the authors describe a way of keeping track of the global phase: They define a classical data format for stabilizer states which they call the *CH-form*. We now briefly describe their approach and refer to [3] for more details. Another in-depth discussion can be found in [12, Section 2.1.4] from where we also borrow our notation. Essentially, one can show that every stabilizer state  $\sigma$  is of the form

$$\sigma = \sigma(w, U, h, s) = wUH(h)(e_{s_1} \otimes \cdots \otimes e_{s_k})$$

where  $w \in \mathbb{C}$ ,  $s, h \in \mathbb{F}_2^k$  and  $U$  is a Clifford unitary composed from gates *CNOT*, *CZ* and *S* only. The unitary  $H(h)$  is a tensor product of  $H$  gates acting on the qubits  $i$  such that  $h_i = 1$  and  $\mathbb{1}_2$  elsewhere. As in the proof of Theorem A.1,

one can now simulate a circuit built from Clifford gates only by updating  $w, U, h$  and  $s$  gate-by-gate. The authors show in [3] that this update can be done with computational cost at most quadratic in  $k$ : Updating the CH form after applying a global phase has constant computational cost, a *CNOT*, *CZ*, or *S* has linear cost in  $k$ , and a Hadamard gate has quadratic cost in  $k$ . Moreover, they show that given a stabilizer state  $\sigma \in \mathcal{S}(\mathcal{V}_k)$  in *CH-form*, one can calculate the amplitude  $(e_{x_1}^* \otimes \cdots \otimes e_{x_k}^*)\sigma$  with computational cost quadratic in the number of qubits. Consequently, one can calculate the overlap

$$\sigma(w, U, h, s)^* \sigma(w', U', h', s') = \bar{w} \cdot w' \cdot (e_{s_1}^* \otimes \cdots \otimes e_{s_k}^*) H(h) U^\dagger \sigma(w', U', h', s')$$

of two stabilizer states given in *CH-form* with computational cost at most cubic in the number of qubits by first updating the *CH-form* of  $H(h)U^\dagger\sigma(w', U', h', s')$  and then calculating the overlap with  $(e_{s_1} \otimes \cdots \otimes e_{s_k})$ . Finally, for a stabilizer state  $\sigma(w, U, h, s)$  given in *CH-form*, an integer  $m \leq k$ , and an orthogonal projector  $\Pi_{x_1 \dots x_m}$  onto  $\text{span}\{e_{x_1} \otimes \cdots \otimes e_{x_m}\}$  for some bitstring  $x_1 \dots x_m$ , one can calculate the *CH-form* of the stabilizer state

$$\left( \Pi_{x_1 \dots x_m} \otimes \mathbb{1}_2^{\otimes k-m} \right) \sigma(w, U, h, s)$$

with computational cost quadratic in  $k$ .

With that, we can now understand the importance of the stabilizer rank as a measure of the computational cost of strong simulation of quantum circuits with general input states. Say, we want to strongly simulate a quantum circuit as in (8) where  $\psi$  is a  $k$ -qubit quantum state and  $U$  is a Clifford unitary. Say furthermore that we can decompose

$$\psi = \sum_{i=1}^r c_i \sigma_i \tag{9}$$

where the  $\sigma_i$  are stabilizer states each specified in *CH-form* and the  $c_i$  are complex numbers. Given a bitstring  $x_1 \dots x_m$ , we want to calculate

$$P(x_1 \dots x_m) = \psi^* U^\dagger (\Pi_{x_1 \dots x_m} \otimes \mathbb{1}) U \psi = \sum_{i,j=1}^r \bar{c}_i \cdot c_j \cdot \sigma_i^* U^\dagger \left( \Pi_{x_1 \dots x_m} \otimes \mathbb{1}_2^{\otimes k-m} \right) U \sigma_j.$$

We can do so by first updating the  $CH$ -form of  $U\sigma_i$  and  $(\Pi_{x_1\dots x_m} \otimes \mathbb{1}_2^{\otimes k-m})U\sigma_j$  followed by calculating  $r^2$  overlaps between stabilizer states. Since for every of the summands the computational cost is linear in the number of gates of which  $U$  is composed and cubic in the number of qubits, the whole cost is cubic in the number of qubits, linear in the number of Clifford gates and quadratic in the number of terms  $r$  appearing in the stabilizer decomposition.

As already done in Section 2, we call the minimal  $r$  such that there exists a decomposition as in equation (9) the *stabilizer rank* of  $\psi$  and denote it  $\chi(\psi)$ . It follows that lower bounds on  $\chi(\psi)$  imply lower bounds on the complexity of simulating a circuit of the form (8) using the approach we have just described. On the other hand, finding upper bounds on  $\chi(\psi)$  by providing a decomposition as in (9) can give us better simulation algorithms for circuits of the form (8).

For a discussion of a weak simulation protocol and an  $\epsilon$ -strong simulation protocol making use of stabilizer rank decompositions see [3, Section 4]. We mention that there the authors deduce that the computational cost of weak simulation scales linearly in the approximate stabilizer rank of  $\psi$  and polynomially in the number of qubits and the number of gates applied; and that the cost of  $\epsilon$ -strong simulation scales linearly in the exact stabilizer rank of  $\psi$  and polynomially in the number of qubits and the number of gates applied.

