UNIVERSITY OF CALIFORNIA
RIVERSIDE

Fault-Tolerant Quantum Computation Through Quantum Low-Density Parity-Check Codes

A Dissertation submitted in partial satisfaction
of the requirements for the degree of

Doctor of Philosophy

in

Physics

by

Weilei Zeng

March 2021

Dissertation Committee:

Dr. Leonid P. Pryadko, Chairperson
Dr. Michael Mulligan
Dr. Boerge Hemmerling

The Dissertation of Weilei Zeng is approved:

Committee Chairperson

University of California, Riverside

Acknowledgments

The five and half years in Riverside has been a wonderful journey. A boy grew up in a small village in Hunan, China, studied hard and made the way to attend a top university in Shanghai, and happened to get a Ph.D. offer from UC Riverside, without knowing much about what he would encounter. Five years later, he became experienced, passionate, beloved, and confident. He is ready to continue his career in the field of quantum computing, and willing to help others with the best he can. He is grateful for all the people that have been part of his life.

My advisor Leonid has been a role model, who devotes himself into research and also show great commitment for his family. He supervised several research projects for me, provided guidance over calculations, coding, writing papers, and presentations. Without him, I wouldn't have reached this far. Leonid is famous to graduate students in the department as a person who seems to know everything. He demonstrated it in his intense teaching style, who is ready to derive anything from the beginning if needed. He has a Russian-origin physics exercise book, which contains all the secrets to beat any comprehensive exam. He doesn't go to the department colloquium much, but if he went, he seldom left without asking questions. He could sit in his office and work for five hours straight, without even going to the bathroom! Every time I talk with him, he would use one hour to present materials that would take me one month to follow up. I have to admit that I sometimes get lost after 10 mins, but I appreciate that he always give comprehensive answers to my questions, which usually turn out to be nice and useful. He writes very nice papers. While doing that, his strong logics, flexible uses of language, broad knowledge in the field of quantum

computation and condensed matter physics, and time management skills becomes rewarded and explains why he keeps working hard all the time.

A PhD student is ready to become a doctor when he/she knows some topic better than his advisor. With Leonid being so knowledgable, that makes my job harder. Leonid and I visited China together twice and enjoyed the food there. The seafood in the reception of QAS 2019 was quite impressive. Among many others, the corn pork soup, was fresh and sweet. Leonid asked, "How do you do with the corn?"I sticked one chopstick into the corn. This surprised him, "Oh, like a BBQ. Thanks! Otherwise, I have to leave it there." This became my most confident moment that I am sure I taught my advisor something.

The friendship from other members in Leonid's group is very precious for me. Nicolas, Yi, Michael, TJ, Xingrui, Renyu, and Cristian have helped me through fruitful discussions. I reply on their feedbacks to ensure I am in the right path.

The faculty members at UCR have taught me a lot through lectures and discussions. Among them are Prof. Vivek Aji, Prof. Kirill Shtengal, Prof. Michael Mulligen, Prof. Chandra Varma. Derek was always passionate and helpful, as the program coordinator. I am also thanksful for Prof Alexei Ashikhmin, who advised my summer intern at Nokia Bell Labs in summer 2018. Prof Bei Zeng and Prof Markus Grassul are very encouraging during our meetings.

Other than research, I spent most of my time in the Church. Those, in turn , helps me to become a better person. The journey of becoming a Christian has changed my life. People in the EFC church are like a home with so many families. They have been so warm and patient and accompanied most of my life here. Jean, Wensong, Patrick, Yongliu,

Rita, Allison, Robert, Frank, Ada, Xiuxiu, Shuwei, Fang, Ruth, have a relationship with me that is overwhelmed by care, love, and confidence. The student fellowship were occupied by happiness and energy, Charlene, Emily, Flora, Shixian, Bowen, Roger, Chris, to name a few. I also want to thank Sophie and King. While I lived in their house for two years, King cooked a lot of delicous food and Sophie introduced me to the EFC church.

The friends from the Bridge church give me the precious opportunity to encounter the life of American Christians. Among them are the Woolls, the Ries, Richard and Cathrine, Jessika, Amond, Susie, Hanah, Jonason and Kim. I heard a lot of truthful words in Ries' group and learned how to pray there.

My family have given me incredible support. It takes a lot of philosophy to accept the reality that I have moved from the poor prelimilary school in a remote village in China to the grad school in UCR that is 10,000 miles away. For my parents, who barely complete their prelimilary education, it must take a lot of determination and wisdom to encourage and support me to take my journey and even proceed further. My three elder sisters made my life story romantic and sweet since I was born. My nephew and nieces are cute and they inspire me by pursuing their own dreams.

My high school sweetheart now sits by my side, as Mrs. Zeng. Yaping has made my life much more meaningful since I met her at the age of 15. I am grateful that we grew together, always love and support each other, and provide the most difficult and honest advices to each other. We have a future to build, a life we want to make, and those keep us young and passionate. I proposed to her in the Bridge church in Jan 2018, which may be the best moment in my life. It brings all parts of my life in Riverside together. Almost everyone

played a part. People from EFC church and Bridge church, both our family members, my other friends and classmates in Riverside, they all come to offer their help and celebrate. I am so grateful that I am surrounded by them.

Among the numerous events I attended or organized in my Ph.D., the one made me the proudest is the Shizitang Reading Club. It is a mixtrue of Toastmaster public speaking club, bible study group and family meetings. Its weekly attendees are mostly family members from my side or Yaping's side. They are farmers, businessman, housewives, start-up owner, programmers, students. They are less educated or have studied abroad. It is a group of people, who want to change their life by educating themselves and helping others. It brings hope, creativity, and confidence, and inspries everyone to make a difference.

It is true that one sometimes suffers from the dark side of life. When I look back for the past five years, life only becomes brighter and brighter.

To my families for all the support.

ABSTRACT OF THE DISSERTATION

Fault-Tolerant Quantum Computation Through Quantum Low-Density Parity-Check Codes

by

Weilei Zeng

Doctor of Philosophy, Graduate Program in Physics
University of California, Riverside, March 2021
Dr. Leonid P. Pryadko, Chairperson

Quantum computation has shown advantages in several problems over the corresponding classical algorithms. The noisy intermediate-size quantum devices with dozens of qubits make it more promising in the past decade, as the quantum advantage was demonstrated experimentally. Before entering the era of scalable quantum computation, one has to resolve the errors in a quantum many-body system, which is inevitable due to the environment interaction during quantum control processes. The goal of quantum error correction is to reduce such errors and increase decoherence time.

The most successful candidates of quantum error correction codes are topological codes, especially surface codes, which were discovered by Alexei Kitaev. The ordered phase of the 2D Ising model on a torus ensures that toric codes are fault-tolerant below a critical error probability. Other than the FT threshold, the topological codes feature efficient encoding and decoding, local measurements, but suffer from asymptotically zero code rate.

To encode more logical qubits with finite resources, one can loosen the condition on locality and extend to a broader class of quantum low-density parity-check (LDPC)codes.

There are many known algebraic constructions for such codes, but only a precious few of them have finite code rates and meet the fault-tolerant condition: the stabilizer weight is bounded and the distance scales at least logarithmically with the code size. In this thesis, I construct the higher-dimensional quantum hypergraph product (HQHP) codes, which generalize quantum hypergraph product (QHP) codes and toric codes in all dimensions. The HQHP codes projected into a single space gives subsystem product codes, which can then be gauge fixed to concatenated codes or homological product codes. Those include some common CSS codes, like Shors codes, Bacon Shors codes, and subsystem QHP codes. The HQHP codes can be mapped to the tensor product of chain complexes, which provides an algebraic framework to construct quantum LDPC codes with finite code rates, square root distances, FT thresholds and single-shot properties with redundant checks. Meanwhile, their rich connection to other codes are very instructive and may lead to further optimizations. Regarding the remained procedures towards fault-tolerant universal quantum computation through quantum LDPC codes, I will discuss the fault-tolerant condition for each code, including distance, stabilizer weight, decoding, fault-tolerant gates and measurement protocols.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Quantum computation and quantum error correction

In the 1980s, the idea of quantum computation was proposed by Feynman and Manin[1, 2]. Various algorithms have confirmed its advantage over classical computers, including Shor's factoring algorithm[3] and Grover's search algorithm[4]. Though still far away from matching DiVincenzo's criteria[5] for quantum computers, Noisy Intermediate Scale Quantum (NISQ) devices[6] have been available with dozens of faulty qubits over the past decade, which may already be useful for quantum simulators of many-body physics [2, 7], variational quantum eigensolvers for quantum chemistry and electronic structure [8], quantum optimizers[9], and quantum machine learning[10]. To move forward towards scalable quantum computation, one needs to reduce error and extend decoherence time of qubits. The main technique is quantum error correction (QEC).

QEC encodes the logical information into a subspace of the Hilbert space of physical qudits/qubits. A quantum error correction code (QECC) needs to be robust against

faulty quantum memory, fault quantum gates, faulty quantum preparation, and faulty measurements. To achieve that goal, a QECC needs to have efficient encoding and decoding, large code distance, finite resource overhead or code rate, redundant checks, and essentially fault-tolerant threshold. Dozens of constructions have been designed to improve different aspects among those features, but none of them have satisfied all the conditions.

1.2 Quantum LDPC codes

Topological QECCs, generalizations of the toric code[11, 12, 13, 14, 15, 16, 17] invented by Kitaev[18], are presently at the crux of research in QEC. Such a code can be constructed from any tessellation of an arbitrary surface or a higher-dimensional manifold. The essential advantage of topological codes is locality: stabilizer generators, operators to be measured frequently, involve only qubits in the immediate vicinity of each other; this is what makes planar surface codes so attractive and practical. However, locality also limits the parameters of topological codes[19, 20, 21, 22]. In particular, for a code of length n with generators local in two dimensions, the number of encoded qubits k and the minimal distance d satisfy the inequality[19] $kd^2 \leq \mathcal{O}(n)$. This implies asymptotically zero rate, $R = k/n \to 0$, whenever d diverges with n.

More general quantum low-density parity-check (LDPC) codes have stabilizer generators of bounded weight but no locality constraint. This is the only class of codes known so far to combine finite rates with non-zero fault-tolerant (FT) thresholds[23, 24], to allow scalable quantum computation with a finite multiplicative overhead[25]. However, unlike in the classical case, where capacity-approaching codes can be constructed from random

sparse matrices[26, 27, 28, 29], matrices suitable for constructing quantum LDPC codes are highly atypical in the corresponding ensembles. Thus, an algebraic ansatz is required to construct large-distance quantum LDPC codes. Precious few examples of algebraic constructions are known that give finite rate codes and also satisfy sufficient conditions[24] for fault-tolerance: bounded weight of stabilizer generators and minimum distance that scales logarithmically or faster with the block length n. Such constructions include hyperbolic codes on two- and higher-dimensional manifolds[30, 31, 32, 33, 34], and quantum hypergraph-product (QHP) & related codes[35, 36, 37, 38]. Further, some constructions, e.g., in Refs. [39, 40, 41, 42, 43], have finite rates and relatively high distances, with the stabilizer generator weights that grow with n logarithmically. It is not known whether these codes have non-zero FT thresholds. However, such codes can be modified into those with provable FT thresholds with the help of weight reduction[44, 45].

1.3 HQHP codes

Central idealization in topology is the focus on continuity while sizes are ignored. Topologically speaking, an opening through a straw is no different than a pinhole in a piece of paper, or a missing pixel in an image. Yet a missing pixel could be just an artifact of the noisy data. No wonder that in practical applications the sizes and distances *are* important, and are incorporated into computational algorithms in a variety of ways[46, 47, 48, 42, 49].

Quantum stabilizer and, more generally, subsystem codes offer an excellent example of a problem where such a distance is extremely relevant[14, 50, 42]. Namely, a qubit quantum stabilizer code is isomorphic to a chain complex $\mathcal{C}$ with three finite-dimensional

binary spaces, where logical operators correspond to elements of the first homology group $H_1(\mathcal{C})$. In the case of a Calderbank-Shor-Steane[51, 52] (CSS) code, the rank of this group gives the number k of encoded qubits, the code length n is the dimension of the corresponding space $\mathcal{C}_1$, while the distance d of the quantum error correcting code (QECC), the minimum weight of a non-trivial element in $H_1(\mathcal{C})$ (or the corresponding co-homology group), has to be sufficiently large for the code to offer protection against environmental errors.

The original QHP ansatz[35] by Tillich and Zémor can be seen as a tensor product of two chain complexes $\mathcal{A}$ and $\mathcal{B}$, each involving just two finite-dimensional binary spaces with chosen bases, so that the corresponding boundary operators are just binary matrices without any additional constraints. The resulting chain complex has three spaces; elements of the first homology group of dimension $k = \operatorname{rank} H_1(\mathcal{A}\times\mathcal{B})$ form half of the quantum code $\mathcal{Q}_1(\mathcal{A}\times\mathcal{B})$ encoding k qubits (the other half comes from the corresponding co-homology group). This dimension can be immediately recovered from the Künneth formula[53, 54]. The main result by Tillich and Zémor is the expression for the minimal distance. This was generalized to homology groups in a tensor product of a general chain complex over binary spaces with that involving just two spaces[38].

In Ref. [55], the distance result was again generalized to a tensor product of two chain complexes of vector spaces over any finite field F, with one of the complexes still required to be a linear map between a pair of spaces. While the original proof[38] would still work with a general field, Ref. [55] gives a simpler proof for the lower bound on the minimum distance, formulated in terms of a *projected* product complex with the level-j

subspace projected onto just one subspace $\mathcal{A}_i \otimes \mathcal{B}_{j-i} \subset (\mathcal{A} \times \mathcal{B})_j$. As a result of the projection, the quantum code $\mathcal{Q}_j(\mathcal{A} \times \mathcal{B})$ associated with the j-th homology group of the product complex is replaced by an F-linear quantum subsystem code; its distance gives a lower bound on the distance associated with the homology group $H_j(\mathcal{A} \times \mathcal{B})$ of the original product complex. When one of the complexes has length two, the minimum distance of the subsystem code can be computed and, as in the binary case, the result saturates the upper bound.

While the construction also works for a product of chain complexes of arbitrary length, we failed to find a tight lower bound on the distance of the corresponding projected codes. Further, we have found a class of examples, a generalization of the homological product of Steane code with itself[40, 42], where the distance in the projected complex is strictly smaller than the upper bound. However, through extensive numerics for $q \in \{2, 3, 2^2, 5, 7, 2^3, 3^2, 11\}$, we could not find a single case where the homological distance in the full product complex would fail to saturate the upper bound. We conjecture that in a product of general chain complexes, the upper bound on the homological distance is saturated.

1.4 Applications of HQHP codes

In theory of QEC, in addition to defining new classes of quantum LDPC codes with parameters known explicitly, our construction of HQHP codes may be useful for: (i) optimizing repeated measurements in the problem of FT quantum error correction[56, 57, 23, 24], (ii) related problem of single-shot error correction[58, 59, 60, 61], (iii) analysis of

transformations between different QECCs, like the distance-balancing trick by Hastings[44], and (iv) construction of asymmetric quantum CSS codes optimized for operation where error rates for X and Z channels may differ strongly[62, 63, 64, 65, 66, 67].

More generally, Künneth formula is one of the most important and widely known results in algebraic topology, see, e.g., Ref. [68]. Its well known consequence is the relation between the Betti numbers of two manifolds and their product, which can be written in terms of a product of the corresponding generating functions, the Poincare polynomials $p(x) = \mathrm{b}_0 + \mathrm{b}_1 x + \mathrm{b}_2 x^2 + \ldots$. Generally, b_k is the rank of the kth homology group. For manifolds in three dimensions, the zeroth Betti number, b_0, gives the number of connected components, the first, b_1, the number of one-dimensional holes (incontractible cycles), and b_2 the number of closed surfaces that cut out internal cavities. In particular, for a torus, $p(x) = 1 + 2x + x^2$, which can be written as $(1 + x)^2$, the square of the Poincare polynomial for a circle.

