



Nonbinary Error-Detecting Hybrid Codes

Andrew Nemeč

Andreas Klappenecker

nemeca@tamu.edu

klappi@cse.tamu.edu

Department of Computer Science & Engineering, Texas A&M University
College Station, Texas

ABSTRACT— Hybrid codes simultaneously encode both quantum and classical information, allowing for the transmission of both across a quantum channel. We construct a family of nonbinary error-detecting hybrid stabilizer codes that can detect one error while also encoding a single classical bit over the residue class rings Zq inspired by constructions of nonbinary non-additive codes.

CCS CONCEPTS

- **Hardware**→Quantum error correction and fault tolerance;
- **Theory of computation**→Quantum information theory.

KEYWORDS

quantum error-correction, nonbinary codes, hybrid codes.

1. INTRODUCTION

Hybrid codes allow for the simultaneous transmission of both quantum and classical information across a quantum channel. While it has long been known that simultaneous transmission can provide an advantage over the time-sharing of the channel for certain small error rates, see [4], most of the early work on the topic focused on information-theoretic results, see [7, 8, 25], while the problem of constructing finite-length hybrid codes remained largely overlooked.

The first examples of hybrid codes were given by Kremsky, Hsieh, and Brun [15], who introduced them as a generalization of entanglement-assisted stabilizer codes. Later, Grassl, Lu, and Zeng [5] gave multiple examples of small hybrid codes constructed using an approach inspired by the construction of nonadditive codeword stabilized quantum codes. Remarkably, these codes provide an advantage over optimal quantum codes regardless of the error rate. Recently, several families of hybrid codes have been constructed including several families constructed by the authors [20] for the Pauli channel using stabilizer pasting and a family constructed by Li, Lyles, and Poon [16] for fully correlated quantum channels. An operator-theoretic approach to hybrid codes has also been put forward in [2, 3, 18].

In [20], the authors constructed several families of binary hybrid codes with good parameters, including a family of $[[n, n - 3; 1, 2]]_2$ error-detecting codes where n is odd. In this paper we provide a generalization of this family to hybrid stabilizer codes over Zq , inspired by the non-additive nonbinary quantum codes constructed from qudit graph states by Hu et al. [9] and Looi et al. [17], as well as the family of single error-detecting codes given by Smolin, Smith, and Wehner [24].

1.1 Nonbinary Quantum Codes

A quantum code is a subspace of a Hilbert space that allows for the recovery of encoded quantum information even in the presence of arbitrary errors on a certain number of physical qudits. A quantum code has parameters $[[n, K, d]]_q$ if and only if it can encode a superposition of K orthogonal quantum states into the Hilbert space $Cq \otimes n \div Cqn$, while protecting the quantum information against all errors

occurring on less than d physical qubits.

Most generalizations of quantum codes from the binary alphabets to the case where $q > 2$ are constructed over the finite fields Fq , where q is a prime power, see [1, 10, 21]. In this paper, we instead follow [9, 17, 24] and construct codes over Zq for reasons that will become apparent in Section 2. Let $a, b \in Zq$. We define the unitary operators $X(a)$ and $Z(b)$ on Cq as

$$X(a)|x\rangle = |x+a\rangle \text{ and } Z(b)|x\rangle = \omega^{bx}|x\rangle,$$

where $\omega = e^{2\pi i/q}$. The operators $X(a)$ and $Z(b)$ may be viewed as a generalization of the Pauli-X bit-flip error and the Pauli-Z phase error respectively. The set $\mathcal{E} = \{X(a)Z(b) | a, b \in Zq\}$ forms a nice error basis on C^q see [11–13], meaning any error on a single qudit may be written as a linear combination of elements from \mathcal{E} . Additionally, any error on Cq^n may be written as a linear combination of errors from $\mathcal{E}_n = \mathcal{E}^{\otimes n} = \{E_1 \otimes E_2 \otimes \dots \otimes E_n | E_k \in \mathcal{E}, 1 \leq k \leq n\}$. By correcting errors from \mathcal{E}_n we are able to deal with arbitrary errors on the n qudits that are linear combinations of those errors. The weight $\text{wt}(E)$ of an error $E \in \mathcal{E}_n$ is the number of non-identity tensor components it contains.

