Bound States for Magic State Distillation in Fault-Tolerant Quantum Computation

Earl T. Campbell and Dan E. Browne
Department of Physics and Astronomy, University College London, Gower Street, London, WC1E 6BT, UK.

Magic state distillation is an important primitive in fault-tolerant quantum computation. The magic states are pure non-stabilizer states which can be distilled from certain mixed non-stabilizer states via Clifford group operations alone. Because of the Gottesman-Knill theorem, mixtures of Pauli eigenstates are not expected to be magic state distillable, but it has been an open question whether all mixed states outside this set may be distilled. In this Letter we show that, when resources are finitely limited, non-distillable states exist outside the stabilizer octahedron. In analogy with the bound entangled states, which arise in entanglement theory, we call such states bound states for magic state distillation.

PACS numbers: 03.67.Pp

The significant noise and decoherence in quantum systems means that harnessing these systems for computational tasks must be performed fault tolerantly [12]. In a wide variety of setups only a limited set of gates, known as the Clifford group, are implemented in a manifestly fault tolerant manner. Examples include some anyonic topological quantum computers [3–5], post-selected quantum computers [6, 7] and measurement based topological quantum computers [8]. This motivates the problem of when such devices, with practically error free Clifford gates, may be promoted to a full quantum computer. The celebrated Gottesman-Knill theorem shows that a Clifford circuit acting on stabilizer states — simultaneous eigenstates of several Pauli operators — can be efficiently simulated by a classical computer [9]. However, given a resource of pure non-stabilizer states, we can implement gates outside the Clifford group. For example, a qubit in an eigenstate of the Hadamard enables one to implement a π/8 phase gate that when supplementing the Clifford group gives a dense covering of all unitary operations [10], and so enables universal quantum computation.

Preparation of non-stabilizer states would usually require a non-Clifford operation, so in this context, one would require that even noisy copies of these states enable high fidelity quantum computation. Bravyi and Kitaev [10] showed that this can be achieved. Coining the term magic state distillation, they showed that most mixed non-stabilizer states can be distilled via Clifford group circuits to fewer copies of a lower entropy state, reaching in the limit of infinite iterations a pure non-stabilizer magic state. However, the protocols they presented do not succeed for all mixed non-stabilizer states. Bravyi and Kitaev were not satisfied by the ambiguous status of these states and concluded that “The most exciting open problem is to understand the computational power of the model in [this] region of parameters.”. Either all non-stabilizer states are efficiently distillable by an undiscovered protocol, or there exist non-stabilizer states that are impossible to distill. Such undistillable states we call bound states for magic state distillation, in analogy with bound states in entanglement distillation [11]. Here we make progress by showing that bound states exist for a very broad class of protocols. By showing that a single round of a finite sized protocol will not improve these states, it follows that repeating such a protocol, even with an infinite number of iterations, will also have no benefit. Hence, we explain why all known protocols fail to distill some states.

The single-qubit stabilizer states, for which the Gottesman-Knill theorem applies, are the six pure stabilizer states (the eigenstates of ±X, ±Y and ±Z) and any incoherent mixture of these. In the Bloch sphere, this convex set with 6 vertices forms the stabilizer octahedron partially shown in figure 1. Single-qubit states have density matrices:

$$\rho(f, a) = \frac{1}{2} (1 + (2f-1)(a_X X + a_Y Y + a_Z Z))/2,$$

where $a = (a_X, a_Y, a_Z)$ is a unit vector, and $f$ is the fidelity w.r.t the pure state $|\psi_a\rangle\langle\psi_a| = (1 + a_X X + a_Y Y + a_Z Z)/2$. Stabilizer states satisfy:

$$|2f-1||a_X| + |a_Y| + |a_Z|| \leq 1$$

where the equality holds for states on the surface of the octahedron, and we denote the fidelity of such surface states as $f^S$, which is unique assuming $f \geq 1/2$.