As an application of the connection between the stabilizer rank of a state  $\psi$  and the classical simulation cost of applying Clifford circuits and computational basis measurements to  $\psi$ , we will now see how low-rank stabilizer decompositions of  $n$  copies of the so-called  $T$ -state can also be used to simulate circuits built from a universal gate set. This strategy has been used for instance in [2]. For simplicity, we will only consider the case here where all qubits in the circuit in (8) are measured in computational basis, that is, the size  $m$  of the output register is equal to the number of qubits  $k$ .

Recall that a gate set  $\mathcal{G}$  is called *universal* if every unitary  $U$  on  $k$  qubits can be approximated arbitrarily well by unitaries  $U_{\mathcal{G}}$  composed solely of gates in  $\mathcal{G}$ . It is well-known that the set of Clifford gates is not universal but, together with the so-called  $T$ -gate

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix},$$

they form a universal gate set [26].

Under the assumption that our quantum device can only prepare a computational basis state  $e_0^{\otimes k}$ , apply Clifford+ $T$  operations and measure the qubits in computational basis, the  $T$ -gates appear, by the preceding discussion, to be responsible for the potential superiority of the quantum device. It is therefore an interesting question how efficiently we can simulate a quantum computation on  $k$  qubits which, in addition to Clifford gates, uses  $n$  single-qubit  $T$ -gates.

A standard way of approaching this question is via the study of *magic state injection* [27]. For this, we note that for the magic state  $T = \frac{1}{\sqrt{2}}(e_0 + e^{i\frac{\pi}{4}}e_1)$ , applying a  $T$ -gate to any qubit state  $\psi$  is the same as applying the circuit

where the double wire denotes a *classical control*: The  $S$  gate on the first system is applied if and only if the outcome of the computational basis measurement on the second system is 1. Therefore, any  $k$ -qubit quantum circuit

$$\begin{array}{c}
\text{---} \\
\vdots \\
\text{---}
\end{array}
\left\{ \begin{array}{l}
\vdots \\
\vdots \\
\vdots
\end{array} \right.
\begin{array}{|c}
\hline
V \\
\hline
\end{array}
\begin{array}{c}
\text{---} \\
\vdots \\
\text{---}
\end{array}
\begin{array}{|c}
\hline
\text{---} \\
\hline
\vdots \\
\hline
\text{---}
\end{array}
\quad (11)$$

where  $V$  is composed of Clifford gates and  $n$   $T$ -gates, can be implemented with a circuit composed from Clifford gates and classical controls acting on the state  $e_0^{\otimes k} \otimes T^{\otimes n}$  by replacing each  $T$ -gate with the gadget in (10). By *postselecting* outcomes 0 for each measurement on a  $T$ -state in this circuit, we see that

$$V e_0^{\otimes k} = 2^{n/2} \left( \mathbb{1}^{\otimes k} \otimes (e_0^*)^{\otimes n} \right) U \left( e_0^{\otimes k} \otimes T^{\otimes n} \right)$$

where  $U$  is composed from Clifford gates only (more precisely, the Clifford gates from  $V$  plus an additional  $CNOT$  gate for each injected  $T$ -state).

With that, it follows that the probability of outcome  $x_1 \dots x_k$  in the circuit in (11) is given by  $|p_{x_1 \dots x_k}|^2$ , where

$$\begin{aligned}
p_{x_1 \dots x_k} &= \left( e_{x_1}^* \otimes \dots \otimes e_{x_k}^* \right) V e_0^{\otimes k} \\
&= 2^{n/2} \left( e_{x_1}^* \otimes \dots \otimes e_{x_k}^* \otimes (e_0^*)^{\otimes n} \right) U \left( (e_0)^{\otimes k} \otimes T^{\otimes n} \right).
\end{aligned} \quad (12)$$

Note that if there are stabilizer states  $\sigma_1, \dots, \sigma_r$  and complex numbers  $c_1, \dots, c_r \in \mathbb{C}$  such that  $\psi = \sum_{i=1}^r c_i \sigma_i$ , then the quantity in (12) decomposes by linearity as

$$p_{x_1 \dots x_k} = 2^{n/2} \sum_{i=1}^r c_i \left( e_{x_1}^* \otimes \dots \otimes e_{x_k}^* \otimes (e_0^*)^{\otimes n} \right) U \left( (e_0)^{\otimes k} \otimes \sigma_i \right). \quad (13)$$

All summands in (13) can be calculated efficiently using the  $CH$ -form as discussed before: They are amplitudes of the outcome of a quantum circuit composed of Clifford gates acting on a stabilizer state.

Summarizing, every stabilizer decomposition of  $T^{\otimes n}$  yields a way to strongly simulate Clifford+ $T$  circuits consisting of  $n$   $T$ -gates. The complexity of this simulation scales linearly in the number of terms appearing in the stabilizer decomposition and polynomially in all other parameters. With this, it follows that finding decompositions of  $T^{\otimes n}$  into few stabilizer states can reduce the complexity of simulating such circuits. Lower bounds on  $\chi(T^{\otimes n})$ , on the other hand, translate directly into lower bounds on the cost of simulating quantum circuits using these methods, namely, stabilizer decompositions and  $CH$ -forms.