Robust Syndrome Extraction via BCH Encoding

Eren Guttentag[1,2], Andrew Nemec[1,2], and Kenneth R. Brown[1,2,3,4]
[1]Duke Quantum Center, Duke University, Durham, NC 27701, USA
[2]Department of Electrical and Computer Engineering, Duke University, Durham, NC 27708, USA
[3]Department of Physics, Duke University, Durham, NC 27708, USA
[4]Department of Chemistry, Duke University, Durham, NC 27708, USA

2024 IEEE International Symposium on Information Theory (ISIT) | 979-8-3503-8284-6/24/$31.00 ©2024 IEEE | DOI: 10.1109/ISIT57864.2024.10619479

***Abstract*—Quantum data-syndrome (QDS) codes are a class of quantum error-correcting codes that protect against errors both on the data qubits and on the syndrome itself via redundant measurement of stabilizer group elements. One way to define a QDS code is to choose a syndrome measurement code, a classical block code that encodes the syndrome of the underlying quantum code by defining additional stabilizer measurements.**

We propose the use of primitive narrow-sense BCH codes as syndrome measurement codes. We show that these codes asymptotically require $O(t \log \ell)$ extra measurements, where ℓ is the number of stabilizer generators of the quantum code and t is the number of syndrome measurement errors corrected by the BCH code.

Previously, the best known general method of constructing QDS codes out of quantum codes required $O(t^3 \log \ell)$ extra measurements. As the number of additional syndrome measurements is a reasonable metric for the amount of additional time a general QDS code requires, we conclude that our construction protects against the same number of syndrome errors with significantly less time overhead.

I. Introduction

The ability to accurately detect, identify, and correct errors is essential to building functional and scalable quantum computers. This is typically achieved through the use of quantum stabilizer codes, which are defined by their stabilizer group. The measurement of the group generators produces a binary syndrome that indicates the locations of errors. These measurements involve several multi-qubit gates, which can introduce errors on the qubits involved and corrupt the measurement outcome.

For syndrome fault tolerance, we can measure additional stabilizer group elements to add redundancy. One common way to do this is to repeatedly measure the same set of stabilizers [1], [2]. However, the syndrome can be protected much more efficiently with the use of quantum data-syndrome (QDS) codes. Introduced over a series of papers by Fujiwara [3], [4] and Ashikhmin, Lai, and Brun [5], [6], [7], QDS codes simultaneously encode quantum information and protect against syndrome errors.

We propose a way of constructing quantum data-syndrome codes using primitive narrow-sense BCH codes. We will also show that such a construction that protects against t syndrome errors requires $O(t \log(n-k))$ additional measurements, which is a significant improvement over other ways of constructing these codes. Recently, BCH codes have also been used to design good flag fault-tolerant syndrome extraction schemes [8].

In this paper we will look at a phenomenological error model, in which individual gates of a stabilizer have a chance of causing an error on the syndrome bit. This model does not consider hook errors propagated onto data qubits, but is intended to be a stepping-stone to exploring a full circuit model in the future.

II. Background

A. Stabilizer codes

Pauli operators on n qubits are n-fold tensor products of Pauli matrices $P_0 = I = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right], P_1 = X = \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right], P_2 = Y = \left[\begin{smallmatrix} 0 & -i \\ i & 0 \end{smallmatrix}\right], P_3 = Z = \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$, of the form

$$i^c \cdot P_{a_0} \otimes P_{a_1} \otimes \cdots \otimes P_{a_{n-1}},$$

with $a_i, c \in \{0, 1, 2, 3\}$. For simplicity's sake we will omit tensor products from our notation; so the three-qubit operator $X \otimes Y \otimes I$ becomes XYI. These operators form the group $\mathcal{P}^n$.

An $[\![n, k, d]\!]$ stabilizer code encoding k logical qubits into n physical qubits is defined by its $\ell := n - k$ independent *stabilizer* generators, $\{g_1, g_2, \ldots, g_\ell\} \subset \mathcal{P}^n$. These operators generate the stabilizer group $\mathcal{S} \subset \mathcal{P}^n$ of the code, which is commutative, does not contain $-I^{\otimes n}$, and has order 2^ℓ. Elements of the stabilizer group fix the states in the quantum code: for any stabilizer $g_i \in \mathcal{S}$ and any codeword $|\psi\rangle$ of the associated quantum code, $g_i |\psi\rangle = |\psi\rangle$.