Prior protocols for magic state distillation [7, 10, 12, 13] increase fidelity towards eigenstates of Clifford gates, such as the Hadamard $H$ and the $T$ gate [13]. These eigenstates have $a_H = (1, 0, 0)/\sqrt{2}$ and $a_T = (1, 1, 1)/\sqrt{3}$, with $f = 1$ for ideal magic states. Given the ability to prepare a mixed non-stabilizer state, $\rho$, we can perform an operation called polarization, or twirling, that brings $\rho$ onto a symmetry axis of the octahedron. For example, by randomly applying $\mathds{1}$, $T$ or $T^\dagger$, we map $\rho \rightarrow \rho(f, a_T)$.

Bravyi and Kitaev proposed the following protocol [10] for $|T\rangle$ state distillation: (1) Prepare 5 copies of $\rho(f, a_T)$; (2) Measure the 4 stabilizers of the five-qubit error correcting code; (3) If all measurements give +1, the protocol succeeds and the encoded state is decoded into a single qubit state, and otherwise restart. Upon a successful implementation of this protocol the output qubit has a fidelity $F(f)$ plotted in figure 2. Provided the initial fidelity is greater than some threshold, a successful implementation yields a higher fidelity. This protocol has a non-tight threshold, and exhibits a gap between the threshold and the set of stabilizer states. Because the initial state was twirled onto the T axis, the threshold forms a plane in the Bloch sphere (see figure 1). In contrast, Reichardt has
Theorem 1 Consider a device capable of ideal Clifford gates, preparation of stabilizer states, classical feedforward and Pauli measurements. For any protocol on this device that takes $\rho(f, a_P) \otimes^n$ and outputs a single qubit, $\rho'$, there exists an $\epsilon > 0$ such that $\rho'$ is not an improvement on $\rho(f, a_P)$ for $f \leq f_{S_H}^\epsilon + \epsilon$.

Theorem 1 covers a wide class of protocols, which attain a fidelity that is upper-bounded by a narrower class of protocols $[14]$, such that theorem 1 follows from:

Theorem 2 Consider all protocols that follow these steps: (i) prepare $\rho(f, a_P) \otimes^n$; (ii) measure the $n-1$ generators of an $n$ qubit stabilizer code $S_{n-1}$ with one logical qubit; (iii) post-select on all “+1” measurement outcomes; (iv) decode the stabilizer code and output the logical qubit as the single qubit state $\rho'$. For all such protocols there exists an $\epsilon > 0$ such that $\rho'$ is not an improvement on $\rho(f, a_P)$ for $f \leq f_{S_H}^\epsilon + \epsilon$.

Prior protocols, such as those based on the STEANE code and 5 qubit code, are covered explicitly by theorem 2. Here we use the structure of stabilizer codes to prove theorem 2 with theorem 1 following directly from the results of $[14]$, where such distillation protocols are shown to have equal efficacy with more general Clifford protocols. It is crucial to consider the implication of these theorems when an $n$-qubit protocol is iterated $m$ times. When a single round provides no improvement on the initial resource, the input into the second round will only differ by Clifford group operations, and hence our theorem applies to the second, and all subsequent, rounds. Hence, repeated iteration cannot be used to circumvent our theorem. Before proving these theorems, we derive a pair of powerful lemmas that identify bound states.

Lemma 1 Consider $n$ copies of an octahedron surface state $\rho(f_{S_H}^\epsilon, a_P)$ projected onto the codespace of $S_{n-1}$ and then decoded. If the output qubit is in the octahedron interior, then
there exists an \( \varepsilon > 0 \) such that for \( f \leq f_{a_P}^S + \varepsilon \) the same projection on \( \rho(f, a_P)^{\otimes n} \) also projects onto a mixed stabilizer state.

