Changing the Local-Dimension of an Entanglement-Assisted Stabilizer Code Removes Entanglement Need

Lane G. Gunderman

The Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada and
Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada

(Dated: December 25, 2020)

Having protected quantum information is essential to perform quantum computations. One possibility is to reduce the number of particles needing to be protected from noise and instead use systems with more states, so called qudit quantum computers. In this paper we show that codes for these systems can be derived from already known codes, and in particular this procedure removes the need for shared entanglement in entanglement-assisted quantum error-correcting codes, which is a result which could prove to be useful for fault-tolerant qudit, and even qubit, quantum computers.

INTRODUCTION

Having protected quantum information is an essential piece of being able to perform controlled quantum computation operations. There are a variety of methods to help protect quantum information such as those discussed in [1]. In this paper we focus on entanglement-assisted quantum error-correcting codes (EAQECC) as first effectively introduced in [2] and further explored in [3]. EAQECC are similar in nature to stabilizer codes—the quantum analog of linear codes—but differ in their use of entanglement to allow for the immediate importing of many more classical linear codes to the quantum setting. Entanglement is a central resource in quantum computing and the sensitivity of entanglement to errors means that we ought to protect these entangled particles as well, meaning that higher-order error-correction will be required. The qudit version of EAQECC was shown in [4]. In this work we consider EAQECC and show that it is possible to remove this entanglement requirement upon changing the local-dimension. We further show that not only can we remove the entanglement need, but also we can at least preserve the distance of the code, and so improve the utility of the code.

An EAQECC is specified by a set of partly non-commuting Pauli generators. Those generators in the code that do not commute can be written such that any non-commutation relations are resolved through the use of an entangled pair of particles and the teleportation protocol [1]. In the qudit case the entangled pair of particles used is given by:

$$|\Phi_q^+\rangle = \frac{1}{\sqrt{q}} \sum_{i=0}^{q-1} |i, i\rangle$$ \hspace{1cm} (1)

EAQECC allow the dual code space constraint from the Calderbank-Shor-Steane (CSS) theorem to be ignored—allowing any classical code to be imported to the quantum case [2]. This allows for immediate translation of classical error-correcting codes into quantum error-correcting codes so long as a source of shared entanglement is available.

A way to retain a similarly sized computational space while reducing the number of particles that need precise controls and carefully regulated environments is to replace the standard choice of qubits with qudits, quantum particles with $q$ levels. Throughout this work we require $q$ to be a prime so that each nonzero element has a unique multiplicative inverse over $\mathbb{Z}_q$. This restriction can likely be removed, but for simplicity and clarity we only consider this case. Experimental realizations of these systems are currently underway [5][6][7], so having more error-correcting codes will aid in protecting such systems. Prior work on qudit error-correcting codes have often had challenging restrictions between the parameters of the code [8][9][10], and we’ve already made progress on reducing this barrier in a prior paper [11]. Our prior work showed the ability to make error-correcting codes that preserved their parameters, generally, even upon changing the local-dimension of the system. Beyond this, these systems also have proven connections to foundational aspects of physics [12].

DEFINITIONS

In this section, we recall common definitions and results for qudit operators. A qubit is defined as a two level system with states $|0\rangle$ and $|1\rangle$. We define a qudit as being a quantum system over $q$ levels, where $q$ is prime. Throughout we take $\mathbb{Z}_q$ as the set $\{0, 1, \ldots, q-1\}$.

Definition 1. Generalized Paulis for a space over $q$ orthogonal levels, where we assume $q$ is prime, are given by:

$$X_q|j\rangle = |(j + 1) \mod q\rangle, \quad Z_q|j\rangle = \omega^j|j\rangle$$ \hspace{1cm} (2)

with $\omega = e^{2\pi i/q}$, where $j \in \mathbb{Z}_q$. These Paulis form a group, denoted $\mathbb{P}_q$.