A stabilizer on n qubits can be seen as a length-n vector with elements in GF(4), under the homomorphism $\tau : \mathcal{P} \to$ GF(4) that maps $I \to 0, X \to 1, Y \to \bar{\omega} = 1 + \omega, Z \to \omega$ and ignores any global phase of $\pm 1, \pm i$. This can be naturally extended to send operators on n qubits from $\mathcal{P}^n$ to GF$(4)^n$ [7]. Under this homomorphism, multiplication of stabilizers corresponds to bitwise addition in GF$(4)^n$. Throughout this paper we will use $g \in \mathcal{P}^n$ to refer to a stabilizer and $\mathbf{g} \in$ GF$(4)^n$ to refer to the corresponding length-n GF(4) vector $\tau(g)$.

The measurement of a code's ℓ stabilizer operators gives as an output a length-ℓ binary vector called the syndrome $\mathbf{s} = (s_1, s_2, \ldots, s_\ell)$. The i-th syndrome bit s_i, corresponding to stabilizer operator g_i, is 0 if E and g_i commute, and 1 if they anticommute. For vectors $\mathbf{x}, \mathbf{y} \in$ GF$(4)^n$ with elements $x_i, y_i \in$ GF(4), the analogous function is the *trace inner product* $\mathbf{x} \star \mathbf{y} :$ GF$(4)^n \times$ GF$(4)^n \to$ GF(2):

$$\mathbf{x} \star \mathbf{y} = \sum_{i=1}^{n} (x_i \bar{y}_i + \bar{x}_i y_i),$$

where $\bar{0}=0, \bar{1}=1, \bar{\omega}=1+\omega, \overline{1+\omega}=\omega$, and multiplication is typical in GF(4) [9]. Essentially, the i-th element of the sum is 0 if $x_i=0$, $y_i=0$, or $x_i=y_i$, and 1 otherwise. The trace inner product is 0 when the Pauli operators represented by $\mathbf{x}$ and $\mathbf{y}$ commute, and is 1 when they anticommute.

B. Quantum Data-Syndrome Codes

We assume that Shor-style syndrome extraction [1], [2] is used for measurement, in which a weight-w stabilizer can be measured fault-tolerantly using w single-qubit measurements. This is done using transversal gates and a w-qubit ancilla cat state to prevent a single error on an ancilla qubit from propagating to more than one data qubit.

In this paper, we focus on the phenomenological model where errors can either occur on the data qubits or on the syndrome bits. We only consider *measurement errors*—errors that result in a single syndrome bit-flip, equivalent to an error on the ancilla qubit after all transversal gates have already occurred, with no propagation to data qubits. Let p_m be the probability of a single-qubit measurement error. Then the probability of incorrectly measuring a stabilizer generator S_i of weight w_i is given by

$$p_{err}(S_i) = \sum_{j \text{ odd}} \binom{w_i}{j} p_m^j \left(1-p_m\right)^{w_i-j}. \tag{1}$$

If any bits of the syndrome are flipped during measurement, the resulting erroneous syndrome vector $\hat{\mathbf{s}} = \mathbf{s} + \hat{\mathbf{e}}$ may suggest an incorrect series of gates to restore the state. Some stabilizer codes have a choice of generators that allow them to correct either a single data error or a single syndrome error [4], [10], but in general, we need to perform additional stabilizer measurements to add redundancy against syndrome errors. Shor accomplished this by repeatedly measuring each stabilizer generator multiple times [11]. However, this can be achieved more efficiently by measuring an overdetermined set of stabilizer elements. We call a quantum code with r extra measurements beyond the $\ell = n-k$ needed an $[\![n,k,d:r]\!]$ quantum data-syndrome (QDS) code if it can correct up to a combined $\lfloor (d-1)/2 \rfloor$ data and syndrome errors, after [7].