This lemma follows directly from the dependence of the output on \( f \), which for finite \( n \) is always continuous. We can observe this lemma at work in figure 2. Our next lemma identifies when octahedron surface states are projected into the octahedron interior. Before stating this we must establish some notation. An initial state, \( \rho(f_{a_P}^S, a_P)^{\otimes n} \), is an ensemble of pure stabilizer states:

\[
\rho(f_{a_P}^S, a_P)^{\otimes n} = \sum_{g \in \{X, Y, Z\}^n} g_{\Psi_g} |\Psi_g\rangle \langle \Psi_g|,
\]

where \( |\Psi_g\rangle \) is stabilized, \( g|\Psi_g\rangle = |\Psi_g\rangle \), by the group \( G_g \) generated by \( g = (g_1, g_2, ..., g_n) \). The operator \( g_i \) is \( X_{i}, Y_{i} \) or \( Z_{i} \), with \( i \) labeling the qubit on which it acts. Each contribution has a weighting \( q_g = \prod_{i}(a_{g_i}/(a_{X} + a_{Y} + a_{Z})) \).

Measuring the generators of \( S_{n-1} \) and post-selecting on \(+1\) outcomes, projects the coset of space of \( S_{n-1} \) with projector \( P = \sum_{n \in S_{n-1}} s/2^{n-1} \), producing:

\[
\frac{P\rho(f_{a_P}^S, a_P)^{\otimes n} P}{\text{tr}[P\rho(f_{a_P}^S, a_P)^{\otimes n} P]} = \sum_{g \in \{X, Y, Z\}^n} q_g'|\Psi_{g'}\rangle \langle \Psi_{g'}|,
\]

with projected terms, \( |\Psi_{g'}\rangle \), of new weighting \( q_{g'} \). Each \( |\Psi_{g'}\rangle \) has its stabilizer generated by \((G_g, s_1, s_2, ..., s_{n-1})\), where \( G_g \) is an independent generator that: (a) was present in the initial group \( G_g \in \hat{G_g} \); and (b) commutes with the measurement stabilizers \( G_g S_{n-1} = S_{n-1} G_g \). In other words, it must be equivalent to one of six logical Pauli operators of the coset space. We denote the set of logical operators as \( L \), and its elements \( \pm X_{L}, \pm Y_{L} \), and \( \pm Z_{L} \), and so \( G_g \in L S_{n-1} \). This defines a decoding via the octahedron interior. This proves lemma 2 and we now show that lemma 2 applies to all stabilizer reductions that do not trivially take \( \rho(f, a_P)^{\otimes n} \rightarrow C_1 \rho(f, a_P) C_1^\dagger \).

Our proof continues by finding canonical generators for the code \( S_{n-1} \). A related method has been used to prove that all stabilizer states are local Clifford equivalent to a graph state 11], and we review this first. All stabilizer states have a stabilizer \( S_n \) with \( n \) generators. Each generator is a tensor product of \( n \) single-qubit Pauli operators. This can be visualized as an \( n \) by \( n \) matrix with elements that are Pauli operators, each row a generator and each column a qubit. Different, yet equivalent, generators are produced by row multiplication, via which we can produce a canonical form. In this form column \( i \) has a non-trivial Pauli operator \( A_i \), that appears on the diagonal, and all other operators in that column are either the identity or another operator \( B_j \). Note that \( A_i \) and \( B_i \) compose a third non-trivial Pauli \( A_i B_i = i(-1)^{\gamma_i} C_i \), with \( \gamma_i = 0, 1 \). Hence, all stabilizer states differ from some graph state by only local Clifford that map \((A_i, B_i) \rightarrow (X_i, Z_i)\).

A code, \( S_{n-1} \), has one less generator than the number of qubits, and so more columns than rows. We can apply the diagonalisation procedure on an \( n - 1 \) by \( n - 1 \) submatrix, to bring this submatrix into canonical form. Hence, we can find generators of \( S_{n-1} \) such that:

\[
s_j = (-1)^{\alpha_j} A_j \prod_{k \neq j, n} B_k^{\beta_j k},
\]