When $q = 2$, these are the standard qubit operators. This group structure is preserved over tensor products since each of these Paulis has order $q$. 
As shown in [13], an EAQECC is specified by $s$ commuting Pauli operators and a set of $c$ Pauli operator pairs $\{X_i, Y_i\}$ such that:

$$X_i \circ Y_i \neq 0, \quad \forall i$$

while all other operators commute. We let $k = s + 2c$ be the total number of Pauli operators used to specify the code. Note that this is slightly different from the standard choice as this work focuses on the total number of generators opposed to many works which focus more on the number of encoded particles.

Although the generators in an EAQECC do not all commute, they do form a group. The entirety of the group, with the scalar coefficient quotiented out, is composed of all possible compositions ($\circ$) of the generators. This forms a subgroup of size $q^k$ as each generator has order $q$. This then leads to there being $q^{n-k}$ orthonormal basis states, or codewords.

Finding the commutator of these generators with an error provides the syndrome of that error. These syndromes provide insight into which error may have occurred so that we can determine the error and potentially undo it.

The standard choice of error model is the depolarizing channel which depends on the weights of the errors:

**Definition 2.** The weight of an $n$-qudit operator is given by the number of non-identity operators in it.

**Definition 3.** An EAQECC, specified by its generators, is characterized by a set of parameters:

- $n$: the number of qudits that the states are over
- $n-k$: the number of encoded (logical) qudits
- $d$ (for non-degenerate codes (where all group members have weight at least $d$)): the distance of the code, given by the lowest weight of an undetectable generalized Pauli error (commutes with all elements of the group, but is not in the group itself)
- $c$: the number of entangled pairs needed in order to resolve commutation relations between the generators of the code

These values are specified for a particular code as: $[[n, n-k, d; c]]_q$, where $q$ is the local-dimension of the qudits.

The minimal value of $c$ needed for a particular set of generators was shown in [13]. Working with tensors of operators can be challenging, and so we make use of the following well-known mapping from these to vectors, following the notation from [11]. This linear algebraic representation will be used for our proofs here.

**Definition 4** ($\phi$ representation of a qudit operator). We define the surjective map:

$$\phi_q : \mathbb{P}^n_q \mapsto \mathbb{Z}^{2n}_q$$

which carries an $n$-qudit Pauli in $\mathbb{P}^n_q$ to a $2n$ vector mod $q$, where we define this map as:

$$\phi_q(\omega^a \otimes I_{i-1} I \otimes X_q^a Y_q^b \otimes n-i) = (0^{n-1} a 0^{n-i} 0^{n-1} b 0^{n-i})$$

which puts the power of the $i$-th $X$ operator in the $i$-th position and the power of the $i$-th $Z$ operator in the $(i + n)$-th position of the output vector. This mapping is defined as a homomorphism with: $\phi_q(s_1 \circ s_2) = \phi_q(s_1) \oplus \phi_q(s_2)$, where $\oplus$ is component-wise addition mod $q$. We denote the first half of the vector as $\phi_{q,x}$ and the second half as $\phi_{q,z}$.

We may invert the map $\phi_q$ to return to the original $n$-qudit Pauli operator with the global phase being undetermined. We make note of a special case of the $\phi$ representation:

**Definition 5.** Let $q$ be the dimension of the initial system. Then we denote by $\phi_\infty$ the mapping:

$$\phi_\infty : \mathbb{P}^n_q \mapsto \mathbb{Z}^{2n}_q$$

where no longer are any operations taken mod some base, but instead carried over the full set of integers.