A quantum code C has the ability to detect an error $E \in \mathcal{E}_n$ if it either reports that an error occurred or reports no error and returns a projection of the message back onto C . Formally, the Knill-Laflamme conditions tell us that an error E is detectable by a quantum code C if and only if $PEP = \lambda EP$ for some scalar $\lambda \in Fq$, where P is the orthogonal projector onto C , see [14].

Stabilizer codes are perhaps the most important class of quantum codes, and are analogous to the linear and additive codes in classical coding theory (hence they are also referred to as additive codes). Stabilizer codes are completely determined by their stabilizer group S , an abelian subgroup of \mathcal{E}_n , and the code is defined as the subspace spanned by all joint eigenvectors of S with eigenvalue 1. Since this subspace will always have dimension $K = q^k$, we say the code has parameters $[[n, k, d]]_q$ to denote it as a stabilizer code.

1.2 Hybrid Codes

In addition to transmitting quantum information, we now want to simultaneously encode a classical message in with the encoded quantum state. A hybrid code has parameters $((n, K; M, d))_q$ if and only if it can simultaneously encode a superposition of K orthogonal quantum states as well as one of M different classical states into $(C^q)^{\otimes n} \cong C^{qn}$ a Hilbert space of dimension q^n , while protecting both the quantum and classical information against all errors of weight less than d .

An $((n, K; M, d))_q$ hybrid code C can be described by a collection of M orthogonal quantum codes C_m of dimension K , each indexed by a classical message $m \in [M] = \{0, 1, \dots, M-1\}$. To transmit a quantum state ϕ and a classical message m , we encode ϕ into the quantum code C_m . The Knill-Laflamme conditions for quantum codes can be generalized to hybrid codes, allowing us to characterize detectable errors: an error E is detectable by the hybrid code C if and only if



$$P_b E P_a = \begin{cases} -\lambda E, a P_a & \text{if } a = b, \\ 0 & \text{if } a \neq b \end{cases} \quad (1)$$

for some scalar $\lambda E, a$ depending on both the error E and the classical message a , where P_a is the orthogonal projector onto the quantum code C_a . Equivalently, if $\{|c_i^{(m)}\rangle\}$ are the codewords of the inner code C_m , we have that E is detectable by C if and only if

$$\langle c_j^{(b)} | E | c_i^{(a)} \rangle = \lambda_{E,a} \delta_{i,j} \delta_{a,b}. \quad (2)$$

If both the inner codes and outer code happen to be stabilizer codes, we say the code is a hybrid stabilizer code with parameters $[[n, k; m, d]]_q$. In this case, the codes have some additional structure, so each inner code can be viewed as a translation from a seed code C_0 by an operator $t_m \in E_n \setminus Z(S_0)$, where $Z(S_0)$ is the centralizer in E_n of the stabilizer S_0 of the seed code C_0 , so that $C_m = t_m C_0$. There are multiple simple constructions of hybrid codes using quantum codes described by Grassl et al. [5]:

- Hybrid codes can be constructed using the following "trivial" constructions:
 - Given an $((n, KM, d))_q$ quantum code of composite dimension KM , there exists a hybrid code with parameters $((n, K; M, d))_q$.
 - Given an $[[n, k; m, d]]_q$ hybrid code with $k > 0$, there exists a hybrid code with parameters $[[n, k-1; m+1, d]]_q$.
 - Given an $[[n_1, k_1, d]]_q$ quantum code and an $[[n_2, m_2, d]]_q$ classical code, there exists a hybrid code with parameters $[[n_1+n_2, k_1; m_2, d]]_q$. In each of these cases the sender is effectively substituting classical information for quantum information, which depending on the context may be considered wasteful. In [5], Grassl et al. showed it was possible to construct genuine hybrid codes that provide an advantage over these simple codes, and provided examples of such codes found using an exhaustive search of small parameters. In [20] the authors constructed several infinite families of genuine hybrid codes, including a family of binary single error-detecting codes which we generalize to the nonbinary case in the next section.