where the variables \( \beta_k \) are unspecified. However, if all these generators have \( T_{j,n} = \mathbb{1} \), then the protocol is trivial and projects \( n - 1 \) qubits into a known stabilizer state and the last qubit untouched, and so no improvement is made for any \( f \). Hence, herein we assume the non-trivial case; in particular we assume stabilizer \( T_{n-1,n} \neq \mathbb{1} \). Since, we can always relabel qubits this is completely
general. Furthermore, we can define $T_{n-1,n} = A_n$. Now we can define a logical operator in the codespace of $S_{n-1}$:

$$Z_L = \left( \prod_{1 \leq j \leq n-2} B^{j}\right) B_{n-1}B_n,$$

where the variables $\zeta_j = 0, 1$ are uniquely fixed by commutation relations $Z_L s_j = s_j Z_L$. Note that $Z_L$ has some inbuilt freedom as $B_n$ is not fixed other than that $B_n \neq A_n, Z_n$.

Furthermore, we can define $T$ act on $p$ qubits and output $q$ qubits ($p > q > 1$). This implies that multi-qubit output iterates may suppress the threshold effectively, and are worth further study. Currently, no such protocol is known. As such, in the asymptotic regime, bound magic states may not exist. However, numerical evidence so far indicates that smaller codes tend to produce better thresholds than larger codes. Nevertheless, the theorem does not rule out infinite cases from attaining a tight threshold. In the regime of finite resources, bound states do exist, and it is interesting ask what computational power Clifford circuits acting on such states possess. Can we find methods of efficiently classically simulating bound states; or can bound states be exploited in algorithms that offer a speedup over classical computation?

Furthermore, our proof assumes a protocol acting on identical copies, which invites study into whether our results extend to non-identical copies. In particular, following the analogy with entanglement distillation, we speculate that bound magic states may be distillable via “catalysis”, where some non-consumed distillable resource activates the distillation [11]. Finally we note that noisy Clifford gates can also enable quantum computation [16, 17], and we conjecture that a similar theorem will apply to a class of noisy Clifford gates analogous to states just above the octahedron faces.

The authors would like to thank Shashank Virmani, Matthew Hoban, Tobias Osborne, Ben Reichardt and Steve Flammia for interesting discussions. We acknowledge support from the Royal Commission for the Exhibition of 1851, the QIP IRC, QNET and the National Research Foundation and Ministry of Education, Singapore.

[1] A. Steane, Proc. Roy. Soc. Lond. A 452, 2551 (1996).
[2] D. Gottesman, Phys. Rev. A 57, 127 (1998).
[3] G. Moore and N. Read, Nucl. Phys. B 360, 362 (1991).
[4] S. Lloyd, Quant. Info. Pro. I, 15 (2002).
[5] B. Doucet and J. Vidal, Phys. Rev. Lett. 88, 227005 (2002).
[6] E. Knill, Nature 434, 39 (2005).
[7] B. W. Reichardt, Algorithmica 55, 517 (2009).
[8] R. Raussendorf, J. Harrington, and K. Goyal, New J. Phys. 9, 199 (2007), quant-ph/0703143.
[9] D. Gottesman, Ph.D. thesis, Caltech, quant-ph/9705052.
[10] S. Bravyi and A. Kitaev, Phys. Rev. A 71, 022316 (2005).
[11] P. Horodecki, M. Horodecki, and R. Horodecki, Phys. Rev. Lett. 82, 1056 (1999); D. Jonathan and M. B. Plenio, Phys. Rev. Lett. 83, 3566 (1999).
[12] B. W. Reichardt, Quant. Info. Pro. 4, 251 (2005).
[13] B. W. Reichardt (2006), quant-ph/0608085.
[14] E. T. Campbell and D. E. Browne, L.N.C.S. TQC Workshop 5906, 20 (2009), arXiv:0908.0838
[15] M. V. den Nest, J. Dehaene, and B. D. Moor, Phys. Rev. A 69, 022316 (2004).
[16] M. B. Plenio and S. Virmani (2008), arXiv:0810.4340.
[17] M. Howard and W. van Dam Phys. Rev. Lett. 103, 170504 (2009).
[18] The T gate performs, $T X T^\dagger = Y$, $T Y T^\dagger = Z$. 

†