The ability to generally define $\phi_\infty$ as a homomorphism still (and with the same rule) is a portion of the results of this paper–shown in Theorem 8. $\phi_q$ is the standard choice for working over $q$ bases, however, our $\phi_\infty$ allows us to avoid being dependent on the local-dimension of our system when working with our code. In general we will write a code in $\phi_q$, perform some operations, then write it in $\phi_\infty$. We shorten this to write it as $\phi_\infty$, and can later select to write it as $\phi_q'$ for some prime $q'$ by taking element-wise mod $q'$. The commutator of two operators in this picture is given by the following definition:

**Definition 6.** Let $s_i, s_j$ be two qudit Pauli operators over $q$ bases, then these commute if and only if:

$$\phi_q(s_i) \circ \phi_q(s_j) = 0 \mod q$$

where $\circ$ is the symplectic product, defined by:

$$\phi_q(s_i) \circ \phi_q(s_j) = \oplus_k [\phi_{q,x}(s_j)_k \cdot \phi_{q,x}(s_i)_k - \phi_{q,x}(s_j)_k \cdot \phi_{q,x}(s_i)_k]$$

where $\cdot$ is standard integer multiplication mod $q$ and $\oplus$ is addition mod $q$.

Before finishing, we make a brief list of some possible operations we can perform on our $\phi$ representation for an EAQECC:

1. We may perform elementary row operations over $\mathbb{Z}_q$, corresponding to relabelling and composing generators together.
2. We may swap registers (qudits) in the following ways:

(a) We may swap columns (Reg $i$, Reg $i+n$) and (Reg $j$, Reg $j+n$) for $0 < i, j \leq n$, corresponding to relabelling qudits.

(b) We may swap columns Reg $i$ and $(-1)\cdot$Reg $i+n$, for $0 < i \leq n$, corresponding to conjugating by a Hadamard gate on register $i$ (or Discrete Fourier Transforms in the qudit case [14]) thus swapping $X$ and $Z$'s roles on that qudit.

All of these operations leave the parameters $n$, $k$, and $d$ alone, but can be used in proofs.

**LOCAL-DIMENSION-INVARIANT EAQECC**

In this section we prove how to remove the entanglement need from EAQECC and under what conditions we can promise the distance of the code is at least preserved.

**Definition 7.** A code is called effectively local-dimension-invariant if all generators commute over $p$ levels, $p \neq q$, upon evaluating all entries at a pre-determined function of $p$ while the original code over $q$ is unchanged.

The key observation needed to show this is that we may break up the commutator of the generators over the levels need from EAQECC and under what conditions we can promise the distance of the code is at least preserved.

Let $\nu = 0 \mod p$, with $\nu \in \mathbb{Z}_p$. Set $n_{ij} = -\nu^{-1}\alpha_{ij}$, then $\alpha_{ij} + n_{ij}\nu \mod p = 0$, but also $\alpha_{ij} + n_{ij}\nu = \alpha_{ij} + n_{ij}q \mod p$, and so $\alpha_{ij} + n_{ij}q = 0 \mod p$. Lastly, setting $L_{ij} = (m_{ij} - n_{ij})q$ and adding this lower triangular matrix enforces commutation over $p$.

Notice that in the above proof the inability to perform this operation over $q$ is manifest as $\nu^{-1}$ is not defined as $0$ never has a multiplicative inverse. Before moving on, we make note a couple of crucial cases in the above proof. When $p > q$ then $L_{ij} = \alpha_{ij}$ and $\nu^{-1} = q^{-1} \mod p$. When $p = 2$, $L_{ij} = \alpha_{ij} + (q-1)\alpha_{ij}$. The only cases where the code is not truly local-dimension-invariant but only effectively local-dimension-invariant is when $2 < p < q$.

This merely transforms an EAQECC into a set of commuting generators. Following Theorem 16 from [11], note that we can always rewrite this as $c_{ij} = \alpha_{ij} + n_{ij}q + (m_{ij} - n_{ij})q$ such that $\alpha_{ij} + n_{ij}q \mod p = 0$, which allows for the removal of all entanglement requirements from the code. The following proof is similar to the original invariant procedure from [11], but requires care around particular cases.