Our results can be seen as equipping Künneth formula with a distance. For example, consider a torus defined via periodic boundary conditions on a plane, e.g., with periods L_x and L_y along the x and y directions. Then, the systola (girth in the case of a graph) is $\min(L_x, L_y)$, while the surface area (number of plaquettes) is $L_x L_y$. More generally, for a tensor product of a circle with perimeter L and an arbitrary manifold with systola L'_1, minimum surface area L'_2, etc., the corresponding dimensions are given by $\min(L, L'_1)$, $\min(LL'_1, L'_2)$, ...

1.5 Data-syndrome codes

Quantum stabilizer codes are designed to be robust against qubit errors. However, syndrome measurement cannot be done perfectly: necessarily, there are some measurement errors whose probability grows with the weight of the checks (stabilizer generators). Furthermore, both the syndrome measurement protocol and the syndrome-based decoding have to operate in a fault-tolerant (FT) regime, to be robust against errors that happen during the measurement.

When all checks have relatively small weights, as in the case of the surface codes, one simple approach is to repeat syndrome measurement several times[13]. Then, FT syndrome-based decoding can be done in the assumption that the data errors accumulate while measurement errors be independently distributed. While there is always a non-vanishing probability to have some errors at the end of the cycle, what matters in practice is the ability to backtrack all errors after completion of several rounds of measurement.

Another approach is to measure an overcomplete set of stabilizer generators, using redundancy to recover the correct syndrome. Such an approach was used in the context of higher-dimensional toric and/or color codes[17, 69], the data-syndrome (DS) codes[58, 59, 60], and single-shot measurement protocols[70, 71, 61]. Here decoding is done in the assumption that data error remains the same during the measurement.

We note that with both approaches, the error models assumed for decoding do not exactly match the actual error probability distribution. In particular, any correlations between errors in different locations and/or different syndrome bits are typically ignored. Nevertheless, simulations with circuit-based error models which reproduce at least some of

the actual correlations show that both the repeated syndrome measurement protocol[72, 73] and the syndrome measurement protocols relying on an overcomplete set of generators[69] can result in competitive values of FT threshold.

The choice of the measurement protocol is typically dictated by the structure of the code, specifically, availability of an overcomplete set of stabilizer generators of the minimum weight. Such an approach is expected to be practical when typical gate infidelities are comparable with the probability of an incorrect qubit measurement. However, there is also a price to pay: codes with redundant sets of small-weight checks can be generally expected to have worse parameters.

On the other hand, if the physical one- and two-qubit gates are relatively accurate, it may turn out more practical to measure redundant sets of checks which include stabilizer generators of higher weights. Then, a DS code can be designed from any stabilizer code[58, 59, 60]. As a result, one faces the problem of constructing an optimal measurement protocol given the known gate fidelities and measurement errors.

I compare several single-shot and repeated measurement/decoding protocols for a simple quantum convolutional code[74] with the parameters $[[24, 6, 3]]$ and syndrome generators of weight 6. We construct several computationally efficient schemes using the classical Viterbi algorithm[75, 76] to decode data and syndrome errors sequentially or simultaneously, and compare their effectiveness both with phenomenological and circuit-based depolarizing error models. In particular, we show that a DS code which requires measuring checks of weight up to $w_{\max} = 9$ has performance (successful decoding probability) exceeding that of the repeated measurement scheme when single-qubit measurement error probability q_1

equals ten times the gate error probability p_1 (taken to be the same for Hadamard and CNOT gates).

1.6 Chapter overview

The outline of the rest of the thesis is as follows.

In Chapter 2 we go over the necessary background facts on the theory of classical and quantum error-correcting codes, as well as chain complexes of vector spaces over a finite field F. We also establish the relation between (co)homology groups in such a complex and F-linear quantum codes.

In Chapter 3 we describe the construction and derive upper and lower bounds for minimal distances of several related families of "product" codes constructed in terms of Kronecker products of matrices associated with a pair of quantum codes whose parameters are known.

In Chapter 4 we formulate main results in application to chain complexes, give detailed proofs, and discuss their use in fault-tolerant quantum error correction.

In Chapter 5, I show an alternative proof for the lower distance bound when one of the chain complexes has length 2, in the binary field. Although it has been proved in the previous chapter with a simpler method, this proof may give some hints on deriving the distance in the general case.

In Chapter 6, I introduce data-syndrome code as a way of adding redundancy in measurements. Both repetition code and a classical convolutional code were used to form

Table 1.1: List of Acronyms

QEC	Quantum error correction
QECC	Quantum error correcting code
LDPC	Low-density parity-check
qLDPC	quantum LDPC
FT	Fault-tolerant
CSS	Calderbank-Shor-Steane
QHP	quantum hypergraph-product
HQHP	higher-dimensional QHP
DS	Data-syndrome

higher-dimensional QHP codes by a tensor product with a quantum convolutional code. Various error models including circuit error model were tested in our numerical simulations.

Finally, in Section 7, we summarize the results and list some open questions in the development of qLDPC codes and beyond.

Chapter 2

Background

In this chapter, I introduce QECCs with qudits in general fields, and the map between CSS codes and chain complexes.

2.1 Classical q-ary codes

A classical q-ary code[77] $\mathcal{C}$ with parameters $(n, K, d)_q$ is a collection of K strings (codewords) of length n over an alphabet with q symbols. The code distance d is the minimum number of positions where two strings in the code differ. A linear q-ary code, where q is a power of a prime, is a k-dimensional subspace of the n-dimensional vector space F^n over the field $F \equiv \mathbb{F}_q$. Such a code contains $K = q^k$ strings. A linear code $\mathcal{C} \equiv \mathcal{C}_G$ with parameters $[n, k, d]_q$ can be defined in terms of a generator matrix G whose rows are the chosen basis vectors; the dimension k of the code $\mathcal{C}_G$ is $k = \operatorname{rank} G$. For a linear code, the distance d is the minimum Hamming weight of a non-zero vector in the code.

A linear subspace in F^n can be also specified in terms of its orthogonal subspace. To this end, one has to choose the inner product to be used[78, 79, 80]. The simplest choice is the usual Euclidean scalar product, $a \cdot b \equiv a\, b^T$, where $a, b \in F^n$ are considered as length-n row vectors, and b^T is the transposed vector. Respectively, the dual $\mathcal{C}^\perp$ of a linear code $\mathcal{C}$ is a collection of q-ary row vectors orthogonal to any vector in $\mathcal{C}$,

$$\mathcal{C}^\perp = \{b \in F^n | c\, b^T = 0, \forall c \in \mathcal{C}\}. \tag{2.1}$$

For a linear code of size $|\mathcal{C}| = q^k$ and dimension k, the dual code has size $|\mathcal{C}^\perp| = q^{n-k}$. Generator matrix H of the dual code, $\mathcal{C}_H \equiv \mathcal{C}_G^\perp$, is called a parity check matrix of the original code. More generally, a pair of n-column matrices G and H with elements in F are called *mutually dual* if

$$GH^T = 0, \quad \operatorname{rank} G + \operatorname{rank} H = n. \tag{2.2}$$

Given a string $c \in F^n$, denote $V \equiv \{1, 2, \ldots, n\}$ the set indexing the individual characters. For any *index set* $I \subseteq V$ of length $|I| = r$, let $c[I] \in F^r$ be a substring of c with the characters in all positions $i \notin I$ dropped. Similarly, for an n-column matrix G with rows g_j, $G[I]$ is formed by the rows $g_j[I]$. If $\mathcal{C} = \mathcal{C}_G$ is an F-linear code with the generating matrix G, the code of length $|I|$ with the generating matrix $G[I]$ is the code *punctured* outside I, $\mathcal{C}_{\rm p}[I] \equiv \{c[I]\,|\,c \in \mathcal{C}\}$.

The *shortened* code $\mathcal{C}_{\rm s}[I]$ is formed similarly, except only from the codewords supported inside I, $\mathcal{C}_{\rm s}[I] = \{c[I]\,|\,c = (c_1, c_2, \ldots, c_n) \in \mathcal{C}$ and $c_i = 0$ for each $i \notin I\}$. The dual of a punctured code $\mathcal{C}_{\rm p}[I]$ is the shortened dual code, $(\mathcal{C}_{\rm p}[I])^\perp = (\mathcal{C}^\perp)_{\rm s}[I]$. To express this relation in terms of matrices, consider a pair of mutually dual matrices in Eq. (2.2) and a code $\mathcal{C} \equiv \mathcal{C}_G = \mathcal{C}_H^\perp$. Denote a generator matrix of the shortened code $\mathcal{C}_{\rm s}[I]$ as G_I. Duality

between the punctured original and the shortened dual codes implies that the corresponding generator matrices G_I and $H[I]$ are also mutually dual[77],

$$H[I]\, G_I^T = 0, \quad \text{rank}\, G_I + \text{rank}\, H[I] = |I|. \tag{2.3}$$

Similarly, H_I is a dual of the punctured matrix $G[I]$.

In relation to quantum codes, we also consider q-ary linear space F^{2n} of length-$2n$ vectors in the form $e = (a|b)$, where both a and b are row vectors of length n. The *symplectic product* of two such vectors is defined as

$$e' \star e \equiv a' \cdot b - b' \cdot a \equiv e' \Sigma\, e^T. \tag{2.4}$$

The right-most form contains the symplectic matrix,

$$\Sigma \equiv \Sigma_n = \begin{pmatrix} & I_n \\ -I_n & \end{pmatrix}, \tag{2.5}$$

with I_n an $n \times n$ identity matrix. For a row vector $e \in \mathbb{F}^{2n}$, the (symplectic) conjugate is $\tilde{e} = e\, \Sigma^T = -e\, \Sigma$, so that the symplectic product can be also written as $e' \star e = e'\, \tilde{e}^T$. The code orthogonal with respect to the symplectic product to a given q-ary code $\mathcal{C} \subseteq F^{2n}$ is denoted $\mathcal{C}^{\perp\star}$. A code $\mathcal{C}_G^{\perp\star}$ orthogonal to $\mathcal{C}_G$ has generator matrix $G^\star$, a (symplectic) parity check matrix of the original code $\mathcal{C}_G$ and also a Euclidean dual of the matrix $\tilde{G} = -G\Sigma$, see Eq. (2.2), except that the code length here is $2n$. Explicitly, for a generator matrix in the block form $G = (A|B)$, where each block has n columns, rows of $G^\star$ are orthogonal to the rows of $\tilde{G} = (B| -A)$, $\tilde{G}(G^\star)^T = 0$.

2.2 Quantum stabilizer codes over qudits

A single qudit is an isolated quantum-mechanical system whose pure states are described by vectors $|\psi\rangle$ in a q-dimensional Hilbert space $\mathcal{H}_q$. Pure states of n qudits are described by vectors in the Hilbert space $\mathcal{H}_q^{\otimes n}$, the tensor product of n single-qudit spaces. The corresponding physical observables are described by Hermitian operators acting in $\mathcal{H}_q^{\otimes n}$. An n-qudit quantum error-correcting code $\mathcal{Q}$ with parameters $((n, K))_q$ is a K-dimensional subspace of $\mathcal{H}_q^{\otimes n}$.

When $q = p^m$ is a power of a prime, there is a particularly nice basis for single-qudit operators acting in $\mathcal{H}_q$. Following Ref. [79], choose q orthonormal basis vectors $|z\rangle \in \mathcal{H}_q$, $z \in F$, enumerated by elements of the finite field $F \equiv \mathbb{F}_q$. Two kinds of unitary operators, $\hat{X}(a)$ and $\hat{Z}(a)$, $a \in F$, also enumerated by elements of the field, are defined in terms of their action on the basis vectors,

$$\hat{X}(a)\,|z\rangle = |z + a\rangle\,, \quad \hat{Z}(b)\,|z\rangle = \omega^{\mathrm{tr}(bz)}\,|z\rangle\,, \tag{2.6}$$

where, with $q = p^m$ a prime power,

$$\mathrm{tr}(x) \equiv \mathrm{tr}_{F/\mathbb{F}_p}(x) = x + x^p + \ldots + x^{p^{m-1}} \tag{2.7}$$

is the trace operation from the extension field $F = \mathbb{F}_q$ to the prime field $\mathbb{F}_p$, and $\omega = e^{2\pi i/p}$ is a primitive pth root of unity. The basis of interest is formed by the q^2 operators $\hat{X}(a)\hat{Z}(b)$, $a, b \in F$.

The same operators can be used to construct a basis of operators acting in an n-qudit Hilbert space $\mathcal{H}_q^{\otimes n}$. Namely, given a q-ary vector $a \in F^n$, define the n-qubit operators $\hat{X}(a)$ and $\hat{Z}(a)$ as tensor products over components, e.g., $\hat{X}(a) = \hat{X}(a_1) \otimes \hat{X}(a_2) \otimes \ldots \otimes$

$\hat{X}(a_n)$. These operators generate the n-qudit Pauli group

$$\mathcal{P}_n = \left\{ \omega^c \hat{X}(a)\hat{Z}(b) | c \in \mathbb{F}_p,\, a, b \in F^n \right\}. \tag{2.8}$$

The weight $\mathrm{wgt}(\hat{U})$ of an operator $\hat{U} \in \mathcal{P}_n$ is defined as the number of qudits that $\hat{U}$ acts upon non-trivially. Up to a phase, a Pauli operator $\hat{U}(a, b; c) \equiv \omega^c \hat{X}(a)\hat{Z}(b)$ can be specified by the vector $e \equiv (a|b) \in \mathbb{F}_q^{2n}$. The commutation relation between two such operators (with inessential phase factors suppressed) reads

$$\hat{U}(a, b)\hat{U}(a', b') = \omega^{\mathrm{tr}(a \cdot b' - b \cdot a')} \hat{U}(a', b')\hat{U}(a, b). \tag{2.9}$$

In particular, the two operators commute if and only if the trace symplectic form $\mathrm{tr}(a \cdot b' - b \cdot a')$ vanishes.

An n-qudit stabilizer code is a common $+1$ eigenspace of all operators in a *stabilizer* group $\mathcal{S}$,

$$\mathcal{Q} \equiv \mathcal{Q}_{\mathcal{S}} = \left\{ |\psi\rangle \in \mathcal{H}_q^{\otimes n} | \hat{U} |\psi\rangle = |\psi\rangle \,, \forall \hat{U} \in \mathcal{S} \right\}, \tag{2.10}$$

where $\mathcal{S}$ is an abelian subgroup of $\mathcal{P}_n$ whose only zero-weight member is the identity operator. It is easy to see that any Pauli operator $\hat{E}$ which does not commute with an element of the stabilizer throws the code $\mathcal{Q}_{\mathcal{S}}$ into an orthogonal space $\hat{E}\mathcal{Q}_{\mathcal{S}}$; such operators are called *detectable* errors. *Undetectable* errors commute with all elements of $\mathcal{S}$. In particular, all elements of $\mathcal{S}$ are undetectable. However, since these operators act trivially in the code, such errors can be ignored. Only undetectable errors outside of $\mathcal{S}$ (up to a phase) are relevant for error correction. Such errors act non-trivially in the code and correspond to *logical* operators. The *distance* d of a stabilizer code is defined as the minimum weight of an undetectable Pauli operator not equal (up to a phase) to an element of $\mathcal{S}$. Similarly,

errors $\hat{E} \in \mathcal{P}_n$ and $\hat{E}' = \omega^c \hat{S}\hat{E}$ that differ by an element $\hat{S} \in \mathcal{S}$ of the stabilizer group (again, up to a phase) are called mutually *degenerate*; for all practical purposes such errors are equivalent.