2 FAMILY OF HYBRID CODES OVER Z_q

The first good non-additive quantum code (that is a quantum code that is not a stabilizer code) was the $((5, 6, 2))_2$ code given by Rainset al. [23]. This code outperforms the optimal $[[5, 2, 2]]_2$ stabilizer code, and was further generalized by Rains [22] into a family of odd-length non-additive codes that outperform optimal stabilizer codes. However, for an odd-length $((n, K, 2))$ quantum code we have the following bound:

$$K \leq 2^{n-2} \left(1 - \frac{1}{n-1}\right) \quad (3)$$

and many families of codes that approach this bound have been constructed. In [20], the authors gave a construction for a family of hybrid stabilizer codes with parameters $[[n, n-3; 1, 2]]_2$ that beat this bound.

Nonbinary quantum codes with similar parameters were hinted at by Rains in [22], and first given by Smolin et al. [24] as a generalization of their family of non-additive binary codes. Soon after, further families were constructed by Hu et al. [9] and Looi et al. [17] using qudit graph states. All of these families are codes over integerrings rather than finite fields, and our construction of nonbinary hybrid stabilizer codes will follow in their footsteps. The reason we

choose to construct codes over Z_q rather than F_q is due to the following result of Grassl and Rötteler:

Theorem 1 ([6, Theorem 12]). Let $q > 1$ be an arbitrary integer, not necessarily a prime power. Quantum MDS codes $C = [[n, n-2, 2]]_q$ exist for all even length n , and for all length $n \geq 2$ when the dimension q of the quantum systems is an odd integer or is divisible by 4.

While the construction below will certainly produce a hybrid stabilizer code when $q \equiv 2 \pmod{4}$, it will not be a genuine hybrid code, as the previous theorem implies that there will be an

$[[n, n-2, 2]]_q$ stabilizer code that can be transformed into a hybrid code using the first construction in Proposition 1. When $q = 2$, Equation 3 tells us that there can be no $[[n, n-2, 2]]_2$ quantum code, implying that the family given in [20] is indeed genuine. To the best of our knowledge there are no known $[[n, n-2, 2]]_q$ codes when $q = 4r+2$, which is why the codes using the construction below may in fact be genuine. However, since F_{4r+2} does not exist except when $r = 0$, we instead construct our codes over Z_q .

Proposition 2. Let n be odd. Then there exists an $[[n, n-3; 1, 2]]_{Z_q}$

hybrid code.

Proof. Let $a, b \in Z_n q$, $m \in Z_q$, and ω a primitive q -th root of unity. Define the following states:

$$|\phi_{a,b}\rangle = \frac{1}{q^n} \sum_{c \in Z_q^n} \omega^{\sum_{i=1}^n (c_{2i-1} - a_i)} |C\rangle$$

$$|\Psi_m\rangle = \frac{1}{\sqrt{q}} \sum_{c \in Z_q} \omega^{mc} |c\rangle$$

Define the inner code C_m as follows:

$$C_m = \{ |\phi_{a,b}\rangle \otimes |\psi_m\rangle \mid a, b \in Z_q, \sum_{i=1}^n a_i = 0, \sum_{i=1}^n b_i = m \}$$

The state $|\Psi_{a,b}\rangle$ is the tensor product of two-qubit states of the form

$$|\phi_{a_i, b_i}\rangle = \frac{1}{q} \sum_{c \in Z_q^2} \omega^{(c_1 - a_i)(c_2 - b_i)} |c\rangle$$

For two of these states

$$|\phi_{a_i, b_i}\rangle, |\phi_{a'_i, b'_i}\rangle \text{ we have}$$

$$\begin{aligned} \langle \phi_{a_i, b_i} | \phi_{a'_i, b'_i} \rangle &= \frac{1}{q^2} \sum_{c \in Z_q^2} \omega^{(c_1 - a_i)(c_2 - b_i) - (c_1 - a'_i)(c_2 - b'_i)} \\ &= \frac{\omega^{a'_i b'_i - a_i b_i}}{q^2} \sum_{c \in Z_q^2} \omega^{c_1 (b'_i - b_i) + c_2 (a_i - a'_i)} \\ &= \frac{\omega^{a'_i b'_i - a_i b_i}}{q^2} \left(\sum_{c_1 \in Z_q} \omega^{c_1 (b'_i - b_i)} \right) \left(\sum_{c_2 \in Z_q} \omega^{c_2 (a_i - a'_i)} \right) \\ &= \begin{cases} 1 & \text{if } a_i = a'_i \text{ and } b_i = b'_i \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