**Theorem 8.** All EAQECC over $q$ levels can be made into an effectively local-dimension-invariant stabilizer code.

**Proof.** Let $S$ be an EAQECC with parameters $[[n, k; d; c]]_q$, we may write this code as $\phi_q(S)$. When using the initial generators of $S$ in $\phi_q(S)$, the symplectic product matrix $[\circ]_q$ will have exactly $2c$ nonzero entries corresponding to the generators whose commutators need to be resolved via entanglement. We will now allow the number of nonzero entries to change by transforming $\phi_q(S)$ via the rules outlined earlier to an EAQECC canonical form:

$$\phi_q(S) = [I_k \ X_2 \ | \ Z_1 \ Z_2]$$

where $Z_1$ is a $k \times k$ matrix. Let $[\circ]_\infty$ be the antisymmetric commutator matrix, written over the integers. We will add a lower triangular matrix $L$ to $Z_1$ such that after this addition we leave the code alone over $mod q$, and yet have $[\circ]_\infty = 0$.

Let $c_{ij} = [[\circ]_\infty]_{ij} = \phi_\infty(s_i) \circ \phi_\infty(s_j)$. Then for the updated generators, $S'$, we have:

\begin{align}
\phi_\infty(s_i') \circ \phi_\infty(s_j') &= [\phi_\infty(s_i) + (0 \ | \ L_i \ 0)] \circ [\phi_\infty(s_j) + (0 \ | \ L_j \ 0)] \\
&= \phi_\infty(s_i) \circ \phi_\infty(s_j) + \phi_\infty(s_i) \circ (0 \ | \ L_j \ 0) + (0 \ | \ L_i \ 0) \circ \phi_\infty(s_j) + (0 \ | \ L_i \ 0) \circ (0 \ | \ L_j \ 0) \\
&= c_{ij} + L_{ij} + 0 \\
&= \alpha_{ij} + n_{ij}q + (m_{ij} - n_{ij})q - L_{ij}.
\end{align}

Let $\nu = q \mod p$, with $\nu \in \mathbb{Z}_p$. Set $n_{ij} = -\nu^{-1}\alpha_{ij}$, then $\alpha_{ij} + n_{ij}\nu \mod p = 0$, but also $\alpha_{ij} + n_{ij}\nu = \alpha_{ij} + n_{ij}q \mod p$, and so $\alpha_{ij} + n_{ij}q = 0 \mod p$. Lastly, setting $L_{ij} = (m_{ij} - n_{ij})q$ and adding this lower triangular matrix enforces commutation over $p$.

Notice that in the above proof the inability to perform this operation over $q$ is manifest as $\nu^{-1}$ is not defined as $0$ never has a multiplicative inverse. Before moving on, we make note a couple of crucial cases in the above proof. When $p > q$ then $L_{ij} = \alpha_{ij}$ and $\nu^{-1} = q^{-1} \mod p$. When $p = 2$, $L_{ij} = \alpha_{ij} + (q-1)\alpha_{ij}$. The only cases where the code is not truly local-dimension-invariant but only effectively local-dimension-invariant is when $2 < p < q$.

This merely transforms an EAQECC into a set of commuting generators. Following Theorem 16 from [11],

in order to make statements about the distance of this transformed code we must bound the maximal entry in $\phi_\infty(S')$:

**Corollary 9.** The maximal entry in $\phi_\infty(S')$, $B$, when $p > q$ satisfies:

$$B \leq |2 + (n-k)(q-1)|(q-1).$$

**Proof.** We begin by noting from our prior work that we have $c_{ij} \leq B - (q-1)$, where $B$ is given by $|2 + (n-k)(q-1)|(q-1)$ [11]. Here we have:

\begin{align}
L_{ij} &= (m_{ij} + \nu^{-1}\alpha_{ij})q \\
&= \alpha_{ij} + m_{ij}q + (\nu^{-1}q - 1)\alpha_{ij} \\
&= c_{ij} + (q^{-1}q - 1)\alpha_{ij} \\
&\leq B - (q-1).
\end{align}
Then the maximal entry is upper bounded by \( B - (q - 1) + (q - 1) = B \), which is the same as for stabilizer codes and any tightening on the bound of \( B \) there will apply in this bound as well.