Up to the choice of the phases of its generators, a stabilizer group can be also represented as a length-$2n$ additive code over $\mathbb{F}_q$, isomorphic to a length-$2nm$ linear code over the prime field $\mathbb{F}_p$, where $q = p^m$. The commutation condition gives an additional requirement that the rows of the generator matrix be mutually orthogonal with respect to the symplectic trace product. In general, any element $x \in \mathbb{F}_q$ of an extension of a field of prime degree p is p-periodic with respect to addition, $p\,x = 0$. Respectively, the size of a stabilizer group is a power of the prime p. This gives the code dimension $K = q^n/|\mathcal{S}| = p^s$, which is not necessarily an integral power of q. Thus, excluding the case of a prime field analyzed in Ref. [81], a stabilizer code does not necessarily encodes an integer number of qudits. The latter condition is satisfied under an additional constraint, $s \bmod m = 0$.

2.3 F-linear quantum codes

In this work we focus on the special case of F-linear length-$2n$ codes formed by vectors of the form $e = (a|b)$, $a, b \in F^n$, and duality implemented in terms of the Euclidean symplectic product (2.4). Unlike in Eq. (2.9), there is no field trace in this expression. Thus, $e \star e' = 0$ gives a sufficient but not a necessary condition for the Pauli operators $\hat{U}(e)$ and $\hat{U}(e')$ to commute, unless q is a prime. Such an approach follows the definition of CSS codes in Ref. [79]. Alternatively, many of the same results can be obtained by classifying generators in terms of a lifted Pauli group as suggested by Gottesman[82].

Degeneracy is the key difference of quantum codes from their classical counterparts. Two vectors e and e' in F^{2n} are called *degenerate* with respect to elements of the F-linear code $\mathcal{C}_G$ generated by an $r \times 2n$ matrix G iff there exists an $\alpha \in F^r$ such that $e' = e + \alpha G$. Degeneracy with respect to $\mathcal{C}_G$ is denoted $e' \overset{G}{\simeq} e$, where the generating matrix may be omitted if the meaning is clear from context.

In the simplest case rows of the generator matrix $H = (A|B)$ (here and below denoted as H to indicate that orthogonality is expected) are mutually orthogonal with respect to the symplectic product,

$$H\tilde{H}^T \equiv H\Sigma H^T = AB^T - BA^T = 0, \tag{2.11}$$

which is equivalent to $\mathcal{C}_H \subseteq \mathcal{C}_H^{\perp\star}$. The space $\mathcal{C}_H$ is readily seen as the symplectic map of a stabilizer group acting in $\mathcal{H}_q^{\otimes n}$. The corresponding dual code $\mathcal{C}_H^{\perp\star}$, with any pair of vectors degenerate with respect to $\mathcal{C}_H$ identified, is called an F-linear *stabilizer code*. The same object is also known as the quotient space $\mathcal{C}_H^{\perp\star}/\mathcal{C}_H$.

Given any set of $(m \operatorname{rank} H)$ additively independent basis vectors of $\mathcal{C}_H$, a stabilizer group $\mathcal{S} \subseteq \mathcal{P}_n$ can be constructed by assigning each generator a phase $c \in \mathbb{F}_p$. With this map, vectors in $\mathcal{C}_H^{\perp\star}$ correspond (up to a phase) to undetectable Pauli errors, i.e., operators acting in the space $\mathcal{Q}_\mathcal{S} \subseteq \mathcal{H}_q^{\otimes n}$ stabilized by $\mathcal{S}$. Stabilizer group being abelian, it is a subgroup of the group $\mathcal{L}_\mathcal{S}$ of all undetectable Pauli errors acting in $\mathcal{H}_q^{\otimes n}$. Thus, mutually non-degenerate logical operators are classified by elements of the quotient group $\mathcal{L}_\mathcal{S}/\mathcal{S}$. If we ignore the phases, this group is isomorphic to the F-linear stabilizer code $\mathcal{C}_H^{\perp\star}/\mathcal{C}_H$. Notice that the subspace $\mathcal{Q}_\mathcal{S} \subseteq \mathcal{H}_q^{\otimes n}$ is also called a stabilizer code, but this should not cause a confusion as we will exclusively use the former meaning.

For an F-linear stabilizer code based on the generator matrix H, any codeword c satisfies $\tilde{H}c^T = 0$, see Eq. (2.11); equivalent codewords are mutually degenerate, $c' \overset{H}{\simeq} c$. Using orthogonalization, we can construct $k = n - \operatorname{rank} H$ pairs of canonically conjugated codewords c_i, c_i' such that $c_i \star c_j' = \delta_{ij}$, $i, j \leq k$. Equivalently, we can construct a *logical generator* matrix L whose rows are orthogonal to those of $\tilde{H}$, $\tilde{H}L^T = 0$, are linearly independent from rows of H, and, in addition,

$$L\Sigma_n L^T = \Sigma_k. \tag{2.12}$$

More generally, with $\tilde{G}G^T$ not necessarily zero, $\mathcal{C}_G$-degeneracy classes of different vectors in $\mathcal{C}_G^{\perp\star}$ correspond to an F-linear *subsystem code*, a generalization of qubit subsystem codes[83, 84]. Elements of $\mathcal{C}_G$ form a symplectic map of subsystem code's *gauge group*, while vectors $c \in \mathcal{C}_G^{\perp\star}$ correspond to *bare* logical operators. Multiplication of a bare logical operator $\hat{U}(c)$ by an element of the gauge group gives a *dressed* logical operator; with the symplectic map this corresponds to adding a linear combination of the rows of G. Nonequivalent logical operators in $\mathcal{P}_n$ map to vectors in F^{2n} which are not degenerate with respect to $\mathcal{C}_G$, $c' \not\simeq c$.

A subsystem code can also be defined in terms of a stabilizer code whose stabilizer group maps to the space $\mathcal{C}_H \equiv \mathcal{C}_G \cap \mathcal{C}_G^{\perp\star}$ of dimension $r = \operatorname{rank} G - 2\kappa$, where $2\kappa = \operatorname{rank}(G\tilde{G}^T)$. The space $\mathcal{C}_H$ is generated by code's *stabilizer generator* matrix H whose rows are linear combinations of the rows of G, and also $\tilde{G}H^T = 0$. The corresponding orthogonal space $\mathcal{C}_H^{\perp\star}$ contains $k + \kappa = n - r$ canonically conjugated vector pairs, including κ such pairs in $\mathcal{C}_G$ (these correspond to gauge qudits) and k pairs in $\mathcal{C}_G^{\perp\star} \setminus \mathcal{C}_G$ corresponding to logical operators of the data qudits.

In the following, we will be mostly interested in CSS codes[79], a special class of F-linear subsystem (or stabilizer) codes whose generator matrices can be chosen in a block-diagonal form, $G = \mathrm{diag}(G_X, G_Z)$, with each block containing n columns. The corresponding stabilizer generator matrix also has a block form, $H = \mathrm{diag}(H_X, H_Z)$; the symplectic orthogonality is equivalent to $G_X H_Z^T = 0$ and $G_Z H_X^T = 0$. Such a code, denoted $\mathrm{CSS}(G_X, G_Z)$, is a direct sum of an X- and a Z-like codes,

$$\mathrm{CSS}(G_X, G_Z) = \mathcal{C}_X \oplus \mathcal{C}_Z = \mathcal{C}_{H_Z}^{\perp}/\mathcal{C}_{G_X} \oplus \mathcal{C}_{H_X}^{\perp}/\mathcal{C}_{G_Z}, \tag{2.13}$$

where each term in the r.h.s. is a quotient of two linear spaces. Clearly, the spaces $\mathcal{C}_X$ and $\mathcal{C}_Z$ are identical to those in *gauge-fixed* stabilizer codes with generator matrices $H_1 = \mathrm{diag}(G_X, H_Z)$ and $H_2 = \mathrm{diag}(H_X, G_Z)$, respectively. Gauge generator matrix contains κ conjugate vector pairs not in $\mathcal{C}_H$, thus $\mathrm{rank}\, G_X = \mathrm{rank}\, H_X + \kappa$ and $\mathrm{rank}\, G_Z = \mathrm{rank}\, H_Z + \kappa$. As a result, both codes in the r.h.s. of Eq. (2.13) contain $k = n - \mathrm{rank}\, H_X - \mathrm{rank}\, G_Z$ inequivalent vectors. The distances of the two codes are

$$d_X = \min_{x \in \mathcal{C}_{H_Z}^{\perp} \setminus \mathcal{C}_{G_X}} \mathrm{wgt}(x),\ d_Z = \min_{x \in \mathcal{C}_{H_X}^{\perp} \setminus \mathcal{C}_{G_Z}} \mathrm{wgt}(x). \tag{2.14}$$

Any k inequivalent codewords from $\mathcal{C}_X$ can be chosen to form the rows of a logical generator matrix L_X; in general $L_X H_Z^T = 0$. However, it is convenient to choose bare codewords for the basis, so that also $L_X G_Z^T = 0$. Using bare codewords for the basis of the logical generator matrix of the other code, L_Z, this matrix will satisfy $L_Z G_X^T = 0$. In addition, choosing conjugate vector pairs for the two bases, we can also ensure

$$L_X L_Z^T = I_k; \tag{2.15}$$

with the full-code logical generator matrix in the block-diagonal form, $L = \mathrm{diag}(L_X, L_Z)$. This is the CSS form of Eq. (2.12). Parameters of such a CSS code are denoted as $[[n, k, (d_X, d_Z)]]_q$, where the usual code distance is given by the minimum, $d = \min(d_X, d_Z)$.

2.4 Chain complex of F-linear spaces.

Generally, a *chain complex* is a sequence of abelian groups and a sequence of homomorphisms (boundary operators) between pairs of consecutive groups such that the image of each homomorphism be included in the kernel of the next. Here we will be concerned with the special case of chain complexes of finite-dimensional vector spaces $\ldots, \mathcal{A}_{j-1}, \mathcal{A}_j, \ldots$ over a finite field $F = \mathbb{F}_q$, where $q = p^m$ is a power of a prime p. In this case the boundary operators are linear transformations $\partial_j : \mathcal{A}_{j-1} \leftarrow \mathcal{A}_j$ that map between each pair of neighboring spaces, with the requirement $\partial_j \partial_{j+1} = 0$, $j \in \mathbb{Z}$. We define an ℓ-complex $\mathcal{A} \equiv \mathcal{K}(A_1, \ldots, A_\ell)$, a bounded chain complex which only contains $\ell + 1$ non-trivial spaces with fixed bases, in terms of $n_{j-1} \times n_j$ matrices A_j with elements from F serving as the boundary operators, $j \in \{1, \ldots, \ell\}$:

$$\mathcal{A} : \ \ldots \leftarrow \{0\} \overset{\partial_0}{\leftarrow} \mathcal{A}_0 \overset{A_1}{\leftarrow} \mathcal{A}_1 \ldots \overset{A_\ell}{\leftarrow} \mathcal{A}_\ell \overset{\partial_{\ell+1}}{\leftarrow} \{0\} \ldots \tag{2.16}$$

Here the neighboring matrices must be mutually orthogonal, $A_{j-1} A_j = 0$, $j \in \{2, \ldots, \ell\}$. In addition to boundary operators given by the matrices A_j, implicit are the trivial operators $\partial_0 : \{0\} \leftarrow \mathcal{A}_0$ and $\partial_{\ell+1} : \mathcal{A}_\ell \leftarrow \{0\}$ (with the image being the zero vector in $\mathcal{A}_\ell$) treated formally as rank-zero $0 \times n_0$ and $n_\ell \times 0$ matrices.

Elements of the subspace $\mathrm{Im}(\partial_{j+1}) \subseteq \mathcal{A}_j$ are called boundaries; in our case these are linear combinations of columns of A_{j+1} and, therefore, form an F-linear code with the

generator matrix A_{j+1}^T, $\mathrm{Im}(A_{j+1}) = \mathcal{C}_{A_{j+1}^T}$. In the singular case $j = \ell$, $\mathrm{Im}(\partial_{\ell+1}) = \{0\}$, a trivial vector space. Elements of $\mathrm{Ker}(\partial_j) \subset \mathcal{A}_j$ are called cycles; in our case these are vectors in a F-linear code with the parity check matrix A_j, $\mathrm{Ker}(A_j) = \mathcal{C}_{A_j}^{\perp}$. In the singular case $j = 0$, $\mathrm{Ker}(\partial_0) = \mathcal{A}_0$, the entire space.

Because of the orthogonality $\partial_j \partial_{j+1} = 0$, all boundaries are necessarily cycles, $\mathrm{Im}(\partial_{j+1}) \subseteq \mathrm{Ker}(\partial_j) \subseteq \mathcal{A}_j$. The structure of the cycles in $\mathcal{A}_j$ that are not boundaries is described by the j th homology group,

$$H_j(\mathcal{A}) \equiv H(A_j, A_{j+1}) = \mathrm{Ker}(A_j)/\,\mathrm{Im}(A_{j+1}). \tag{2.17}$$

Group quotient here means that two cycles [elements of $\mathrm{Ker}(A_j)$] that differ by a boundary [element of $\mathrm{Im}(A_{j+1})$] are considered equivalent; non-zero elements of $\mathcal{H}_j(\mathcal{A})$ are equivalence classes of homologically non-trivial cycles. Explicitly, the equivalence of x and y in $\mathcal{A}_j$ implies that for some $\alpha \in \mathcal{A}_{j+1}$, $y = x + \alpha A_{j+1}^T$. The rank of j-th homology group is the dimension of the corresponding vector space; one has

$$k_j \equiv \mathrm{rank}\, H_j(\mathcal{A}) = n_j - \mathrm{rank}\, A_j - \mathrm{rank}\, A_{j+1}. \tag{2.18}$$

The homological *distance* d_j is the minimum Hamming weight of a non-trivial element (any representative) in the homology group $H_j(\mathcal{A}) \equiv H(A_j, A_{j+1})$,

$$d_j = \min_{0 \not\sim x \in H_j(\mathcal{A})} \mathrm{wgt}\, x = \min_{x \in \mathrm{Ker}(A_j) \setminus \mathrm{Im}(A_{j+1})} \mathrm{wgt}\, x. \tag{2.19}$$

By this definition, $d_j \geq 1$. To address singular cases, throughout this work we define the minimum of an empty set as infinity; $k_j = 0$ is always equivalent to $d_j = \infty$. In particular, the distance of the homology group $H_0(\mathcal{A})$ is $d_0 = 1$, unless A_1 has full row rank, giving $k_0 = 0$, in which case we get $d_0 = \infty$. In the case of the homology group $H_\ell(\mathcal{A})$, the distance

d_ℓ is that of the F-linear code $\mathcal{C}_{A_\ell}^\perp$. Again, we get $d_\ell = \infty$ if $k_\ell = 0$, which happens when A_ℓ has full column rank.

In addition to the homology group $H(A_j, A_{j+1})$, there is also a *co-homology* group $\tilde{H}_j(\tilde{\mathcal{A}}) = H(A_{j+1}^T, A_j^T)$ of the same rank (2.18); this is associated with the *co-chain complex* $\tilde{\mathcal{A}}$ formed from the transposed matrices A_j^T taken in the opposite order. A quantum CSS code with generator matrices $G_X = A_j$ and $G_Z = A_{j+1}^T$ is isomorphic with the direct sum of the groups H_j and $\tilde{H}_j$, cf. Eq. (2.13),

$$\mathrm{CSS}(A_j, A_{j+1}^T) \cong H(A_j, A_{j+1}) \oplus H(A_{j+1}^T, A_j^T). \tag{2.20}$$

The two terms correspond to Z and X logical operators, respectively. This gives for the homological distances in the chain complex and in the co-chain complex, respectively, $d_j = d_Z$ and $\tilde{d}_j = d_X$.