Therefore for the full states $|\phi_{a,b}\rangle, |\phi_{a',b'}\rangle$ we have the same:

$$\langle \phi_{a,b} | \phi_{a',b'} \rangle = \begin{cases} 1 & \text{if } a = a' \text{ and } b = b' \\ 0 & \text{otherwise} \end{cases}$$

Similarly, for $|\psi_m\rangle, |\psi_{m'}\rangle$ we have

$$\langle \psi_m | \psi_{m'} \rangle = \begin{cases} 1 & \text{if } m = m' \\ 0 & \text{otherwise} \end{cases}$$

Thus all of the codewords are orthogonal to one another.

Consider two codewords $|\phi_{a,b}\rangle \otimes |\psi_m\rangle, |\phi_{a',b'}\rangle \otimes |\psi_{m'}\rangle$ Suppose



that a Pauli-X(u) error occurs on the first n - 1 qudits. Without loss of generality, we can assume that the error occurred on either the first or second qudit. If $m \neq m', a_i \neq a'_i$, or $b_i \neq b'_i$ for $1 < i \leq n$, then

$$\langle \langle \psi_{a,b} | \otimes \langle \psi_m | \rangle X(u) (| \phi_{a',b'} \rangle \otimes | \psi_{m'} \rangle) \rangle = 0$$

by the orthogonality relations above. Therefore we can restrict our attention to the case where $m = m', a_i = a'_i$ and $b_i = b'_i$

for ($1 < i \leq n$). We note that these restrictions along with the requirement that the a_i and a'_i sum to 0 and b_i and b'_i sum to 0 and $m = m'$ respectively completely determine the values a_i and b_i and in particular we must have $a_1 = a'_1$ and $b_1 = b'_1$. If the error

occurred on the first qudit, we have

$$\langle \phi_{a_1, b_1} | X(u) | \phi_{a_1, b_1} \rangle$$

$$\begin{aligned} &= \frac{1}{q^2} \left(\sum_{c \in \mathbb{Z}_q^2} \omega^{-(c_1 - a_1)(c_2 - b_1)} \langle c_1 c_2 | \right) \left(\sum_{c \in \mathbb{Z}_q^2} \omega^{(c_1 - a_1)(c_2 - b_1)} | c_1 c_2 \rangle \right) \\ &= \frac{1}{q^2} \left(\sum_{c \in \mathbb{Z}_q^2} \omega^{-(c_1 - a_1)(c_2 - b_1)} \langle c_1 c_2 | \right) \left(\sum_{c \in \mathbb{Z}_q^2} \omega^{(c_1 - a_1 - u)(c_2 - b_1)} | c_1 c_2 \rangle \right) \\ &= \frac{1}{q^2} \sum_{c_2 \in \mathbb{Z}_q^2} \omega^{u(b_1 - c_2)} \\ &= \begin{cases} 1 & \text{if } u = 0 \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

A similar argument holds if the error occurs on the second qudit, thus the code can detect any single Pauli-X(u) error that occurs on the first n - 1 qudits. Now suppose that a Pauli-Z(v) error occurs on the first n - 1 qudits. As above, we restrict our attention to the case where $a = a', b = b'$ and $m = m'$, and the error occurs on one of the first two qudits. If the error occurs on the first qudit we have

$$\begin{aligned} &\langle \phi_{a_1, b_1} | Z(v) | \phi_{a_1, b_1} \rangle \\ &= \frac{1}{q^2} \sum_{c \in \mathbb{Z}_q^2} \omega^{(c_1 - a_1)(c_2 - b_1) - (c_1 - a_1)(c_2 - b_1) + v c_1} \\ &= \frac{1}{q} \sum_{c \in \mathbb{Z}_q^2} \omega^{v c_1} \\ &= \begin{cases} 1 & \text{if } v = 0 \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

The same argument holds if the error occurs on the second qudit, thus the code can detect any single Pauli-Z(v) error that occurs on the first n - 1 qudits. Now suppose that a Pauli error E occurs on the last qudit. If $a \neq a', b \neq b'$, or $m \neq m'$ then the orthogonality of the first n - 1 qudits gives us

$$\langle \langle \phi_{a,b} | \otimes \langle \psi_m | \rangle E (| \phi_{a',b'} \rangle \otimes | \psi_{m'} \rangle) \rangle = 0$$

so again we only need to examine the case where the two codewords are the same.