Applying this entry bound, then the EAQECC will have at least the same distance, according to Theorem 16 from [11], if brought from \( q \) levels to \( p \) levels with \( p > p' \), where \( p^* = B^{2(d-1)}/2(d - 1)(d-1) \). This immediately provides the following theorem:

**Theorem 10.** We may transform a non-degenerate \([n, n - k, d; c]]_q\) EAQECC into a \([n, n - k, d'; 0]]_p\) stabilizer code with \( d' \geq d \) so long as \( p \) is a prime with \( p > p^* \).

Using the same reasoning as in our prior work, we can also define logical operators for these codes [11]. Putting together all the results, we have defined quantum error-correcting codes which can protect information, remove entanglement use, and have logical operators, and while the distance of the code can only be promised at sufficiently many bases, it is possible to preserve the distance even below this cutoff as the following examples show.

We now apply this procedure to the \([4, 0, 3; 1]]_2\) code from [3]:

\[
(ZXZI, ZZIZ, YXXZ, ZYYX).
\]  

We put this into canonical form by applying a Hadamard on particle four, then performing RREF. Applying Theorem 8, we obtain an invariant form of:

\[
\begin{bmatrix}
1 & 0 & 0 & 0 & | & 1 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & | & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & | & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & | & 1 & 2 & -1 & 0
\end{bmatrix}
\]  

(20)

This code has \( d = 3 \) for \( p > 3 \) as no linear combination of columns corresponding to weight two Paulis are linearly dependent. We have transformed this into a \([4, 0, 3; 0]]_p\) code for \( p > 3 \). Note that this does not mean for \( p = 3 \) it is not possible to modify the code such that the distance is still preserved, just that this prescriptive method does not provide it given the canonical form used.

A more concise way to summarize this result is by considering the rate of this code upon performing this transformation. This technique improves the rate of an EAQECC in the following ways, following the definitions from [13]:

- The trade-off rate is altered from \((n - k)/n, c/n\) to \((n - k)/n, 0\).
- The catalytic rate is altered from \((n - k - c)/n \) to \((n - k)/n\).

In both cases the code now matches the entanglement-assisted rate. Both of these improvements require the pair of caveats that: one, the local-dimension must be changed, and, two, these rate improvements are only proper so long as the distance of the code is also at least preserved. If the distance is not preserved, the rate will improve still, but the quality of protection for the code has dropped making the comparison on unequal footing.

**FUTURE DIRECTIONS**

While the above example considered \( p > q \), the following example shows that it’s possible to have \( p < q \) and still obtain at least as good parameters:

\[
\begin{bmatrix}
0 & 11 & 3 & 4 & | & 12 & 11 & 11 & 12 \\
14 & 6 & 14 & 9 & | & 13 & 8 & 5 & 0 \\
4 & 13 & 10 & 11 & | & 10 & 1 & 3 & 2 \\
0 & 13 & 4 & 9 & | & 11 & 5 & 0 & 0
\end{bmatrix}
\]  

(21)

This is a \([4, 0, 2; 2]]_5\) code as well as a \([4, 0, 3; 0]]_3\) code. Not only does the application of this result remove the need for entanglement for this code, but it also improved the distance of the code.

Our final theorem provides a promise on the distance of the code. For choices of \( p < p^* \) one would need to computationally check whether the distance of the code is at least preserved. As remarked before, this procedure for making the code effectively local-dimension-invariant is not unique. Even if the distance is not preserved at a value of \( p \) using this procedure, it does not mean that there is not another procedure which will preserve the distance of the code while obtaining the entanglement removal. We have not yet been able to find a procedure which always preserves the distance for \( p > q \), but believe that it is possible, and so leave this as a future direction.