A reasonable metric for the amount of extra time a QDS code takes is the number of extra syndrome measurements that take place. Assuming elements of the stabilizer group are of roughly equal weight, the measurement of each syndrome bit involves a similar number of gates to be performed, and thus takes a similar amount of time. This assumes that stabilizer measurements are done sequentially; the ability to measure in parallel could produce further improvement, but when considering the general case, we cannot assume that measurements can be performed in parallel [12]. Because of this, a QDS code that requires fewer additional stabilizer measurements to correct a certain number of syndrome errors is generally more efficient than one that requires more additional measurements. This is one reason that encoding syndrome information by simply repeating stabilizer measurements is inefficient—an m-fold repetition of ℓ stabilizer measurements that can correct up to $\lfloor \frac{m-1}{2} \rfloor$ syndrome errors requires $O(m\ell)$ additional measurements.

A general framework for designing a QDS code with a desired total distance $2t_c+1$ was proposed by Fujiwara [4]. It involves *s-detection parity check matrices* (s-DPMs), which are parity-check matrices for codes that can *detect* up to s errors [4]. Specifically, an s-DPM(m,w) is a binary $m \times w$ matrix such that any $m \times s$ submatrix contains a row of odd weight. In [4, Theorem 3.5], Fujiwara showed that a $2i$-DPM(m,w) exists so long as:

$$m \geq \left\lceil \log_2 \left(\binom{w}{2i} - \binom{w-2i}{2i} \right) + \log_2 e \right\rceil.$$

Fujiwara in [4] shows that for a $[\![n,k,2t+1]\!]$ stabilizer code, up to t total errors including up to t_c syndrome errors (for $t_c \leq t$) can be corrected if a $2i-$DPM$(m_i, n-k)$ exists for each $1 \leq i \leq t_c$. The resulting matrix of stabilizer group elements to be measured has $|S|$ rows where:

$$|S| = n-k+2t_c + \sum_{i=1}^{t_c} (2t_c - 2i + 1) m_i,$$

$$m_i = \left\lceil \log_2 \left(\binom{n-k}{2i} - \binom{n-k-2i}{2i} \right) + \log_2 e \right\rceil.$$

Theorem 1. *The construction in [4] requires $O(t_c^3 \log \ell)$ additional stabilizer measurements.*

Proof. As we have $\ell = n-k$, then we can express m_i in terms of ℓ as:

$$m_i = \left\lceil \log_2 \left(\binom{\ell}{2i} - \binom{\ell-2i}{2i} \right) + \log_2 e \right\rceil.$$

As we are interested in the behavior of this code asymptotically, we look at the behavior for larger ℓ. The binomial coefficient $\binom{n}{k}$ can in general be expressed as the polynomial:

$$\binom{n}{k} = \sum_{i=0}^{k} s(k,i) \frac{n^i}{k!}, \tag{2}$$

where $s(k,i) = (-1)^{k-i} \left[{k \atop i} \right]$ are the Stirling numbers of the first kind [13]. There are several special values of Stirling numbers of the first kind; most valuable to us are $s(n,n) = \left[{n \atop n} \right] = 1$ and $s(n,n-1) = -\left[{n \atop n-1} \right] = -\binom{n}{2} = -\frac{n(n-1)}{2}$.

Now consider the terms in these expansions with order greater than $2i-2$:

$$\binom{\ell}{2i} = \left[{2i \atop 2i} \right] \frac{\ell^{2i}}{(2i)!} - \left[{2i \atop 2i-1} \right] \frac{\ell^{2i-1}}{(2i)^!} + O(\ell^{2i-2}),$$

$$\binom{\ell-2i}{2i} = \left[{2i \atop 2i} \right] \frac{(\ell-2i)^{2i}}{(2i)!} - \left[{2i \atop 2i-1} \right] \frac{(\ell-2i)^{2i-1}}{(2i)!} + O(\ell^{2i-2}).$$

Expanding the $(\ell-2i)^{2i}$ and $(\ell-2i)^{2i-1}$ terms, we see:

$$(\ell-2i)^{2i} = \ell^{2i} - (2i)^2 \ell^{2i-1} + O(\ell^{2i-2}),$$

$$(\ell-2i)^{2i-1} = \ell^{2i-1} + O(\ell^{2i-2}),$$

so in fact the ℓ^{2i} and ℓ^{2i-1} terms of the polynomials are (evaluating the Stirling numbers of the first kind):

$$\binom{\ell}{2i} = \frac{\ell^{2i}}{(2i)!} - \frac{2i(2i-1)}{2}\frac{\ell^{2i-1}}{(2i)^!} + O(\ell^{2i-2}),$$

$$\binom{\ell-2i}{2i} = \frac{\ell^{2i}}{(2i)!} - \frac{(2i)^2\ell^{2i-1}}{(2i)!} - \frac{2i(2i-1)}{2}\frac{\ell^{2i-1}}{(2i)!} + O(\ell^{2i-2}).$$