The tensor product $\mathcal{A} \times \mathcal{B}$ of two chain complexes $\mathcal{A}$ and $\mathcal{B}$ is defined as the chain complex formed by linear spaces decomposed as direct sums of Kronecker products,

$$(\mathcal{A} \times \mathcal{B})_j = \bigoplus\nolimits_{i \in \mathbb{Z}} \mathcal{A}_i \otimes \mathcal{B}_{j-i}, \tag{2.21}$$

with the action of the boundary operators

$$\partial'''(a \otimes b) \equiv \partial' a \otimes b + (-1)^i a \otimes \partial'' b, \tag{2.22}$$

where $a \in \mathcal{A}_i$, $b \in \mathcal{B}_{j-i}$, and the boundary operators ∂', ∂'', and ∂''' act in complexes $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{A} \times \mathcal{B}$, respectively. Notice that the two terms in Eq. (2.22) are supported in different subspaces of the expansion (2.21). When both $\mathcal{A}$ and $\mathcal{B}$ are *bounded*, that is, they include finite numbers of non-trivial spaces, the dimension $n_j(\mathcal{C})$ of a space $\mathcal{C}_j$ in the product

$\mathcal{C} = \mathcal{A} \times \mathcal{B}$ is

$$n_j(\mathcal{C}) = \sum\nolimits_i n_i(\mathcal{A})\, n_{j-i}(\mathcal{B}). \tag{2.23}$$

The homology groups of the product $\mathcal{C} = \mathcal{A} \times \mathcal{B}$ are isomorphic to a simple expansion in terms of those of $\mathcal{A}$ and $\mathcal{B}$ which is given by the Künneth formula,

$$H_j(\mathcal{C}) \cong \bigoplus\nolimits_i H_i(\mathcal{A}) \otimes H_{j-i}(\mathcal{B}). \tag{2.24}$$

One immediate consequence is that the rank $k_j(\mathcal{C})$ of the j th homology group $H_j(\mathcal{C})$ is

$$k_j(\mathcal{C}) = \sum\nolimits_i k_i(\mathcal{A})\, k_{j-i}(\mathcal{B}). \tag{2.25}$$

Such a convolution can be also written as a product of the Poincare polynomials $p_{\mathcal{A}}(x) \equiv \sum_j k_j(\mathcal{A}) x^j$ corresponding to the two complexes, $p_{\mathcal{C}}(x) = p_{\mathcal{A}}(x) p_{\mathcal{B}}(x)$.

Chapter 3

Minimal distances of certain F-linear CSS codes

The HQHP codes generalize quantum hypergraph product (QHP) codes and toric codes in all dimensions. The HQHP codes projected into a single space gives subsystem product codes, which can then be gauge fixed to concatenated codes or homological product codes. Those include some common CSS codes, like Shors codes, Bacon Shors codes, and subsystem QHP codes. In this chapter I introduce those codes and related properties.

3.1 Subsystem product codes and their gauge-fixed versions

Our main tool is the map (2.20) between a CSS code and the homology groups of associated chain and co-chain complexes. In this section we derive the minimum distances of several classes of CSS codes which are relevant for the analysis of the homological distances

in the tensor products of chain complexes. Although the derivations are not technically hard, these results may be of independent value.

The distance bounds are constructed using the following two Lemmas which, in turn, follow from Eq. (2.3) and the fact that for any CSS stabilizer code $\mathrm{CSS}(H_X, H_Z)$ with logical generator matrix $L = \mathrm{diag}(L_X, L_Z)$, the dual code $\mathcal{C}_{H_X}^{\perp}$ coincides with the space generated by the combined rows of H_Z and L_Z, while $\mathcal{C}_{H_Z}^{\perp}$ coincides with the space generated by rows of H_X and L_X combined.

Lemma 1 (Z-puncturing bound) *Consider a stabilizer code $\mathcal{Q} = \mathrm{CSS}(H_X, H_Z)$; denote V the set indexing its variable nodes (columns of the matrices H_X, H_Z). For any decomposition into complementary sets $I \subset V$ and $J = V \setminus I$, let $Q' = \mathrm{CSS}\big((H_X)_I, H_Z[I]\big)$ and $Q'' = \mathrm{CSS}\big((H_X)_J, H_Z[J]\big)$ be the codes whose X generator matrices are shortened and Z generator matrices punctured to I and J, respectively. Then the Z-distances of the three codes satisfy the inequality $d_Z \geq \min(d'_Z, d''_Z)$, if the logical qubits satisfy $k = k' + k''$.*

Proof. Assume the code Q encodes $k > 0$ qudits (the case $k = 0$ is trivial), and let the matrix H_Z contain r rows. The distance d_Z of the code is the minimum weight in the set $Q_Z = \mathcal{C}_{H_X}^{\perp} \setminus \mathcal{C}_{H_Z}$ of all non-trivial codewords and their equivalent vectors. For any $c \in Q_Z$, the punctured codeword $c[I]$ is either trivial or it is in Q'_Z. Similarly, $c[J]$ is either trivial or in Q''_Z. For any $c \in \Omega_Z$, we have $\mathrm{wgt}\, c[I] + \mathrm{wgt}\, c[J] = \mathrm{wgt}\, c > 0$. The punctured codewords $c[I]$ and $c[J]$ contribute to the distances of the corresponding codes only if the corresponding weight is non-zero. Let $d(c)$ equal infinity if $\mathrm{wgt}\, c = 0$, and $\mathrm{wgt}\, c \geq 1$ otherwise. Then, $\min\big(d(c[I]), d(c[J])\big) \leq d(c)$. Minimize over all $c \in \mathcal{Q}_Z$ to get the desired inequality. ∎

Lemma 2 (Z-shortening bound) *Consider a stabilizer code $\mathcal{Q} = \mathrm{CSS}(H_X, H_Z)$ with the set V indexing its variable nodes. For any index set $I \subset V$, let $Q' = \mathrm{CSS}\left(H_X[I], (H_Z)_I\right)$ be the code whose X generator matrix is punctured and Z generator matrices shortened to I. Then (i) the Z-distances of the original code does not exceed that of Q', $d_Z \leq d'_Z$. (ii) This inequality is saturated if the support of a minimum-weight codeword in Q_Z is contained in I.*

Proof. This follows from the facts that (a) any codeword in Q'_Z is also in Q_Z, and (b) that any codeword in Q_Z which is supported on I is also in Q'_Z. ■

We now consider several "product" codes related to the subsystem code $\mathcal{Q}^{\mathrm{subs}} = \mathrm{CSS}(G_X, G_Z)$ with the gauge generator matrices

$$G_X = \begin{pmatrix} H_X^A \otimes I(n_B) \\ \\ I(n_A) \otimes H_X^B \end{pmatrix}, \; G_Z = \begin{pmatrix} H_Z^A \otimes I(n_B) \\ \\ I(n_A) \otimes H_Z^B \end{pmatrix}, \tag{3.1}$$

constructed in terms of generator matrices of a pair of stabilizer codes $Q_A = \mathrm{CSS}(H_X^A, H_Z^A)$ and $Q_B = \mathrm{CSS}(H_X^B, H_Z^B)$ with parameters $[[n_A, k_A, (d_X^A, d_Z^A)]]_q$ and $[[n_B, k_B, (d_X^B, d_Z^B)]]_q$, respectively.

Lemma 3 (Subsystem product code) *Denote L_X^A, L_Z^A and L_X^B, L_Z^B the logical generator matrices of the CSS stabilizer codes $\mathrm{CSS}(H_X^A, H_Z^A)$ and $\mathrm{CSS}(H_X^B, H_Z^B)$, respectively, chosen so that*

$$L_X^A (L_Z^A)^T = I(k_A), \quad L_X^B (L_Z^B)^T = I(k_B). \tag{3.2}$$

Then the subsystem product code *with CSS gauge generator matrices (3.1) has logical generator matrices*

$$L_X = L_X^A \otimes L_Z^B, \quad L_Z = L_Z^A \otimes L_Z^B, \tag{3.3}$$

and stabilizer generator matrices

$$H_X = \begin{pmatrix} H_X^A \otimes H_X^B \\ H_X^A \otimes L_X^B \\ L_X^A \otimes H_X^B \end{pmatrix}, \quad H_Z = \begin{pmatrix} H_Z^A \otimes H_Z^B \\ H_Z^A \otimes L_Z^B \\ L_Z^A \otimes H_Z^B \end{pmatrix}. \tag{3.4}$$

Proof. Matrices

$$P_A = \begin{pmatrix} L_Z^A \\ H_Z^A \end{pmatrix}, \quad P_B = \begin{pmatrix} L_Z^B \\ H_Z^B \end{pmatrix} \tag{3.5}$$

are the parity check matrices for the classical F-linear codes with generator matrices H_X^A and H_X^B, respectively. Thus, a classical code with generator matrix G_X in Eq. (3.1) has a parity check matrix $P_A \otimes P_B$. Out of the four row blocks of the latter matrix, only rows of $L_Z = L_Z^A \otimes L_Z^B$ are linearly independent from the rows of G_Z, as can be verified by taking scalar products with the rows of L_X. The remaining row blocks can be readily seen as linear combinations of the rows of G_Z; they form the matrix H_Z. The proof for L_X and H_X is similar. ■

Theorem 4 (Concatenated-stabilizer CSS code) *Let $\mathcal{Q}_A$ and $\mathcal{Q}_B$ be two F-linear CSS stabilizer codes used to define matrices (3.1), with logical generator matrices (3.2). Use n_B copies of the code $\mathcal{Q}_A$, with logical operators used as qudits for the outer code, to form a* concatenated-stabilizer code $\overline{\mathcal{Q}}$ *with CSS generator matrices*

$$\overline{H}_X = \begin{pmatrix} H_X^A \otimes I(n_B) \\ L_X^A \otimes H_X^B \end{pmatrix}, \; \overline{H}_Z = \begin{pmatrix} H_Z^A \otimes I(n_B) \\ L_Z^A \otimes H_Z^B \end{pmatrix}. \tag{3.6}$$

The logical generator matrices of thus constructed code are given by Eq. (3.3), and the parameters are given by the corresponding products $[[n_A n_B, k_A k_B, (d_X^A d_X^B, d_Z^A d_Z^B)]]_q$.

Proof. It is easy to check that $\overline{H}_X \overline{H}_Z^T = 0$; this is a stabilizer code. Similarly, we get $\overline{H}_X L_Z^T = 0$, $\overline{H}_Z L_X^T = 0$, $L_X L_Z^T = I(k_A) \otimes I(k_B)$, and the matrix ranks

$$\begin{aligned} \operatorname{rank} \overline{H}_X &= \operatorname{rank} H_X^A \, n_B + k_A \operatorname{rank} H_X^B, && (3.7) \\ \operatorname{rank} \overline{H}_Z &= \operatorname{rank} H_Z^A \, n_B + k_A \operatorname{rank} H_Z^B, && (3.8) \\ \operatorname{rank} L_X &= \operatorname{rank} L_Z = k_A k_B; && (3.9) \end{aligned}$$

these expressions add up to the code length $n_A n_B$. This verifies the CSS construction and the number of encoded qudits $k = k_A k_B$. The case $k = 0$ is trivial; in the following, assume $k > 0$. To construct the upper distance bounds, e.g., $d_Z \leq d_Z^A d_Z^B$, consider pairs of conjugated codewords a, a' and b, b' in $\mathcal{Q}_A$ and $\mathcal{Q}_B$, respectively, where a and b are Z-like with $\operatorname{wgt} a = d_Z^A$, $\operatorname{wgt} b = d_Z^B$, and $a' a^T = b' b^T = 1$. Then the vector $c = a \otimes b$ of weight $d_Z^A d_Z^B$ satisfies $\overline{H}_X c^T = 0$. Further, its dual $a' \otimes b'$ is orthogonal to the rows of $\overline{H}_Z$, which implies that c cannot be a linear combination of the rows of $\overline{H}_Z$. Taken together, this proves $c \in \overline{\mathcal{Q}}_Z$, thus its weight gives a valid upper bound on d_Z.

To construct a matching lower distance bound, assume there is a non-trivial codeword $c \in \overline{\mathcal{Q}}_Z$ such that $\operatorname{wgt}(c) < d_Z^A d_Z^B$. This implies $\overline{H}_X c^T = 0$, and also that c must be linearly independent from the rows of $\overline{H}_Z$. Let $e_j \in F^{n_B}$, $j \in \{1, \ldots, n_B\}$ be vectors with all zero components except a one at position j. Consider a decomposition

$$c = \sum_j a_j \otimes e_j, \quad \text{where} \quad a_j \in F^{n_A}. \tag{3.10}$$

From the upper row blocks of the generators (3.6), each non-zero a_j must either be a non-trivial Z-like vector in the code $\mathcal{Q}_A$, or a linear combination of the rows of H_Z^A. This implies that any non-zero a_j such that $\operatorname{wgt}(a_j) < d_Z^A$ can be removed from c (set to zero) without

any other changes; the resulting vector c' should remain in the code as the two vectors are degenerate with respect to $\mathcal{C}_{\overline{H}_Z}$. This vector has weight $\mathrm{wgt}(c') \leq \mathrm{wgt}(c) < d_Z^A d_Z^B$, and any non-zero component a_j in its expansion (3.10) has weight d_Z^A or larger. Let $J \subset \{1, 2, \ldots, n_B\}$ be the set of positions j corresponding to non-zero a_j in the expansion of c'. By this logic,

$$d_Z^A d_Z^B > \mathrm{wgt}(c') = \sum_{j \in J} \mathrm{wgt}(a_j) \geq d_Z^A |J|; \tag{3.11}$$

the total number of positions in J satisfies $|J| < d_Z^B$. Denote $V_A = \{1, 2, \ldots, n_A\}$ and $I \equiv V_A \otimes J$; the punctured vector $c'[I]$ preserves all non-zero positions in c'. Thus, $c'[I]$ should be in the code $\mathcal{Q}' = \mathrm{CSS}\left(\overline{H}_X[I], (\overline{H}_Z)_I\right)$, see Lemma 2. By construction, the matrices $\overline{H}_X[I]$ and $(\overline{H}_Z)_I$ have the same structure (3.6), except the code $\mathcal{Q}_B$ is replaced with $\mathcal{Q}'_B = \mathrm{CSS}\left(H_X[J], (H_Z)_J\right)$ of length $|J|$. This latter code also satisfies Lemma 2; we expect the corresponding distance to serve as an upper bound to d_Z^B. However, since its length $|J| < d_Z^B$, the only possibility is for the code $\mathcal{Q}'_B$ to encode no qubits, $k'_B = 0$. Necessarily, the code Q' also has $k' = k_A k'_B = 0$, which makes the initial assumption about the existence of the codeword c invalid; this proves $d_Z = d_Z^A d_Z^B$. ■

3.2 Bounds on the minimal distance

Notice that rows of H_Z in Eq. (3.4) are linear combinations of rows of $\overline{H}_Z$ in Eq. (3.6), whose rows are, in turn, linear combinations of rows of G_Z in Eq. (3.1). Similar relation exists between the corresponding X matrices. As a result, there is a sequence of inclusions,

$$\mathcal{C}^{\perp}_{G_X} \setminus \mathcal{C}_{H_Z} \subseteq \mathcal{C}^{\perp}_{\overline{H}_X} \setminus \mathcal{C}_{\overline{H}_Z} \subseteq \mathcal{C}^{\perp}_{\overline{H}_X} \setminus \mathcal{C}_{G_Z}, \tag{3.12}$$

which implies a sequence of inequalities for the three related codes:

$$d_Z(G_X, H_Z) \geq d_Z(\overline{H}_X, \overline{H}_Z) \geq d_Z(H_X, G_Z), \tag{3.13}$$

where, e.g., $d_Z(G_X, H_Z)$ is the Z-distance in the code $\mathrm{CSS}(G_X, H_Z)$.