If we have a Pauli-X(u) error on the last qudit we have

$$\begin{aligned} \langle \psi_m | X(u) | \psi_m \rangle &= \frac{1}{q} \left(\sum_{c \in \mathbb{Z}_q} \omega^{-m c |c|} \right) \left(\sum_{c \in \mathbb{Z}_q} \omega^{m c |c+u|} \right) \\ &= \frac{1}{q} \sum_{c \in \mathbb{Z}_q} \omega^{-m u} \\ &= \omega^{-m u} \end{aligned}$$

meaning that the error is degenerate. Note that since the value depends on the classical information, each inner code can detect the error but the outer code (as a quantum code) cannot. If a Pauli-Z(v) error occurs on the last qudit we have

$$\begin{aligned} \langle \psi_m | Z(v) | \psi_m \rangle &= \frac{1}{q} \left(\sum_{c \in \mathbb{Z}_q} \omega^{-m c |c|} \right) \left(\sum_{c \in \mathbb{Z}_q} \omega^{m c |c+v|} |c| \right) \\ &= \frac{1}{q} \sum_{c \in \mathbb{Z}_q} \omega^{v c} \\ &= \begin{cases} 1 & \text{if } v = 0 \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

We also mention in passing that this construction can be generalized further to codes over Frobenius rings by replacing the primitive root of unity by an irreducible additive character of the additive group of the ring [19].

3 CONCLUSION AND DISCUSSION

Hybrid codes simultaneously transmit both quantum and classical information across quantum channels, and can provide an advantage over using quantum codes for simultaneous transmission.

We have generalized a family of single error-detecting codes constructed in [20] from the binary case to the nonbinary case. While it is known that the construction gives genuine hybrid codes when $q = 2$, the existence of quantum codes with the similar parameters when $q \equiv 0, 1, 3 \pmod{4}$ means the construction does not produce genuine hybrid codes in all cases. One open question is whether or not the codes given by the construction are always genuine when $q \equiv 2 \pmod{4}$. As the code family here is the only construction of nonbinary hybrid codes, further investigation is needed.

REFERENCES

- [1] Alexei Ashikhmin and Emanuel Knill. 2001. Nonbinary Quantum Stabilizer Codes. *IEEE Trans. Inform. Theory* 47, 7 (2001), 3065–3072.
- [2] Cédric Bény, Achim Kempf, and David W. Kribs. 2007. Generalization of Quantum Error Correction via the Heisenberg Picture. *Phys. Rev. Lett.* 98, 10 (2007), 100502.
- [3] Cédric Bény, Achim Kempf, and David W. Kribs. 2007. Quantum error correction of observables. *Phys. Rev. A* 76, 4 (2007), 042303.
- [4] I. Devetak and P. W. Shor. 2005. The Capacity of a Quantum Channel for Simultaneous Transmission of Classical and Quantum Information. *Commun. Math. Phys.* 256, 2 (2005), 287–202.
- [5] Markus Grassl, Sirui Lu, and Bei Zeng. 2017. Codes for Simultaneous Transmission of Quantum and Classical Information. In *Proc. 2017 IEEE Int. Symp. Inform. Theory (ISIT)*. Aachen, Germany, 1718–1722.
- [6] Markus Grassl and Martin Rötteler. 2015. Quantum MDS Codes over Small Fields. In *Proc. 2015 IEEE Int. Symp. Inform. Theory (ISIT)*. Hong Kong, China, 1104–1108.