Then the difference between these two binomial coefficients will have a highest-order term in ℓ of the form ℓ^{2n-1}:

$$\binom{\ell}{2i} - \binom{\ell-2i}{2i} = \frac{2i\ell^{2i-1}}{(2i-1)!} + O(\ell^{2i-2}).$$

We know the m_i is at least $(2i-1)\log_2 \ell$:

$$m_i = \left\lceil \log_2 \left(\binom{\ell}{2i} - \binom{\ell-2i}{2i} \right) + \log_2 e \right\rceil$$

$$\Downarrow$$

$$m_i > \log_2 \left(\frac{2i\ell^{2i-1}}{(2i-1)!} \right) = (2i-1)\log_2 \ell + O(1).$$

So the number of redundant stabilizer measurements required by this construction is at least

$$2t_c + \sum_{i=1}^{t_c} (2t_c - 2i + 1)(2i-1)\log_2 \ell.$$

This sum can actually be evaluated to a closed form; $\sum_{i=1}^{t_c}(2i-1)(2t_c-2i+1)\log_2 \ell = \log_2 \ell(\frac{2t^3+t}{3})$. So in terms of t and ℓ, the total number of additional stabilizers constructed is

$$|S| - (n-k) = 2t_c + \frac{\log_2 \ell}{3}\left(2t_c^3 + t_c\right).$$

The dominant term of this is $\frac{2t_c^3 \log_2 \ell}{3}$, and

$$\frac{2t_c^3 \log_2 \ell}{3} \in O(t_c^3 \log \ell).$$

□

III. Syndrome Measurement Codes

In general, given a stabilizer code, it is nontrivial to choose a set of stabilizer generators such that the resulting QDS code has a good total minimum distance. Instead we make use of *syndrome measurement (SM) codes* [5]. A syndrome measurement code is a $[n_S, \ell, 2t_S+1]$ classical block code that defines an overdetermined set of n_S stabilizer operators to be measured. This allows for a two-step decoding protocol that is simpler than simultaneously decoding syndrome and data errors, but can perform suboptimally in comparison [7]. In the classical decoding step, the measured length-n_C bit string is decoded with a decoder of the SM code. This results in a length-ℓ syndrome for the stabilizer code, which is then used to correct quantum errors in the second step. One advantage of using a SM code is that the number of correctable syndrome bit-flip errors is easy to dictate and independent from the minimum distance of the stabilizer code.

If we have a stabilizer code $[\![n, k, d]\!]$ whose syndrome is encoded in a $[n_C, \ell, d_C]$ classical code, then the overall minimum distance of the QDS code is $d' \geq \min(d, d_C)$, and it can correct up to a simultaneous $\lfloor \frac{d-1}{2} \rfloor$ errors on the data qubits and $\lfloor \frac{d_C-1}{2} \rfloor$ errors on the syndrome bits. This ability to control the distance of the SM code makes the codes particularly useful for systems with relatively high probability of measurement error.

IV. Protecting Syndromes with BCH Codes

We propose the use of primitive narrow-sense Bose-Chaudhuri-Hocquenghem (BCH) codes as SM codes to encode the syndrome bits. These codes are a class of cyclic binary codes of the form $[2^m - 1, 2^m - R(m,t) - 1, 2t+1]$, where $R(m,t) \leq mt$ for a chosen $m, t \in \mathbb{N}$. The properties of a BCH code are defined by the degree of the least common multiple of certain irreducible polynomials [14], [15], [16]. Any BCH code can be shortened to create a $[2^m - 1 - a, 2^m - R(m,t) - 1 - a, 2t+1]$ code. Note that because both the number of logical and data bits both decrease by a, this process does not change the difference between the number of logical and data bits. This means that whether we use a regular or shortened BCH code as an SM code, the number of additional stabilizers measured will still be $R(m,t)$.