On the other hand, from linear relations between the rows of matrices involved, Lemma 3 and Theorem 4, it follows that all of the three codes in Eq. (3.12) are gauge-fixed versions of the subsystem code with the generators (3.1). They share the logical generator matrices (3.3), which implies a common upper bound $d_Z \leq d_Z^A d_Z^B$; the proof is similar to that in Statement 4. We get

$$d_Z(G_X, G_Z) = d_Z(H_X, G_Z) \leq d_Z^A d_Z^B, \tag{3.14}$$

$$d_Z(G_X, H_Z) = d_Z(\overline{H}_X, \overline{H}_Z) = d_Z^A d_Z^B. \tag{3.15}$$

Unfortunately, we are not able to get the exact values for the Z-distances in the l.h.s. of Eq. (3.14). It is clear that the general upper bound (3.14) is sharp. In particular, the upper bound is saturated whenever one of the codes has distance one. This follows from the following two lower bounds which we adapted from Ref. [42].

Statement 5 (Lower distance bound I) *Consider an F-linear code $\mathrm{CSS}(H_X, G_Z)$ with stabilizer generator matrices H_X and G_Z given by Eqs. (3.4) and (3.1), respectively. (a) The corresponding Z-distance satisfies the inequality*

$$d_Z(H_X, G_Z) \geq \max(d_Z^A, d_Z^B). \tag{3.16}$$

(b) In addition, assume that $d_Z^A > 1$. Then, with $F = \mathbb{F}_q$,

$$d_Z(H_X, G_Z) \geq \frac{q}{q-1}\, d_Z^B. \tag{3.17}$$

The proof is based on the following Lemma from Ref. [42]:

Lemma 6 (Lower distance bound II) *Consider an F-linear stabilizer code $\mathcal{Q} = \mathrm{CSS}(H_X, G_Z)$ with generator matrices H_X and G_Z in Eqs. (3.4) and (3.1), respectively. Given $a \in \mathcal{Q}_A^X$, consider a set $\Omega_A(a) = \{x_1, x_2, \ldots, x_N\}$ of vectors degenerate with a with respect to $\mathcal{C}_{H_X^A}$, such that each $i \in \{1, 2, \ldots, n_A\}$ is in the support of no more than K of these vectors. Then, for any Z-like codeword $c \in \mathcal{Q}^Z$ such that $[a \otimes I(n_B)]\, c^T \neq 0$,*

$$\mathrm{wgt}(c) \geq \left\lceil \frac{N}{K}\, d_Z^B \right\rceil . \tag{3.18}$$

Proof. Given c in Eq. (3.18), consider an expansion

$$c = \sum_{j=1}^{n_A} f_j \otimes b_j, \quad b_j \in F^{n_B},$$

where components of $f_j \in F^{n_A}$ are all zero except for $f_j[j] = 1$, $j \in \{1, \ldots, n_A\}$. By assumption, the dot-product $a_i \otimes I(n_B)$ with c is non-zero; for any $a_i \in \Omega_A(a)$,

$$x_i^T \equiv (a_i \otimes I_{n_B})\, c^T = \sum_j a_i[j]\, b_j^T .$$

It is easy to check that the resulting vector $x_i \in F^{n_B}$ satisfies $H_X^B x_i^T = 0$, while $L_X^B x_i^T \neq 0$. That is, x_i is in $\mathcal{Q}_B^Z$, so that $\mathrm{wgt}(x_i) \geq d_Z^B$. Let us now sum the weights of vectors x_i corresponding to all elements of $\Omega_A(a)$,

$$\begin{aligned} N d_Z^B \leq \sum_{i=1}^{N} \mathrm{wgt}(x_i) &\leq \sum_{j=1}^{n_A} \sum_{i=1}^{N} \mathrm{wgt}(a_i[j]\, b_j^T) \\ &\leq K \sum_{j=1}^{n_A} \mathrm{wgt}(b_j) = K\, \mathrm{wgt}(c), \end{aligned}$$

which gives Eq. (3.18) since $\mathrm{wgt}(c)$ is an integer. ■

Proof of Statement 5. Both (a) and (b) are trivial if $k_A k_B = 0$; assume otherwise below. (a) The construction is symmetric with respect to constituent codes $\mathcal{Q}_A$

and $\mathcal{Q}_B$; without limiting generality assume $d_Z^B \geq d_Z^A$. Use the set $\Omega_A(a) = \{a\}$ in Lemma 6 with $N = K = 1$, which proves $d_Z(H_X, G_Z) \geq d_Z^B$. (b) The condition $d_Z^A > 1$ implies that any all-zero column in H_X^A (say, at position $i \leq n_A$) must be matched by a row (or a linear combination of rows) of H_Z^A with the only non-zero element at i. This guarantees that any X-like codeword a has no support at such position(s). For any $a \in \mathcal{Q}_X^A$, consider the set $\Omega \equiv \Omega_A(a)$ of size $N = q^{\operatorname{rank} H_A^X}$ which contains all vectors degenerate with a. For any $i \leq n_A$, the set of characters $\Omega[i] \equiv \{x[i] : \forall x \in \Omega_A(a)\}$ either contains all zeros, or contains equal numbers of all elements of F—this can be seen by considering a generating matrix with all except one row not supported on i. For such a set, $K = (q-1)q^{(\operatorname{rank} H_A^X - 1)}$, which proves Eq. (3.17). ■

Another application of Lemma 6 is demonstrated by the following

Example 7 *Let $\mathcal{Q}^A = \mathrm{CSS}(H_X^A, H_Z^A)$ be a single-qubit encoding (consta)cyclic CSS code with parameters $[[n_A, 1, (d_X^A, d_Z^A)]]$. Then, for any $\mathcal{Q}^B = \mathrm{CSS}(H_X^A, H_Z^A)$, the Z-distance of the product code $\mathrm{CSS}(H_X, G_Z)$ with stabilizer generator matrices (3.4) and (3.1) satisfies*

$$d_Z(H_X, G_Z) \geq \lceil n_A d_Z^B / d_X^A \rceil. \tag{3.19}$$

Proof. Use Lemma 6 with $\Omega_A(a)$ a set of size $N = n_A$ constructed by shifting an X-like minimum-weight codeword $a \in \mathcal{Q}_A^X$, $\mathrm{wgt}(a) = d_X^A$ by 0, 1, ..., $n_A - 1$ positions. The resulting vectors $x_i \in \Omega_A(a)$ cannot be linear combinations of rows H_X^A, or else the original vector a would be too, thus they must be in the code. Since $k_A = 1$, they must be degenerate with a. The lower bound (3.19) is obtained if we notice that for this set, $K = d_X^A$. ■

The discussed lower distance bounds are pretty far from the generic upper bound (3.14). On the other hand, at least in the binary case, it is not easy to construct an

example of a subsystem product code with the distance strictly below the upper bound. Discovering such examples is dramatically simplified with the help of the ansatz in the following Theorem 8, a generalization of the construction based on the homological product of Steane's $[[7,1,3]]$ code with itself[40, 42] (see Example 11 below)

Theorem 8 (X–Z-symmetric product codes) *Consider codes $\mathcal{Q}_A = \mathrm{CSS}(H_X^A, H_Z^A)$ and $\mathcal{Q}_B = \mathrm{CSS}(H_Z^A, H_X^A)$ with X and Z generator matrices interchanged. The distances of the corresponding subsystem product code $\mathrm{CSS}(G_X, G_Z)$ with generators (3.1) satisfy*

$$d_X(G_X, G_Z) \leq n_A, \quad d_Z(G_X, G_Z) \leq n_A. \tag{3.20}$$

The inequality (3.14) becomes strict if $n_A < d_Z^A d_Z^B \equiv d_Z^A d_X^A$.

Proof. The construction is symmetric with respect to X and Z parts of $\mathcal{Q}_A$; it is sufficient to prove the bound for $d_Z \equiv d_Z(G_X, G_Z) = d_Z(H_X, G_Z)$ with H_X in Eq. (3.4). We have $n_A = n_B$; consider a vector $c = \sum_{j=1}^{n_A} e_j \otimes e_j$ of weight n_A, where e_j are weight-one vectors as in Eq. (3.10). Using Eq. (3.2) and the orthogonality between the rows of remaining X and Z generator matrices, verify that $H_X c^T = 0$ while $L_X c^T \neq 0$. Thus, c is a valid Z-like codeword in $\mathrm{CSS}(H_X, G_Z)$ and $d_Z \leq n_A$. ■

It is known that long CSS codes with distances scaling linearly with the code length n exist[51]. For a pair of such codes, the generic upper bound (3.14) has asymptotic scaling $d \leq \mathcal{O}(n_A n_B)$, linear in the length of the product code. On the other hand, the upper bound for the corresponding X–Z-symmetric product codes, see Theorem 8, gives $d \leq n_A$, a square root of the length of the product code. Thus, we can not expect the generic upper bound to be saturated. The following explicit Examples demonstrate that such a saturation does not happen for any finite field F.

Example 9 *For any field $F = \mathbb{F}_q$ with $q \equiv 2t+1$ odd, consider a $[[3,1,(2,2)]]_q$ code with CSS generators $H_X = (1,1,1)$, $H_Z = (t,t,1)$. The corresponding X–Z-symmetric product code in Theorem 8 has distances $d_X = d_Z = 3$, smaller than the upper bound (3.14). For $q = 3$, this saturates the lower bound (3.17).*

Example 10 *For any $q = 2^m$ with m even, so that $r \equiv (q-1)/3$ be an integer, consider a stabilizer code $[[3,1,(2,2)]]_q$ with cyclic H_X^A and constacyclic H_Z^B generators,*

$$H_X^A = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}, \quad H_Z^A = \begin{pmatrix} 1 & x^r & x^{2r} \end{pmatrix}, \tag{3.21}$$

where $x \in \mathbb{F}_q$ is a primitive element, i.e., $x^{q-1} = 1$. Construct an X–Z-symmetric product code as in Theorem 8. Combining Eq. (3.20) with the lower bound (3.19) again gives $d_Z(G_X, G_Z) = 3$, smaller than $d_Z^A d_Z^B = d_Z^A d_X^A = 4$.

Example 11 (Square of Steane's code[40, 42]) *For any $q = 2^m$, $m \in \mathbb{N}$, consider a pair of identical cyclic codes $[[7,1,(3,3)]]_q$ with stabilizer generator polynomials $h_X^A(x) = h_Z^B(x) = 1 + x^2 + x^3 + x^4$. Combination of the X–Z symmetric product construction from Theorem 8 and the lower bound (3.19) gives $d_Z(G_X, G_Z) = 7$, smaller than $d_Z^A d_Z^B = 9$.*

3.3 Previously known constructions

In the remainder of this Section, we discuss several existing code families which can be described as special cases of the subsystem product code construction in Lemma 3, or as gauge-fixed versions of such codes.

The first such family, homological product codes from Refs. [40, 42], is based on square nilpotent matrices such that $\delta^2 = 0$, with elements from a field $F = \mathbb{F}_q$ with $q = 2^m$,

$m \in \mathbb{N}$. Such a matrix δ and its transposed δ^T can be used to construct the stabilizer code $\mathrm{CSS}(\delta, \delta^T)$ and its symmetric $\mathrm{CSS}(\delta^T, \delta)$. Alternatively, stabilizer generators of a CSS code with $\operatorname{rank} H_X = \operatorname{rank} H_Z$ can be used to form such a nilpotent matrix, $\delta = H_X^T M H_Z$, where M is a matrix of appropriate dimensions chosen to preserve the rank of the product.

Example 12 (Homological product codes) *For $q = 2^m$, $m \in \mathbb{N}$, consider a pair of F-linear stabilizer codes $\mathcal{Q}^\mu = \mathrm{CSS}(\delta_\mu, \delta_\mu^T)$ with parameters $[[n_\mu, k_\mu, (d_X^\mu, d_Z^\mu)]]_q$ based on nilpotent matrices δ_μ, where $\mu \in \{A, B\}$. Then the matrix $\delta_C = I(n_A) \otimes \delta_B + \delta_A \otimes I(n_B)$ is also nilpotent. The corresponding code $\mathrm{CSS}(\delta_C, \delta_C^T)$ has logical generator matrices given by Eq. (3.1), and parameters $[[n_A n_B, k_A k_B, (d_X^C, d_Z^C)]]_q$, where, e.g.,*

$$d_Z(G_X, G_Z) \leq d_Z^C \leq d_Z^A d_Z^B. \tag{3.22}$$

Proof. It is easy to check that the logical generator matrices are given by Eq. (3.3); the upper bound on the distance follows. On the other hand, rows of δ_C and δ_C^T, respectively, are linear combinations of the rows of G_X and G_Z, see Eq. (3.1). This implies that the stabilizer code defined by this matrix is a gauge-fixed version of the subsystem product code $\mathrm{CSS}(G_X, G_Z)$, which gives the lower bound. ■

As before, the upper distance bound is sharp, but it is not necessarily saturated. In particular, an example[40] can be constructed along the lines of Example 11, as a homological product code combining two Steane's codes with identical symmetric nilpotent matrices δ. Such a code has distance $d = 7$, while the the upper bound in Eq. (3.22) gives $d \leq 9$.

Our last example shows that subsystem product codes and the corresponding gauge-fixed codes from Lemma 3 can be seen as a generalization of subsystem hypergraph-

product codes and corresponding gauge-fixed codes recently constructed by Li and Yoder[85] which are, in turn, a generalization of Bacon-Shor[84] and Shor's[86] codes, respectively. The Li–Yoder construction is based on a pair of classical codes, it is similar but not identical to those in Refs. [87, 88]. Namely, the gauge and stabilizer generator matrices can be obtained from Eqs. (3.1) and (3.4) by considering the classical codes as degenerate quantum codes with empty H_Z^A and H_X^B matrices.

Example 13 (Subsystem QHP codes[85]) *Given a pair of F-linear classical codes with parameters $[n_\mu, k_\mu, d_\mu]_q$, parity check matrices P_μ, and generator matrices Q_μ, where $\mu \in \{A, B\}$, consider a subsystem code $\mathrm{CSS}(G_X, G_Z)$ with gauge generator matrices*

$$G_X = (P_A \otimes I_{n_B}), \quad G_Z = (I_{n_A} \otimes P_B). \tag{3.23}$$

The corresponding stabilizer generator matrices are

$$H_X = (P_A \otimes Q_B)\,, \quad H_Z = (Q_A \otimes P_B)\,. \tag{3.24}$$

Assuming $k_A k_B > 0$, the parameters of the subsystem and both gauge-fixed codes are $[[n_A n_B, k_A k_B, (d_A, d_B)]]_q$.

The parameters of the codes follow from Theorem (4) where we should use $d_X^A = d_Z^B = 1$. In particular, we get the original Bacon-Shor (BS) and Shor's codes if we take repetition codes for both classical codes.

We also notice that a subsystem product code constructed from a BS code and a repetition code coincides with the 3-dimensional BS code as proposed by Napp and Preskill[89] (this construction differs from the 3D code originally suggested by Bacon[84]). Napp & Preskill construction can be seen as a three-fold subsytem product of repetition

codes, and can be generalized to higher dimensions. However, it is easy to check that these single-qubit encoding codes are just rearrangements of conventional BS codes from a 2D lattice to higher dimensions. The only differences are the measurement redundancy and local connectivity of neighboring qubits, as defined by the specific sets of gauge generators used in the construction.