In this work we’ve proven a method to remove the needed entanglement in EAQECC upon changing the local-dimension as well as conditions to ensure the distance of the code remains. This provides another use of local-dimension-invariant stabilizer codes, and so naturally there are questions as to what other uses this technique will have. In addition to this method, is it possible to apply this technique to show some foundational aspect of quantum measurements? Beyond this, this work also makes the challenge of reducing \( p^* \) more crucial than before as it would reduce the number of values of \( p \) that need to have their distance computationally checked.

**ACKNOWLEDGMENTS**

We thank Arun Moorthy for help with writing a program to generate the example from equation (21) and David Cory for helpful feedback.
FUNDING

This work was supported by Industry Canada, the Canada First Research Excellence Fund (CFREF), the Canadian Excellence Research Chairs (CERC 215284) program, the Natural Sciences and Engineering Research Council of Canada (NSERC RGPIN-418579) Discovery program, the Canadian Institute for Advanced Research (CIFAR), and the Province of Ontario.

*lgunderman@uwaterloo.ca*

[1] Daniel A Lidar and Todd A Brun. Quantum error correction. Cambridge university press, 2013.

[2] Charles H Bennett, David P DiVincenzo, John A Smolin, and William K Wootters. Mixed-state entanglement and quantum error correction. Physical Review A, 54(5):3824, 1996.

[3] Todd Brun, Igor Devetak, and Min-Hsiu Hsieh. Correcting quantum errors with entanglement. science, 314(5798):436–439, 2006.

[4] Lan Luo, Zhi Ma, Zhengchao Wei, and Riguang Leng. Non-binary entanglement-assisted quantum stabilizer codes. Science China Information Sciences, 60(4):42501, 2017.

[5] Pei Jiang Low, Brendan M White, Andrew Cox, Matthew L Day, and Crystal Senko. Practical trapped-ion protocols for universal qudit-based quantum computing. arXiv preprint arXiv:1907.08569, 2019.

[6] Poolad Imany, Jose A Jaramillo-Villegas, Mohammed S Ahsaykh, Joseph M Lukens, Ogaga D Odele, Alexander J Moore, Daniel E Leaard, Minghao Qi, and Andrew M Weiner. High-dimensional optical quantum logic in large operational spaces. npj Quantum Information, 5(1):1–10, 2019.

[7] Rahul Sawant, Jacob A Blackmore, Philip D Gregory, Jordi Mur-Petit, Dieter Jaksch, Jesus Aldegunde, Jeremy M Hutson, MR Tarbutt, and Simon L Cornish. Ultracold polar molecules as qudits. New Journal of Physics, 22(1):013027, 2020.

[8] Avanti Ketkar, Andreas Klappenecker, Santosh Kumar, and Pradeep Kiran Sarvepalli. Nonbinary stabilizer codes over finite fields. IEEE Transactions on Information Theory, 52(11):4892–4914, 2006.

[9] Yang Liu, Ruihu Li, Guanmin Guo, and Junli Wang. Some nonprimitive bch codes and related quantum codes. IEEE Transactions on Information Theory, 65(12):7829–7839, 2019.

[10] Xiaoshan Kai, Shixin Zhu, and Ping Li. Constacyclic codes and some new quantum mds codes. IEEE Transactions on Information Theory, 60(4):2080–2086, 2014.

[11] Lane G Gunderman. Local-dimension-invariant qudit stabilizer codes. Physical Review A, 101(5):052343, 2020.

[12] Mark Howard, Joel Wallman, Victor Veitch, and Joseph Emerson. Contextuality supplies the ‘magic’ for quantum computation. Nature, 510(7505):351–355, 2014.

[13] Mark M Wilde and Todd A Brun. Optimal entanglement formulas for entanglement-assisted quantum coding. Physical Review A, 77(6):064302, 2008.

[14] Daniel Gottesman. Fault-tolerant quantum computation with higher-dimensional systems. In NASA International Conference on Quantum Computing and Quantum Communications, pages 302–313. Springer, 1998.

[15] Mark M Wilde and Todd A Brun. Entanglement-assisted quantum convolutional coding. Physical Review A, 81(4):042333, 2010.