In order to encode a syndrome of an $[\![n, k, d]\!]$ quantum code (with a $\ell \times 2n$ stabilizer matrix H) in a BCH code with distance $d_S = 2t_S + 1$, we choose m to be the smallest integer such that $\ell \leq 2^m - mt_S - 1$. Note that this means $2^{m-2} < \ell < 2^m < 4\ell$, and so $\log_2 \ell$ is $O(m)$ and m is $O(\log \ell)$.

We use this m and our desired t_S to find the corresponding $[2^m - 1, 2^m - R(m,t_S) - 1, 2t_S + 1]$ BCH code, and if $2^m - R(m,t_S) - 1 > \ell$ we shorten it by an appropriate amount so that it is a $[\ell + R(m,t_S), \ell, 2t_S + 1]$ code. This code has a $\ell \times (\ell + R(m,t_S))$ generator matrix G_B. We can use this matrix to generate the $(\ell + R(m,t_S)) \times 2n$ stabilizer matrix for our $[\![n, k, d : R(m,t_S)]\!]$ QDS code, $H_Q := G_B^T H$.

Theorem 2. *Using a BCH code or shortened BCH code that can correct up to t errors as a SM code encoding ℓ syndrome bits requires $O(t \log \ell)$ additional stabilizer measurements.*

Proof. When we encode ℓ bits in a BCH code with distance $2t+1$, we find the m used to construct the code as the smallest m such that $2^m - 1 - mt > \ell$, and we can see m is in $O(\log \ell)$. The number of additional stabilizer measurements required when using a BCH code as a syndrome measurement code is the difference between the number of encoded and data bits in the BCH code. This is definitionally $R(m,t) \leq mt$, so $R(m,t) \in O(mt) \implies R(m,t) \in O(t \log \ell)$. This $R(m,t)$ is the same for a BCH code and any resulting shortened BCH code, so our methodology requires $O(t \log \ell)$ additional stabilizer measurements. □

The significance of this improvement can be seen by considering the rotated surface code. A $[\![d^2, 1, d]\!]$ rotated surface code is defined by $\ell = d^2 - 1$ stabilizers; this means that $\ell \in O(t^2)$ for $t = \lfloor \frac{d-1}{2} \rfloor$. A standard way to protect against t syndrome errors, proposed by Shor, requires at least $2t$ and up to t^2 additional rounds of syndrome extraction [1].

A minimum-weight perfect-matching (MWPM) space-time decoder is the standard method for fault tolerant syndrome extraction for the surface code [17], [18]. The method uses $d = 2t+1 \in O(t)$ rounds of syndrome measurements, yielding $O(\ell t)$ total measurements. In terms of t, this means that the most efficient t-fault-tolerant syndrome extraction for the surface code requires $O(t^3)$ additional measurements. Fujiwara's methodology requires $O(t^3 \log \ell)$ additional measurements, which is $O(t^3 \log t)$ in terms of t. In contrast, using our methodology, we require $O(t \log \ell)$ additional measurements; in terms of t this means our method is $O(t \log t)$ for the surface code, significantly better than the alternatives in terms of measurements, but at the cost of a complex syndrome extraction circuit relative to MWPM.

A. Example: encoding the $[\![7,1,3]\!]$ Steane code in a BCH code

The Steane code is a CSS code that encodes X and Z errors using the $[7,4,3]$ Hamming code. This Hamming code has parity check matrix:

$$H_H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

So the generators of the Steane code's stabilizer group $\mathcal{S}$ and corresponding binary parity-check matrix H_S are:

$$\mathcal{S} = \langle XIXIXIX, IXXIIXX, IIIXXXX, \\ ZIZIZIZ, IZZIIZZ, IIIZZZZ \rangle,$$

$$H_S = \begin{bmatrix} 0 & H_H \\ H_H & 0 \end{bmatrix}.$$

This code gives us a syndrome of length 6. Say we want to protect against $t_S = 3$ possible syndrome errors. Then we determine our relevant BCH code. The smallest m such that $6 < 2^{m-1} - 3m - 1$ is $m = 5$, so our BCH code is a $[31, 16, 7]$ code. We need to shorten it by $a = 10$ bits in order for it to encode exactly 6 bits; the resulting code is a $[21, 6, 7]$ code with generator matrix G_B:

$$G_B = \begin{bmatrix} 1&0&0&0&0&0&0&0&0&1&0&1&0&1&1&0&1&0&0&1&0 \\ 0&1&0&0&0&0&0&0&0&0&1&0&1&0&1&1&0&1&0&0&1 \\ 0&0&1&0&0&0&1&1&1&1&0&0&0&0&1&0&0&1&1&0&0 \\ 0&0&0&1&0&0&0&1&1&1&1&0&0&0&0&1&0&0&1&1&0 \\ 0&0&0&0&1&0&0&0&1&1&1&1&0&0&0&0&1&0&0&1&1 \\ 0&0&0&0&0&1&1&1&1&0&1&0&1&1&1&1&1&0&0&0&1 \end{bmatrix}.$$