Chapter 4

Homological distances in tensor products of chain complexes

Example 13 may serve as a nice introduction to the subject of this chapter. Indeed, Bacon-Shor code can be obtained from Kitaev's toric code by erasing qubits on all vertical (or all horizontal) bonds. The latter code corresponds exactly to a CW-complex associated with a square lattice with periodic boundary conditions—a tensor product of two cycle graphs. More general gauge generator matrices (3.23) can be seen as a result of erasing one of the blocks in a QHP code[35, 36] with stabilizer generator matrices

$$\begin{aligned} H_X &= (P_A \otimes I_{n_B} | I_B \otimes P_B^T), \\ H_Z &= (I_{n_A} \otimes P_B | - P_A^T \otimes I_A), \end{aligned} \tag{4.1}$$

where the dimensions of the identity matrices I_A and I_B match the numbers of rows in the two check matrices. The matrices H_X and H_Z^T correspond exactly to the boundary operator matrices in a product of the chain complexes $\mathcal{K}(P_A)$ and $\mathcal{K}(P_B^T)$. In this section we consider

tensor products of general bounded F-linear chain complexes. The corresponding boundary operators, see Eq. (4.8) below, have row- and column-blocks with the structure of the gauge generator matrices (3.1).

4.1 Main results for F-linear chain complexes

Our main result is the expression for the homological distance in a tensor product of two bounded chain complexes of finite-dimensional vector spaces over a finite field F, where one of the complexes contains just two non-trivial spaces. Specifically, let $\mathcal{A}$ be such a complex of any length specified in terms of boundary operators $\partial_j : \mathcal{A}_{j-1} \leftarrow \mathcal{A}_j$ defined explicitly as matrices, $\partial_j = A_j$ such that $A_j A_{j+1} = 0$, and $\mathcal{B}$ a complex with just two non-trivial spaces $\mathcal{B}_0$ and $\mathcal{B}_1$ and a single non-trivial boundary operator (matrix) $B_1 : \mathcal{B}_0 \leftarrow \mathcal{B}_1$ mapping between them. Then, the homological distance $d_j(\mathcal{C})$ for the j th homology group in the tensor product $\mathcal{C} = \mathcal{A} \times \mathcal{B}$ of the two complexes is

$$d_j(\mathcal{C}) = \min\big(d_j(\mathcal{A})d_0(\mathcal{B}), d_{j-1}(\mathcal{A})d_1(\mathcal{B})\big). \tag{4.2}$$

This is a generalization of the identical expression for the tensor product of binary chain complexes from Ref. [38].

There is actually a stronger statement which concerns the homological distance $d_j(\mathcal{C}_{i,j-i})$ after a projection onto a single subspace $\mathcal{C}_{i,j-i} = \mathcal{A}_i \otimes \mathcal{B}_{j-i}$, where $j - i \in \{0, 1\}$. Here, a chain complex with the space $\mathcal{C}_j$ reduced to its subspace has modified boundary operators ∂'_i and ∂'_{i+1}. The latter is defined as a composition of a projector P and the original boundary operator ∂_{i+1}, $\partial'_{i+1} \equiv P\partial_{i+1}$, where $P^2 = P$ and the image of P is the subspace of interest. The modified boundary operator ∂'_i is defined to ensure the composition to vanish,

$\partial'_i \partial'_{i+1} = 0$. For thus defined chain complex $\mathcal{C}'_{i,j-i}$ with the space $\mathcal{C}_j$ in the original product complex $\mathcal{C}$ projected to its subspace $\mathcal{C}_{i,j-i}$, the homological distance at level j is given by one term only,

$$d_j(\mathcal{C}'_{i,j-i}) = d_i(\mathcal{A}) d_{j-i}(\mathcal{B}), \quad j - i \in \{0, 1\}. \tag{4.3}$$

Our third result concerns with the minimal distance in a tensor product of two arbitrary-length chain complexes of vector spaces over a finite field F. Here the upper bound on the homological distance reads

$$d_j(\mathcal{C}) \leq \min_{i \in \mathbb{Z}} d_i(\mathcal{A}) d_{j-i}(\mathcal{B}). \tag{4.4}$$

A lower bound for the same distance $d_j(\mathcal{C})$ can be constructed by projecting onto the individual product spaces $\mathcal{A}_i \otimes \mathcal{B}_{j-i}$, $i \in \mathbb{Z}$, whose direct sum gives the degree-j space $\mathcal{C}_j$ in the product complex. This gives $d_j(\mathcal{C}) \geq \min_i d(\mathcal{C}'_{i,j-i})$. The result of the projection can be seen as an F-linear quantum subsystem code with CSS gauge generator matrices in the product form (3.1),

$$G_X = \begin{pmatrix} I(a_i) \otimes B_{j-i} \\ \\ A_i \otimes I(b_{j-i}) \end{pmatrix}, \; G_Z = \begin{pmatrix} I(a_i) \otimes B^T_{j-i+1} \\ \\ A^T_{i+1} \otimes I(b_{j-i}) \end{pmatrix}, \tag{4.5}$$

where $I(a) \equiv I_a$ is the size-a identity matrix, and a_i and b_i, respectively, are the dimensions of the degree-i spaces in the chain complexes $\mathcal{A}$ and $\mathcal{B}$. Thus, the Z-distance of the subsystem code with CSS generators (4.5) may serve as a lower bound for $d_j(\mathcal{C})$, complimentary to Eq. (4.4).

Unfortunately, such a projection is not an ideal tool for finding the minimum distances in the product complex, as the distance may actually be reduced in some cases.

The examples of such a reduction are based on Theorem 8 in the previous Section; it may happen for any finite field.

However, this reduction only concerns the minimum distances in tensor products of chain complexes after projection to one of the subspaces, it does not prevent the inequality (4.4) from being saturated. We conducted extensive numerical calculations finding homological distances for products of random $\mathbb{F}_q$-linear chain complexes with $q \in \{2, 3, 2^2, 5, 7, 2^3, 3^2, 11\}$ and space dimensions of up to 12, and an exhaustive enumeration of products of binary chain complexes with individual spaces of dimension up to 7. Yet we haven't been able to find a single example of a pair of chain complexes whose product would fail to reach the upper bound (4.4). Combined with analytical results for multiple products of chain complexes involving just two spaces, we *conjecture* that in general, for any finite field $F = \mathbb{F}_q$, the homological distances in a tensor product of a pair of bounded chain complexes of vector spaces over F satisfy the equality

$$d_j(\mathcal{A} \times \mathcal{B}) = \min_{i \in \mathbb{Z}} d_i(\mathcal{A}) d_{j-i}(\mathcal{B}). \tag{4.6}$$

4.2 Upper bound on the distance

Statement 14 *Consider two F-linear chain complexes $\mathcal{A} = \mathcal{K}(A_1, \ldots, A_\ell)$ and $\mathcal{B} = \mathcal{K}(B_1, \ldots, B_{\ell'})$. Then, for any $i, j \in \mathbb{Z}$, the homological distance of the product complex $\mathcal{C} = \mathcal{A} \times \mathcal{B}$ at level j satisfies the inequality*

$$d_j(\mathcal{C}) \leq d_i(\mathcal{A}) d_{j-i}(\mathcal{B}). \tag{4.7}$$

Proof. By definition, the distances $d_i(\mathcal{A})$ and $d_{j-i}(\mathcal{B})$ are natural or infinite. Thus, if one or both homology groups are trivial, $k_i(\mathcal{A}) = 0$ or $k_{j-i}(\mathcal{B}) = 0$ (in which case the corresponding distance is infinite), the r.h.s. of Eq. (4.7) equals infinity, so that the inequality in question is trivially satisfied.

Otherwise, with both homology groups non-trivial, consider a pair of minimum-weight homologically non-trivial vectors $a \in \mathcal{H}_i(\mathcal{A})$ and $b \in \mathcal{H}_j(\mathcal{B})$ such that $\mathrm{wgt}(a) = d_i(\mathcal{A})$ and $\mathrm{wgt}(b) = d_j(\mathcal{B})$. Vector a is a non-trivial Z-like codeword in the stabilizer code $\mathrm{CSS}(A_i, A_{i+1}^T)$; denote a' an X-like codeword in the same code conjugate to a, that is, $a' \cdot a = 1$. In other words, this vector is a co-cycle in $\tilde{\mathcal{A}}_i$. [In fact, a' is a member of the co-homology group $H_i(\tilde{\mathcal{A}})$, but this is not needed for the proof.] Similarly, denote b' an X-like codeword in the code $\mathrm{CSS}(B_{j-i}, B_{j-i+1}^T)$ conjugate to b, a co-cycle in $\tilde{\mathcal{B}}_j$. Construct $c \in \mathcal{C}_j$ by assigning non-zero value $c_{i,j-i} = a \otimes b$ in the subspace $\mathcal{A}_i \otimes \mathcal{B}_{j-i}$, and zero in all other subspaces at level j. Clearly, $\mathrm{wgt}(c) = d_i(\mathcal{A}) d_{j-i}(\mathcal{B})$; to prove the upper bound (4.7) we just need to show that $c \not\simeq 0$. To this end, consider a vector c' constructed similarly to c but from vectors a' and b'; it is easy to check that $c \cdot c' = 1$. In addition, this vector is a co-cycle in $\tilde{\mathcal{C}}_j$, i.e., $c' C_{j+1} = 0$, where the matrix is a boundary operator in the product complex $\mathcal{C}$, cf. Eq. (2.22). Any vector equivalent to c has the form $c + x(C_{j+1})^T$, for some $x \in \mathcal{C}_{j+1}$. However, such a combination is never zero, as can be verified by taking a dot product with c'. ■

The upper bound (4.4) immediately follows from Statement 14 by minimizing over i.

4.3 Lower bounds on the distance

To make the map with the product codes in Sec. 3 evident, we start by writing out the block form of a matrix in the product complex $\mathcal{C} = \mathcal{A} \otimes \mathcal{B}$, where the spaces $\mathcal{A}_i$ and $\mathcal{B}_j$ have dimensions a_i and b_j, respectively:

$$C_j = \left(\begin{array}{c|c|c|c|c} A_j \otimes I(b_0) & (-1)^{j-1} I(a_{j-1}) \otimes B_1 & & & \\ \hline & A_{j-1} \otimes I(b_1) & (-1)^{j-2} I(a_{j-2}) \otimes B_2 & & \\ \hline & & \ddots & \ddots & \\ \hline & & & A_1 \otimes I(b_{j-1}) & I(a_0) \otimes B_j \end{array}\right). \tag{4.8}$$

For ease of mapping of the homology group $H_j(\mathcal{C})$ to the CSS stabilizer code with generators $H_X = C_j$ and $H_Z = C_{j+1}^T$, we also write the latter matrix explicitly

$$C_{j+1}^T = \left(\begin{array}{c|c|c|c|c} A_{j+1}^T \otimes I(b_0) & & & & \\ \hline (-1)^j I(a_j) \otimes B_1^T & A_j^T \otimes I(b_1) & & & \\ \hline & (-1)^{j-1} I(a_{j-1}) \otimes B_2^T & A_{j-1}^T \otimes I(b_2) & & \\ \hline & & \ddots & \ddots & \\ \hline & & & -I(a_1) \otimes B_{j-1}^T & A_1^T \otimes I(b_j) \\ \hline & & & & I(a_0) \otimes B_{j+1}^T \end{array}\right). \tag{4.9}$$

Clearly, in general, the generator matrices $H_X = C_j$ and $H_Z = C_{j+1}^T$ have $j+1$ column blocks, with each block row and block column incident on no more than two non-zero blocks. Our strategy is to construct bounds on the distance of these codes using Lemmas 1 and 2.

First, let us construct the codes $\mathcal{Q}^{(i,j-i)}$, $i \in \mathbb{Z}$, each projected into a single subspace $\mathcal{A}_i \otimes \mathcal{B}_{j-i}$ as in Lemma 1. The corresponding lower bound on the homological distance at the level j of the product complex $\mathcal{C}$ reads

$$d_j(\mathcal{C}) \geq \min_{i \in \mathbb{Z}} d_Z\left(\mathcal{Q}^{(i,j-i)}\right). \tag{4.10}$$

Denote $I \equiv I_i^j$ the index set corresponding to the subspace $\mathcal{A}_i \otimes \mathcal{B}_{j-i}$ in $\mathcal{C}_j$. The punctured matrix $G_Z[I]$ is obtained by selecting the appropriate column block in the matrix (4.9). When expressed in terms of the two small stabilizer codes $\mathcal{Q}_A = \mathrm{CSS}(A_i, A_{i+1}^T)$ and $\mathcal{Q}_B = \mathrm{CSS}(B_{j-i}, B_{j-i+1}^T)$ associated with the homology groups $H_i(\mathcal{A})$ and $H_{j-i}(\mathcal{B})$, respectively, the resulting matrix has exactly the form of the gauge generator matrix G_Z in Eq. (3.1). To construct the matching shortened matrix $(H_X)_I$, notice that only two row blocks in C_j give non-zero contribution,

$$C_j[I_{i+1}^j \cup I_i^j \cup I_{i-1}^j]$$

$$= \left(\begin{array}{c|c|c} (-1)^{i+1} I(a_{i+1}) \otimes B_{j-i-1} & & \\ \hline A_{i+1} \otimes I(b_{j-i-1}) & (-1)^i I(a_i) \otimes B_{j-i} & \\ \hline & A_i \otimes I(b_{j-i}) & (-1)^{i-1} I(a_{i-1}) \otimes B_{j-i+1} \\ \hline & & A_{i-1} \otimes I(b_{j-i+1}) \end{array}\right).$$

The shortening to the middle column block, I_i^j, is achieved with the help of row operations equivalent to left multiplication of the second row block by $A^* \otimes I(b_{j-i-1})$ and of the third row block by $I(a_{i-1}) \otimes B^*$, where

$$A^* = \begin{pmatrix} A_i \\ \\ L_X^A \end{pmatrix}, \quad B^* = \begin{pmatrix} B_{j-i} \\ \\ L_X^B \end{pmatrix} \tag{4.11}$$

are the largest-rank matrices with rows orthogonal to the columns of A_{j+1} and B_{j-i+1}, respectively. Here and below, we denote L_X^A, L_Z^A and L_X^B, L_Z^B the canonical logical generator matrices (2.15) of the same stabilizer codes, $\mathcal{Q}_A$ and $\mathcal{Q}_B$. As a result of the multiplication, we obtain the shortened matrix $(H_X)_I$ in the exact form of the stabilizer generator matrix H_X in Eq. (3.4), again, when expressed in terms of the matrices associated with the codes

$\mathcal{Q}_A$ and $\mathcal{Q}_B$. According to Lemma 3, the corresponding stabilizer code CSS $\big((H_X)_I, H_Z[I]\big)$ has exactly the same Z-distance as the subsystem code CSS $\big(H_X[I], H_Z[I]\big)$ obtained by puncturing both matrices $H_X = C_j$ and $H_Z = C_{j+1}^T$ to the single subspace $\mathcal{A}_i \otimes \mathcal{B}_{j-i}$.

With the help of the upper bound (3.14) and the loose lower bound (3.16), we obtain

Statement 15 *The Z-distance $d_Z \equiv d_Z(\mathcal{Q}^{(i,j-i)})$ of the F-linear CSS code $\mathcal{Q}^{(i,j-i)}$ obtained by Z-puncturing the CSS code corresponding to homology group $H_j(\mathcal{A} \otimes \mathcal{B})$ to the subspace $\mathcal{A}_i \otimes \mathcal{B}_{j-i}$ satisfies the bounds*

$$\max\big(d_i(\mathcal{A}), d_{j-i}(\mathcal{B})\big) \leq d_Z \leq d_i(\mathcal{A}) d_{j-i}(\mathcal{B}). \tag{4.12}$$

Since $d_0(\mathcal{A})$ and $d_0(\mathcal{B})$ are restricted to be either zero or infinity, this gives exact values for the distance in two special cases:

$$d_Z(\mathcal{Q}^{(j,0)}) = d_j(\mathcal{A}) d_0(\mathcal{B}), \tag{4.13}$$

$$d_Z(\mathcal{Q}^{(0,j)}) = d_0(\mathcal{A}) d_j(\mathcal{B}). \tag{4.14}$$

In addition, the structure of the homologically non-trivial vectors is somewhat clarified by the following restricted result:

Statement 16 *Consider a vector $c \in \mathcal{C}_j$ at level j in the product chain complex $\mathcal{C} = \mathcal{A} \times \mathcal{B}$, and assume that for some $i \leq j$, c has a non-zero weight in $H_i(\mathcal{A}) \otimes H_{j-i}(\mathcal{B})$, while the components of c are zero in spaces $\mathcal{A}_{i'} \otimes \mathcal{B}_{j-i'}$ with $i' < i$. Then* $\mathrm{wgt}(c) \geq d_i(\mathcal{A}) d_{j-i}(\mathcal{B})$.