- [7] Min-Hsiu Hsieh and Mark M. Wilde. 2010. Entanglement-Assisted Communication of Classical and Quantum Information. *IEEE Trans. Inform. Theory* 56, 9 (2010), 4682–4704
- [8] Min-Hsiu Hsieh and Mark M. Wilde. 2010. Trading Classical Communication, Quantum Communication, and Entanglement in Quantum Shannon Theory. *IEEE Trans. Inform. Theory* 56, 9 (2010), 4705–4730.
- [9] Dan Hu, Weidong Tang, Meisheng Zhao, Qing Chen, Sixia Yu, and C. H. Oh. 2008. Graphical nonbinary quantum error-correcting codes. *Phys. Rev. A* 78, 1 (2008), 012306.
- [10] Avanti Ketkar, Andreas Klappenecker, Santosh Kumar, and Pradeep Kiran Sarvepalli. 2006. Nonbinary Stabilizer Codes Over Finite Fields. *IEEE Trans. Inform. Theory* 52, 11 (2006), 4892–4914.
- [11] Andreas Klappenecker and Martin Rötteler. 2002. Beyond Stabilizer Codes I: Nice Error Bases. *IEEE Trans. Inform. Theory* 48, 8 (2002), 2392–2395.
- [12] Andreas Klappenecker and Martin Rötteler. 2003. Unitary Error Bases: Constructions, Equivalence, and Applications. In *Applied Algebra, Algebraic Algorithms, and Error Correcting Codes - Proceedings 15th International Symposium, AAECC-15, Toulouse, France, Marc Fossorier, Tom Höholdt, and Alain Poli (Eds.)*. Springer-Verlag, 139–149.
- [13] E. Knill. 1996. Non-binary Unitary Error Bases and Quantum Codes. (Jun. 1996). Los Alamos National Laboratory Report LAUR-96-2717.
- [14] Emanuel Knill and Raymond Laflamme. 1997. Theory of quantum errorcorrecting codes. *Phys. Rev. A* 55, 2 (1997), 900–911.
- [15] Isaac Kremsky, Min-Hsiu Hsieh, and Todd A. Brun. 2008. Classical enhancement of quantum-error-correcting codes. *Phys. Rev. A* 78, 1 (2008), 012341.
- [16] Chi-Kwong Li, Seth Lyles, and Yiu-Tung Poon. 2019. Error correction schemes for fully correlated quantum channels protecting both quantum and classical information. (Jun. 2019). arXiv:1905.10228v2 [quant-ph].
- [17] Shiang Yong Looi, Li Yu, Vlad Gheorghiu, and Robert B. Griffiths. 2008. Quantum error-correcting codes using qudit graph states. *Phys. Rev. A* 78, 4 (2008), 042303.
- [18] Shayan Majidy. 2018. A unification of the coding theory and OQEC perspective on hybrid codes. (Jun. 2018). arXiv:1806.03702 [quant-ph].
- [19] Sushma Nadella and Andreas Klappenecker. 2012. Stabilizer Codes over Frobenius Rings. In *Proc. 2012 IEEE Int. Symp. Inform. Theory (ISIT)*. Cambridge, Massachusetts, 165–169.
- [20] Andrew Nemeec and Andreas Klappenecker. 2019. Infinite Families of Quantum-Classical Hybrid Codes. (Nov. 2019). arXiv:1911.12260 [quant-ph].
- [21] Eric M. Rains. 1999. Nonbinary Quantum Codes. *IEEE Trans. Inform. Theory* 45, 6 (1999), 1827–1832.
- [22] Eric M. Rains. 1999. Quantum Codes of Minimum Distance Two. *IEEE Trans. Inform. Theory* 45, 1 (1999), 266–271.
- [23] Eric M. Rains, R. H. Hardin, Peter W. Shor, and N. J. A. Sloane. 1997. Nonadditive Quantum Code. *Phys. Rev. Lett.* 79, 5 (1997), 953–954.
- [24] John A. Smolin, Graeme Smith, and Stephanie Wehner. 2007. Simple Family of Nonadditive Quantum Codes. *Phys. Rev. Lett.* 99, 13 (2007), 130505.
- [25] Jon Yard. 2005. Simultaneous classical-quantum capacities of quantum multiple access channels. Ph.D. Dissertation. Stanford University, Stanford, CA. arXiv