Multiplying G_B^T by our matrix H_S gives us a 21×14 matrix that defines a set of stabilizers whose measurement returns a length-21 syndrome vector. This can be decoded by appending $a = 10$ zeroes to the beginning of the vector and passing it through the decoder for the original $[31, 16, 7]$ code (for more on the decoding of cyclic codes see [15]). The resulting length-16 vector will begin with 10 zeros that can be removed, and we are left with a 6-bit syndrome—which can be used to identify and correct errors on our 7 data qubits in the usual way.

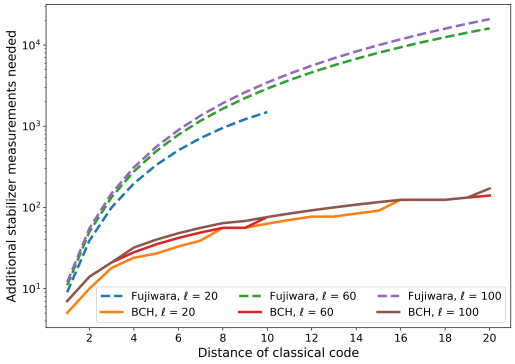

Fig. 1. Comparison between the number of additional measurements required by our BCH encoding vs. the additional measurements required by Fujiwara's construction for several values of $\ell = n-k$. Note that the latter's construction is also limited by the number of stabilizer generators in the quantum code.

B. Time overhead

A QDS code that uses a BCH code as an SM code will need only $O(mt_S)$ additional measurements to be performed. Note that $m \in O(\log \ell)$, so the number of additional measurements is $O(t_S \log \ell)$. Compared to Fujiwara's construction, which is $O(t_c^3 \log \ell)$, we can see that ours gives a significant improvement. Note that Fujiwara's construction restricts t_c to be at most the t of the quantum code the QDS code is based on. If we desire to protect against a number of syndrome errors fewer than those corrected by the base code, our construction outperforms. If we instead protect against more syndrome errors than t, our construction allows for this while Fujiwara's does not. Specifically, if we have a quantum code and want to protect against fewer than t syndrome errors, Fujiwara's construction grows with the number of errors cubed. For the same code and desired correctable syndrome errors, our BCH construction requires a number of additional stabilizer measurements that is linear in t. For a comparison of the additional stabilizer measurements needed to obtain the same error-correcting properties between our and Fujiwara's constructions see Fig. 1.

This means that protecting against a specific number of syndrome errors can be done with significantly less time overhead using our encoding procedure than using Fujiwara's construction. It also means that if a circuit has a limited amount of time to perform stabilizer measurements, our construction can correct significantly more errors on the syndrome bits than Fujiwara's construction.

As an example of this, consider a code with $\ell = 10$. If we want to protect against up to 3 syndrome errors, Fujiwara's construction requires up to 76 additional stabilizers. The highest-distance BCH code encoding $\ell = 10$ bits such that $R(m,t) \leq 76$ is the $[80, 10, 23]$ shortened BCH code (shortened from a $[127, 57, 23]$ code) that only needs 70 additional measurements while protecting against up to 12 syndrome errors. Our methodology allows for significantly more well-protected syndrome measurement in the same amount of time.

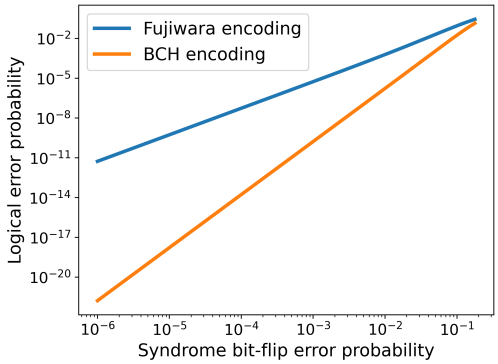

Fig. 2. Behavior of BCH and Fujiwara encoding on a code with $\ell = 10$, $t_c = 3$, $t_{BCH} = 12$, and the same number of additional stabilizer measurements. This shows the probability of a logical error arising from incorrect stabilizer decoding. Errors in the results due to sample error from the Monte Carlo simulations are negligible.