Proof. The vector is a Z-like codeword in the CSS code with generator matrices (4.8) and (4.9). The condition can be used to construct a Z-shortened code, with all blocks to the

right of the block $\mathcal{A}_i \otimes \mathcal{B}_{j-i}$ removed as in Lemma 2. This amounts to dropping all column blocks of C_j and C_{j+1}^T to the right of the $(j-i+1)$ th block-column which corresponds to the subspace $\mathcal{A}_i \otimes \mathcal{B}_{j-i}$, and multiplication of the last block-row that remains non-zero in C_{j+1}^T by $(A^*)^T \otimes I(b_{j-i})$, where A^* is given by Eq. (4.11). After a subsequent application of a Z-puncture, so that all block columns to the left of the block $\mathcal{A}_i \otimes \mathcal{B}_{j-i}$ are removed as in Lemma 1, we obtain exactly the concatenated-stabilizer code in Theorem 4, constructed from $\mathcal{Q}_A = \mathrm{CSS}(A_i, A_{i+1}^T)$ and $\mathcal{Q}_B = \mathrm{CSS}(B_{j-i}, B_{j-i+1}^T)$. The Z-distance of this code is $d_Z = d_Z^A d_Z^B = d_i(\mathcal{A}) d_{j-i}(\mathcal{B})$. Moreover, by assumption, vector c punctured to the space $\mathcal{A}_i \otimes \mathcal{B}_{j-i}$ is non-trivial in the product code, which guarantees $\mathrm{wgt}(c) \geq d_Z$. ■

Clearly, the same lower bound also applies for vectors with zero weight in all spaces $\mathcal{A}_{i'} \otimes \mathcal{B}_{j-i'}$ with $i' > j$. In addition, the condition of Statement 16 is automatically satisfied when B_{j-i} is the last non-trivial matrix in the complex $\mathcal{B}$, i.e., $j - i = \ell'$, see Statement 14. In this case, again, the upper bound in Eq. (4.12) is saturated, $d_Z(\mathcal{Q}^{(i,\ell')}) = d_i(\mathcal{A}) d_{\ell'}(\mathcal{B})$. The same is true also when A_i is the last non-trivial boundary operator in the complex $\mathcal{A}$, $i = \ell$; we have $d_Z(\mathcal{Q}^{(\ell,j)}) = d_\ell(\mathcal{A}) d_j(\mathcal{B})$.

The special cases in Statements 15 and 16 combine to give exact distances in the case where one of the complexes in the product contains just one non-trivial boundary operator. This gives an extension of the main result in Ref. [38] to F-linear chain complexes:

Theorem 17 *Consider a tensor product $\mathcal{C} = \mathcal{A} \times \mathcal{B}$ of two F-linear chain complexes, where one of the complexes contains just two non-trivial spaces, e.g., $\mathcal{A} = \mathcal{K}(A_1, \ldots, A_\ell)$ and $\mathcal{B} = \mathcal{K}(B_1)$. Then, for any $j \in \mathbb{Z}$, the homological distance at level j of the product*

complex $\mathcal{C} = \mathcal{A} \times \mathcal{B}$ *is*

$$d_j(\mathcal{C}) = \min_{i \in \mathbb{Z}} d_i(\mathcal{A}) d_{j-i}(\mathcal{B}). \tag{4.15}$$

In Ref. [38], we conjectured that in the binary case, $q = 2$, the identity (4.15) be applicable to products of arbitrary bounded complexes. The conjecture was based on extensive numerical simulations of products of length-three binary complexes corresponding to pairs of randomly-generated CSS codes.

In addition, here we have conducted numerical simulations of product chain complexes based on pairs of random $\mathbb{F}_q$-linear stabilizer codes, with all CSS generators of full-row-rank, so that in the corresponding chain complexes only the homology groups $H_1(\mathcal{A})$ and $H_1(\mathcal{B})$ be non-trivial. For each $q \in \{2, 3, 2^2, 5, 7, 2^3, 3^2, 11\}$, we generated some 2×10^4 such code pairs of length $3 \leq a_1 \leq b_1 \leq 11$, and calculated the homological distances $d_2(\mathcal{C})$ and $d_2(\tilde{\mathcal{C}})$ of the corresponding (co)chain product complexes using a version of the covering set algorithm[90, 91, 92]. Not a single instance was found where the inequality (4.7) would not be saturated.

Notice that our search went over a tiny fraction of all code pairs, in particular, since the number of codes (matrices) scales exponentially with the number of entries, i.e., super-exponentially with the matrix size. To ensure that we did not miss any instances, we also enumerated all pairs of non-trivial binary CSS codes of size $n \leq 7$, and constructed tensor products of the corresponding chain complexes. Eq. 4.15 was satisfied for all of these.

Based on these numerical results, combined with the analytical result in Theorem 17 and the results for multiple products of 1-complexes, see Sec. 4.4, we propose

Conjecture 18 *The homological distances $d_j(\mathcal{A} \times \mathcal{B})$ in a product of any pair of bounded chain complexes of vector spaces over a finite field is given by Eq. (4.15).*

Of course, one should be aware that, even when highly suggestive, numerical evidence cannot substitute a proof. A recent example is the Hedetniemi conjecture about the chromatic number in a tensor product of graphs[93, 94]. The conjecture held up for over half a century; a counterexample was only recently discovered by Yaroslav Shitov in a beautiful 2019 paper[95, 96]. Significantly, the smallest graphs known so far to provide a counterexample to Hedetniemi's conjecture have over 10^4 vertices[97].

4.4 Applications in quantum error correction

In classical error correction it is usually safe to assume a channel model, where errors may happen during transmission but not during encoding/decoding. In comparison, when a quantum error-correcting code (QECC) is used, errors may happen at any step; to measure a syndrome one has to perform a complex set of elementary quantum unitaries, gates, which may result not only in additional data errors but also syndrome measurement errors. Measurement errors become more likely with operators of large weight, as the measurement circuit has to be constructed from elementary quantum gates which typically can operate at most on two qudits at a time.

As a result, FT operation requires quantum codes where all (or most) stabilizer generators have small weights. These are analogous to classical LDPC codes.

Here we consider tensor products of several F-linear 1-complexes, chain complexes with just two non-trivial spaces. Basic parameters such as space dimensions, row and

column weights, or homological distances do not depend on the order of the terms in the product. Further, if the matrices used to construct 1-complexes are (υ, ω)-sparse, that is, their column and row weights do not exceed υ and ω, respectively, the matrices in the resulting m-chain product complex are $(m\upsilon, m\omega)$-sparse. In particular, when $\mathcal{K} = \mathcal{K}(R)$ is a 1-complex associated with a circulant check matrix of the repetition code, $\mathcal{K}^{\times D}$ recovers all the D-dimensional toric codes.

First, consider an $r \times c$ full-row-rank q-ary matrix P with $r < c$, and assume that the F-linear code $\mathcal{C}_P^{\perp}$ has distance δ. The 1-complex $\mathcal{K} \equiv \mathcal{K}(P)$ has two non-trivial spaces of dimensions r and c; the corresponding homology groups have ranks 0, κ and the distances ∞, δ. The 1-complex $\tilde{K} \equiv \mathcal{K}(P^T)$ generated by the transposed matrix has equivalent spaces taken in the opposite order, with the same homology group ranks, but the distances are now 1 and ∞, respectively. It is easy to see that in any chain complex constructed as tensor products of $\mathcal{K}$ and/or $\tilde{\mathcal{K}}$, there is going to be only one homology group with a non-zero rank. Since order of the products is not important, we will write these as powers. For $(a+b)$-complex $\mathcal{K}^{(a,b)} \equiv \mathcal{K}^{\times a} \times \tilde{\mathcal{K}}^{\times b}$, the only non-trivial homology group is $H_a(\mathcal{K}^{(a,b)})$, acting in the space of dimension

$$n_a(\mathcal{K}^{(a,b)}) = \sum_{i=0}^{a} c^{2i} r^{a+b-2i} \binom{a}{i} \binom{b}{i} < (r+c)^{a+b},$$

it has rank κ^{a+b} and distance δ^a. The corresponding quantum CSS code has the minimum distance $\min(\delta^a, \delta^b)$, and its stabilizer generators have weights not exceeding $(a + b)\max(\upsilon, \omega)$.

Good weight-limited classical LDPC codes with asymptotically finite rates κ/c and finite relative distances δ/c can be obtained from ensembles of large random matrices[26,

27, 28, 29, 98, 99]. Any of these can be used in the present construction. Then, for any pair (a, b) of natural numbers, we can generate weight-limited quantum LDPC codes with finite rates and the distances $d_X = \delta^a$, $d_Z = \delta^b$ whose product scales linearly with the code length. The quantum hypergraph-product codes are a special case of this construction with $a = b = 1$.

More generally, take arbitrary $r_i \times c_i$ matrices P_i, $i = 1, 2, \ldots$ with elements from $F \equiv \mathbb{F}_q$. Let F-linear codes with parity check matrices P_i and P_i^T, respectively, have parameters $[c_i, \kappa_i, \delta_i]$ and $[r_i, \tilde{\kappa}_i, \tilde{\delta}_i]$, where the distance is assumed infinite whenever the corresponding code is trivial, $\kappa = 0$. Then, for a product of m such 1-complexes, the space dimensions and ranks of the homology groups following from the Künneth formula can be written in terms of the generating polynomials

$$\begin{aligned} n^{(m)}(x) &\equiv n_0^{(m)} + x n_1^{(m)} + \ldots x^m n_m^{(m)} \\ &= \prod_{j=1}^{m} (r_j + x c_j), \\ k^{(m)}(x) &\equiv k_0^{(m)} + x k_1^{(m)} + \ldots x^m k_m^{(m)} \\ &= \prod_{j=1}^{m} (\tilde{\kappa}_j + x \kappa_j). \end{aligned}$$

The homological distance $d_j^{(m)}$ can be seen as the minimum over the products of distances corresponding to those terms that give non-zero contributions to $k_j^{(m)}$, with the substitution $\kappa_j \to \delta_j$, $0 \neq \tilde{\kappa}_j \to 1$.

It is easy to check that none of the higher-dimensional quantum hypergraph-product codes discussed here have parameters that are better than for regular QHP codes ($m = 2$) originally constructed by Tillich and Zémor[35]. In addition, the row- and column-weights of the corresponding matrices tend to get bigger with increasing m. The advantage

of higher-dimension QHP codes, or, more generally, codes from m-chain complexes with $m \geq 4$, is that the rows of matrices $G_X^{(a)} = \mathcal{K}_a$, $G_Z^{(a)} = \mathcal{K}_{a+1}^T$ satisfy a large number of linear relations resulting from the orthogonality with the matrices K_{a-1} and K_{a+2}, respectively. These can be used to correct syndrome measurement errors. Even though the resulting syndrome codes do not have large distances (with a finite probability some errors remain), the use of such codes in repeated measurement setting could simplify the decoding and/or improve the decoding success probability in the case of adversarial noise[61]. Such improvements with stochastic noise have been demonstrated numerically in the case of $D = 4$ toric codes in Ref. [100].

4.5 Extensions

Throughout this work, we concentrated on the Hamming distance. A simple, and yet offering a range of possible applications, extension of Theorem 4, Statement 14, and Theorem 17 can be given by using *weighted distances*, defined for a vector $c \in F^n$ in terms of the norm

$$\underset{W}{\mathrm{wgt}}(c) \equiv \sum_{i:c[i]\neq 0} W_i, \tag{4.16}$$

where $W \equiv (W_1, W_2, \ldots, W_n)$ is a vector of positive weights $W_i > 0$, $i \leq n$. For the corresponding proofs to work, the only requirement is that the weights $W^{C_{i,j}}$ in each space $\mathcal{C}_{ij} \equiv \mathcal{A}_i \otimes \mathcal{B}_j$ used to form the product complex $\mathcal{C} = \mathcal{A} \times \mathcal{B}$ be related to the weights W^{A_i} and W^{B_j} in the original complexes, namely, $W^{C_{i,j}} = W^{A_i} \otimes W^{B_j}$. Indeed, all the proofs are based either on Eq. (3.3), or a projection inequality as in Eq. (3.11); both arguments are readily modified to account for weighted norm (4.16).

In particular, this implies an extension to extremal length L_1 (systole) and higher-dimensional analogs L_j, $j > 1$, representing minimal structures with non-trivial homology on a given manifold(see e.g. [101]). Indeed, in the simplest case, the edge ($j = 1$), plaquette ($j = 2$), etc. weights associated with a given tessellation can be chosen as the corresponding Euclidean length, area, etc. Then the weighted norm (4.16) gives the corresponding measure of the elements in the structure, and the homological distance—the corresponding minimum, going over to L_j in the continuum limit. We assume the manifolds be sufficiently smooth so that the corresponding limits exist (see e.g. [102]).

Second, an extension of some of the bounds to chain complexes of K-modules, modules over a commuting ring K, is possible if K is a principal ideal domain (PID). Here we only consider the ring $K = \mathbb{Z}_q$ of modular integers, and assume torsion-free case, i.e., with all Smith normal form invariants of all matrices either zero or one. In this case one gets[103] $d_Z^C \geq d_Z^A d_Z^B$ for the stabilizer-product code in Theorem 4. Further, the lower bound in Theorem (5) remains intact, while Eq. (4.15) also becomes an inequality, $d_j(\mathcal{C}) \geq \min_{i\in\mathbb{Z}} d_i(\mathcal{A}) d_{j-i}(\mathcal{B})$.

Chapter 5

Alternative proof in the binary field

The previous chapter has demonstrated the distances in general field, when one of the chain complexes has length 2. The proof cannot be extended to the general cases with arbitrary chain complexes, due to existing counter examples. As another attempt to prove the distance for arbitrary chain complexes, this chapter gives an alternative proof for the distance in the special case with one of the chain complex has length 2 in the binary field. Though this one hasn't resulted in a general proof yet, it may give some hint on how to move farward.

5.1 Introduction

We start by introducing some notation of error correcting codes in the binary field. Meanwhile, one should assume all the chain complexes and codes in this chapter are in the binary field.

A classical binary linear code $\mathcal{C}$ with parameters $[n, k, d]$ is a k-dimensional subspace of the vector space $\mathbb{F}_2^n$ of all binary strings of length n. The code distance d is the minimal Hamming weight of a nonzero string in the code. A code $\mathcal{C} \equiv \mathcal{C}_G$ can be specified in terms of the generator matrix G whose rows are the basis vectors of the code. All vectors orthogonal to the rows of G form the dual code $\mathcal{C}_G^\perp = \{c \in \mathbb{F}_n^2 | Gc^T = 0\}$. The matrix G is also called the parity check matrix of the code $\mathcal{C}_G^\perp$.