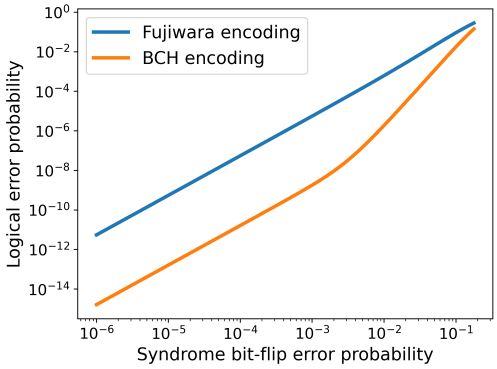

Fig. 3. Behavior of BCH and Fujiwara encoding on the Steane code when qubit error probability is 100x less that syndrome bit-flip error probability. This shows that at very high error probabilities, both codes perform relatively similarly; however the BCH code performs significantly better at lower error probabilities.

V. Comparisons

To illustrate this, we perform Monte Carlo simulation over many error weights. To obtain accurate results despite the need for high-weight errors with low probability, we use the importance sampling methodology outlined in [19]. For a system with probability of syndrome error p_s on a number of syndrome bits ℓ, and probability of qubit error p_q on number of qubits q, we can calculate the probability of a logical error:

$$p_{err}(p_q, p_s) = \sum_{w_s=1}^{\ell} \sum_{w_q=1}^{q} A_{w_q,w_s}(p_q, p_s) p_L(w_q, w_s),$$

where $A_w(p, n) = \binom{n}{w}(p)^w(1-p)^{n-w}$ is the probability that w errors will occur on n possible locations when an error occurs with probability p (and errors occur independently), and $A_{w_q,w_s}(p_q, p_s) = A_{w_q}(p_q, q) \cdot A_{w_s}(p_s, \ell)$ is the probability that exactly w_q qubit errors and w_s syndrome errors will occur. Then $p_L(w_q, w_s)$ is the Monte Carlo-determined probability of an error resulting from the decoding process when w_q qubit errors and w_s syndrome errors occur.

Our construction performs significantly better than Fujiwara's under a wide range of possible measurement error probabilities. As an example, consider this encoding of an $\ell = 10$ code (Fig. 2). The probability of a set of bit flips resulting in a logical error is significantly lower with the BCH SM code at all bit-flip error probabilities, with a very pronounced effect at lower probabilities due to the significantly higher distance in the BCH construction.

In a realistic model, it is likely that qubit errors and syndrome bit-flip error probabilities are similar to each other. It can be helpful then to look at the behavior of these codes while varying both errors. In Fig. 3 we look at an encoding of the Steane code in a BCH code and in Fujiwara's construction for syndrome bit-flip probability 100x greater than the Pauli error probability. We can see that the codes both reach the same slope, because the probability of qubit error becomes more significant than the probability of measurement error. However, because the BCH code has a higher distance, it behaves significantly better.

VI. Conclusion

We show that using the family of classical BCH codes, we can protect against any number of syndrome errors t we choose, while only requiring a number of additional stabilizer measurements linear in t. This is a significant improvement on the previous construction given in [4], which requires a number of additional measurements cubic in t. Our use of BCH codes confers two advantages. First, for a specific desired number of syndrome errors to correct, our construction requires significantly fewer syndrome measurements and therefore takes significantly less time than that in [4]. Second, if we have a certain amount of time allocated for syndrome measurement, our construction allows for significantly more syndrome errors to be corrected with the same overhead as Fujiwara's method.

Although BCH codes are generally good codes, this methodology may not the optimal choice for specific quantum codes. For highly structured families of quantum codes, using BCH codes as SM codes may not preserve the structure of the underlying quantum code. For example, a good classical code may not be a good SM code for a QLDPC code if it measures high-weight stabilizer elements. For surface codes, using a BCH code as a SM code likely will not preserve the locality of stabilizer elements. For a CSS code it may be desirable to avoid having to measure the product of both X- and Z-type stabilizers, and therefore to encode the X- and Z-type subgroups separately with SM codes. Future work may therefore include encoding subsets of the stabilizer generators in separate syndrome measurement codes to preserve certain properties of the base quantum code.

Acknowledgements

This work was supported by the ARO/LPS QCISS program (W911NF-21-1-0005) and the NSF QLCI for Robust Quantum Simulation (OMA-2120757). Support is also acknowledged from the U.S. Department of Energy, Office of Science, National Quantum Information Science Research Centers, Quantum Systems Accelerator.

REFERENCES

[1] P. W. Shor, "Fault-tolerant quantum computation," in *Proceedings of the 37th IEEE Symposium on Foundations of Computer Science (FOCS)*, Burlington, Vermont, USA, Oct. 1996, pp. 56–67.

[2] D. P. DiVincenzo and P. W. Shor, "Fault-Tolerant Error Correction with Efficient Quantum Codes," *Physical Review Letters*, vol. 77, no. 15, pp. 3260–3263, 1996.

[3] Y. Fujiwara, "Ability of stabilizer quantum error correction to protect itself from its own imperfection," *Phys. Rev. A*, vol. 90, p. 062304, Dec 2014. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.90.062304

[4] ——, "Global Stabilizer Quantum Error Correction with Combinatorial Arrays," in *Proceedings of the 2015 IEEE International Symposium on Information Theory (ISIT)*, Hong Kong, China, Jun. 2015, pp. 1114–1118.

[5] A. Ashikhmin, C.-Y. Lai, and T. A. Brun, "Robust Quantum Error Syndrome Extraction by Classical Coding," in *Proceedings of the 2014 IEEE International Symposium on Information Theory (ISIT)*, Honolulu, Hawaii, USA, Jun. 2014, pp. 546–550.

[6] ——, "Correction of Data and Syndrome Errors by Stabilizer Codes," in *Proceedings of the 2016 IEEE International Symposium on Information Theory (ISIT)*, Barcelona, Spain, Jul. 2016, pp. 2274–2278.

[7] ——, "Quantum Data Syndrome Codes," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 3, pp. 449–462, 2020.

[8] B. Anker and M. Marvian, "Flag Gadgets based on Classical Codes," 2022, arXiv:2212.10738 [quant-ph].

[9] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over gf(4)," 1997.

[10] A. Nemec, "Quantum Data-Syndrome Codes: Subsystem and Impure Code Constructions," 2023, arXiv:2302.01527 [quant-ph].

[11] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A*, vol. 52, pp. R2493–R2496, Oct 1995.

[12] N. Delfosse, B. W. Reichardt, and K. M. Svore, "Beyond single-shot fault-tolerant quantum error correction," *IEEE Transactions on Information Theory*, vol. 68, no. 1, pp. 287–301, jan 2022.

[13] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions with formulas, graphs, and mathematical tables*. U.S. Dept. of Commerce, National Bureau of Standards, 1972.

[14] R. C. Bose and D. K. Ray-Chaudhuri, "Further Results on Error Correcting Binary Group Codes," *Information and Control*, vol. 3, no. 3, pp. 279–290, 1960.

[15] ——, "On A Class of Error Correcting Binary Group Codes," *Information and Control*, vol. 3, no. 1, pp. 68–79, 1960.

[16] A. Hocquenghem, "Codes correcteurs d'erreurs," *Chiffres*, vol. 2, pp. 147–156, 1959.

[17] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, "Topological quantum memory," *Journal of Mathematical Physics*, vol. 43, no. 9, pp. 4452–4505, 08 2002. [Online]. Available: https://doi.org/10.1063/1.1499754

[18] A. G. Fowler, "Proof of finite surface code threshold for matching," *Phys. Rev. Lett.*, vol. 109, p. 180502, Nov 2012. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.109.180502

[19] M. Gutiérrez, M. Müller, and A. Bermúdez, "Transversality and lattice surgery: Exploring realistic routes toward coupled logical qubits with trapped-ion quantum processors," *Physical Review A*, vol. 99, no. 2, feb 2019. [Online]. Available: https://doi.org/10.1103%2Fphysreva.99.022330