Using the same proof in Chapter 4, one can get an upper bound on the distances of the homological groups in a chain complex $\mathcal{A} \times \mathcal{B}$, an immediate extension of Cor. 2.14 from Ref. [42],

$$d_j(\mathcal{C}) \leq \min_i d_i(\mathcal{A})\, d_{j-i}(\mathcal{B}). \tag{5.1}$$

5.2 Lower bound on the distance

Here I present an alternative proof for the lower bound on the distance for the special case where $\mathcal{B} = \mathcal{K}(P)$ is a 1-complex induced by an $r \times c$ binary matrix P. This bound matches the upper bound in Eq. (5.1), and thus ensures the equality for the case where $\mathcal{B}$ is a 1-complex. This expression,

$$d_j(\mathcal{A} \times \mathcal{B}) = \min\big(d_j(\mathcal{A})\, d_0(\mathcal{B}), d_{j-1}(\mathcal{A})\, d_1(\mathcal{B}), \big), \tag{5.2}$$

where $\mathcal{B} = \mathcal{K}(P)$ is a 1-complex, is our main result.

With $\mathcal{A}$ the m-complex in Eq. (2.16), the tensor product $\mathcal{C} \equiv \mathcal{A} \times \mathcal{B}$ can be written as an $(m+1)$-complex, $\mathcal{C} = \mathcal{K}(C_1, \ldots, C_{m+1})$, with the block matrices

$$C_{j+1} = \left(\begin{array}{c|c} A_{j+1} \otimes E_r & (-1)^j E_{n_j} \otimes P \\ \hline & A_j \otimes E_c \end{array} \right), \tag{5.3}$$

where E_r denotes the $r \times r$ identity matrix. The sign in the top-right corner ensures orthogonality $C_j C_{j+1} = 0$; in our case spaces are binary and signs have no effect. We also notice that since ∂_0 and ∂_{m+1} in $\mathcal{A}$ are both trivial, matrices C_1 and C_{m+1}, respectively, will be missing the lower and the left block pairs. If we denote $u \equiv \operatorname{rank} P$, the two homology groups associated with $\mathcal{B}$ have ranks $\kappa_0 \equiv k_0(\mathcal{B}) = r - u$ and $\kappa_1 \equiv k_1(\mathcal{B}) = c - u$, respectively. Equations (2.23) and (2.25) give in this case,

$$n'_j = n_j r + n_{j-1} c \quad \text{and} \quad k'_j = k_j \kappa_0 + k_{j-1} \kappa_1, \tag{5.4}$$

where we use the primes to denote the parameters of $\mathcal{C}$, $n'_j \equiv n_j(\mathcal{C})$ and $k'_j \equiv k_j(\mathcal{C})$. We now prove the claimed lower bound for the distance:

Theorem 19 *Consider m-complex $\mathcal{A}$ in Eq. (2.16), and assume that homological groups $H_j(\mathcal{A})$ have distances d_j, $0 \le j \le m$. Given an $r \times c$ binary matrix P of rank u, construct matrices C_j in Eq. (5.3). Denote δ the minimum distance of a binary code with the parity check matrix P; by our convention, $\delta = \infty$ if $u = c$. The minimum distance $d'_j \equiv d_j(\mathcal{C})$ of the homology group $H(C_j, C_{j+1})$, $0 \le j \le m+1$, satisfies the following lower bounds:*

(i) *if $r > u$, $d'_j \ge \min(d_j, d_{j-1}\delta)$, otherwise,*

(ii) *if $r = u$, $d'_j \ge d_{j-1}\delta$.*

We notice that in Eq. (13), $d_j(\mathcal{A}) \equiv d_j$, $d_1(\mathcal{B}) = \delta$, while $d_0(\mathcal{B}) = 1$ in case (i) and it is infinite in case (ii).

Given a matrix A_j and a subset I of its column indices, we consider a *punctured* matrix $A_j[I]$ formed only by the columns in I. Obviously, for any vector e such that $A_j e^T = 0$, as long as the support of e is included in I, we also have $A_j[I](e[I])^T = 0$.

Further, our chain complex $\mathcal{A}$ also has a boundary operator A_{j+1} such that $A_j A_{j+1} = 0$. In order to preserve the orthogonality when we puncture A_j to $A_j[I]$, we also need to modify A_{j+1}. It is clearly not sufficient to just take a subset I of its rows, as the orthogonality would not necessarily be preserved in this case. Instead, from all linear combinations of the columns of A_{j+1} we select those with the support in I. We call any basis of this linear subspace, with all-zero rows outside of I dropped, a *row-shortened matrix* A_{j+1} to I, denoted as $I(A_{j+1})$.

Explicitly, let D_I be a matrix such that $A_{j+1}D_I$ has all zero rows outside I, and any linear combination of the columns of A_{j+1} with the support in I can be constructed as a linear combination of columns of $A_{j+1}D_I$. Then $I(A_{j+1}) = (E[I])^T A_{j+1} D_I$ is formed by dropping the (all-zero) rows of $A_{j+1}D_I$ outside I (here $E \equiv E_{n_j}$ is the identity matrix in the space $\mathcal{A}_j$). In this case, if e has support in I, and $(e[I])^T = I(A_{j+1})\alpha^T$ is a linear combination of the rows of the row-shortened matrix, then $e^T = A_{j+1}D_I\alpha^T$ gives an explicit form of the corresponding linear combination of the rows of the original matrix A_{j+1}. This is correct since any vector in the form $A_{j+1}D_I\alpha^T$ has support limited to I.

Conversely, if e^T has support in I and is a linear combination of columns of A_{j+1}, by construction, $(e[I])^T$ is a linear combination of columns of $I(A_{j+1})$.

In the proof below we start with a pair of matrices C_j, C_{j+1}, and certain vector e such that $C_j e^T = 0$, and construct a sequence of transformations of the corresponding chain complex $\mathcal{C}$ which include punctures/row-shortenings and the equivalence transformations, to arrive at a chain complex $\mathcal{C}''$ with the boundary operators given by matrices C''_j, C''_{j+1}, and a vector e'' such that $C''_j (e'')^T = 0$, with the trivial homology group, $\operatorname{rank} H(C''_j, C''_{j+1}) = 0$. This implies e'' must be a linear combination of the columns of C''_{j+1}; unraveling the transformations proves the original vector e a linear combination of the columns of C_{j+1}.

Detailed Proof of Theorem 19. Start with case (i). Take a block vector $e = (e_1|e_2)$, with $e_1 \in \mathbb{F}_2^{n_j r}$, $e_2 \in \mathbb{F}_2^{n_{j-1} c}$, component weights $w_1 \equiv \operatorname{wgt}(e_1) < d_j$, $w_2 \equiv \operatorname{wgt}(e_2) < d_{j-1}\delta$, and assume $C_j e^T = 0$. We are going to show that e is a linear combination of columns of C_{j+1}.

Step 1: This step is needed if d_j is finite; otherwise let $C'_j = C_j$, $C'_{j+1} = C_{j+1}$, $e' = e$, and proceed to step 2.

In this step we construct a set $I_1 \subseteq \{1, 2, \ldots, n_j\}$ and matrices $A'_j = A_j[I_1]$, $A'_{j+1} = I_1(A_{j+1})$ such that the $(j-1)$st homology group $H(A_{j-1}, A'_j) \cong H(A_{j-1}, A_j)$ is preserved, while the jth homology group $H(A'_j, A'_{j+1})$ becomes trivial. We show that the corresponding matrices C'_j and C'_{j+1} constructed from A_{j-1}, A'_j, A'_{j+1} and P using Eq. (14) can be also obtained from C_j and C_{j+1}, respectively, as a puncture and row-shortening to a set J_1 such that $e[J_1]$ retains all non-zero bits of e.

Begin by marking the columns of A_j which are incident on non-zero positions in e_1. That is, write

$$e_1 = \sum_{i=1}^{r} a_i \otimes x_i,$$

where $a_i \in \mathbb{F}_2^{n_j}$, and $x_i \in \mathbb{F}_2^r$ with the only non-zero bit at position i. Take I_0 the union of the supports of all vectors a_i. Let $A_j^{(0)} = A_j[I_0]$ denote A_j punctured to I_0, and $A_{j+1}^{(0)} \equiv I_0(A_{j+1})$ denote A_{j+1} row-shortened to I_0.

By construction, $n_j^{(0)} \equiv |I_0| \leq w_1$; since $w_1 < d_j$ and any element in $H(A_j^{(0)}, A_{j+1}^{(0)})$ can be mapped back to an element in $H(A_j, A_{j+1})$ with the same weight, the homology group $H(A_j^{(0)}, A_{j+1}^{(0)})$ must be trivial. Further, the homology group remains trivial if we increase I_0 by adding a set of all linearly independent columns of A_j, to form an enlarged column set $I_1 \supseteq I_0$, such that $A'_j \equiv A_j[I_1]$ satisfies $|I_1| - |I_0| = \mathrm{rank}(A'_j) - \mathrm{rank}(A_j^{(0)})$ and $\mathrm{rank}(A'_j) = \mathrm{rank}(A_j)$. Indeed, denote A'_{j+1} as A_{j+1} row-shortened to I_1; the inclusion $I_0 \subseteq I_1$ gives the lower bound, $\mathrm{rank}(A'_{j+1}) \geq \mathrm{rank}(A_{j+1}^{(0)})$. On the other hand, the orthogonality, $A'_j A'_{j+1} = 0$, gives the matching bound:

$$\begin{aligned} \mathrm{rank}(A'_{j+1}) &\leq |I_1| - \mathrm{rank}(A'_j) \\ &= |I_0| - \mathrm{rank}(A_j^{(0)}) = \mathrm{rank}(A_{j+1}^{(0)}), \end{aligned}$$

which proves the equality. The equality implies that A'_j and A'_{j+1} form an exact sequence (trivial homology):

$$\begin{aligned} \mathrm{rank}\, H(A'_j, A'_{j+1}) &= |I_1| - \mathrm{rank}(A'_j) - \mathrm{rank}(A'_{j+1}) \\ &= |I_0| - \mathrm{rank}(A_j^{(0)}) - \mathrm{rank}(A_{j+1}^{(0)}) \\ &= 0. \end{aligned}$$

Meanwhile, since the column space of A'_j coincides with that of the original matrix A_j, the $(j-1)\,\mathrm{st}$ homology group remains unchanged, $H(A_{j-1}, A_j) = H(A_{j-1}, A'_j)$.

Now use Eq. (14) to construct the corresponding matrices

$$C'_j = \left(\begin{array}{c|c} A'_j \otimes E_r & E_{n_{j-1}} \otimes P \\ \hline & A_{j-1} \otimes E_c \end{array}\right),$$

$$C'_{j+1} = \left(\begin{array}{c|c} A'_{j+1} \otimes E_r & E_{n'_j} \otimes P \\ \hline & A'_j \otimes E_c \end{array}\right),$$

and define the punctured vectors $e'_1 = \sum_i a_i[I_1] \otimes x_i$, $e' = (e'_1|e_2) \equiv e[J_1]$. Since we only removed zero positions, the new vector satisfies $C'_j(e')^T = 0$. Moreover, using the explicit form, $A'_j = A_j[I_1] = A_j E_{n_j}[I_1]$, it is easy to see that $C'_j = C_j[J_1]$, while the matrix C'_{j+1} is a row-shortening of C_{j+1} to J_1. Indeed, if $A'_{j+1} = (E_{n_1}[I_1])^T A_{j+1} D_{I_1}$, then $C'_{j+1} = (E[J_1])^T C_{j+1} D_{J_1}$, with

$$D_{J_1} = \left(\begin{array}{c|c} D_{I_1} \otimes E_r & E_{n_j}[I_1] \otimes E_c \\ \hline & E_{n_j}[I_1] \otimes E_c \end{array}\right).$$

This is row-shortening of C_{j+1} since any vector in the form $C_{j+1} D_{J_1} \alpha^T$ has support limited to J_1.

Step 2: Here we construct a vector $\bar{e}' \simeq e'$ equivalent to e' in the chain complex $\mathcal{C}'$ with boundary operators given by the matrices C'_j, C'_{j+1}. Explicitly, the transformation has the form $(\bar{e}')^T = e'^T + C'_{j+1}(0|\beta_2)^T$. This transformation is designed to remove some portions from the second block of e'. At the same time we disregard any changes to its first block which is no longer relevant since we are going to show that the j th homology group of $\mathcal{C}''$ is trivial, $d''_j = \infty$.

Consider the decomposition

$$e_2 = \sum_{\ell=1}^{c} f_\ell \otimes y_\ell, \; f_\ell \in \mathbb{F}_2^{n_{j-1}}, \tag{16}$$

where $y_\ell \in \mathbb{F}_2^c$ has the only non-zero bit at ℓ. The identity $C'_j(e')^T = 0$ implies $A_{j-1} f_\ell^T = 0$ for any $1 \le \ell \le c$. For those ℓ where f_ℓ^T is linearly dependent with the columns of A'_j, $f_\ell^T = A'_j \alpha_\ell^T$ with some $\alpha_\ell \in \mathcal{C}'_j = \mathbb{F}_2^{n'_j}$, render this vector to zero by the equivalence transformation,

$$(e')^T \to (e')^T + C'_{j+1}(0|\alpha_\ell \otimes y_\ell)^T.$$

Such a transformation may modify the first block of e' in a non-trivial fashion, but only affects the vector f_ℓ in its second block. The resulting vector $\bar{e}' = (\bar{e}'_1|e'_2) = e' + (0|\beta_2)C'^T_{j+1}$ has the second block of weight $\mathrm{wgt}(e'_2) \le \mathrm{wgt}(e_2) < d_{j-1}\delta$, it satisfies $C'_j(\bar{e}')^T = 0$, and in its block representation (16) the remaining non-zero vectors $f_\ell \in H(A_{j-1}, A'_j)$ have weights d_{j-1} or larger. Hence, there remains fewer than δ of non-zero vectors f_ℓ.

Step 3: In a decomposition, $e'_2 = \sum_{j=1}^{n_{j-1}} z_j \otimes c_j$, where $z_j \in \mathbb{F}_2^{n_{j-1}}$ have the only non-zero bit at j, and $c_j \in \mathbb{F}_2^c$, the union of supports of the vectors c_j, I_2, has a length $c' \equiv |I_2| < \delta$. Indeed, I_2 is just the set of the indices ℓ corresponding to the remaining non-zero vectors f_ℓ. Construct a punctured matrix $P' = P[I_2]$ by dropping the columns of P outside of I_2. Since there are fewer than δ columns left, $c' < \delta$, the resulting classical code with parity check matrix P' contains no non-zero vectors, $c' = \mathrm{rank}\, P'$. Construct the modified matrices

$$C''_j = \left(\begin{array}{c|c} A'_j \otimes E_r & E_{n_{j-1}} \otimes P' \\ \hline & A_{j-1} \otimes E_{c'} \end{array}\right),$$

$$C''_{j+1} = \left(\begin{array}{c|c} A'_{j+1} \otimes E_r & E_{n'_j} \otimes P' \\ \hline & A'_j \otimes E_{c'} \end{array}\right),$$

and define the punctured vectors $e''_2 = \sum_{j=1}^{n_0} z_j \otimes c_j[I_2]$ and $e'' = (\bar{e}'_1|e''_2)$. This yields $C''_j(e'')^T = 0$.

Now, after we trimmed the columns of both A_j and of P, according to Eq. (15), the homology group $H(C''_j, C''_{j+1})$ is trivial. This implies that e'' must be a linear combination of the columns of C''_{j+1}, that is, $(e'')^T = C''_{j+1}\beta^T$, for some binary vector β.

Now, it is easy to see that C''_{j+1} can be also written as a row-shortening of C'_{j+1}. Explicitly, $C''_{j+1} = F^T C'_{j+1} D$, where

$$F = \left(\begin{array}{c|c} E_{n'_j} \otimes E_r & \\ \hline & E_{n_{j-1}} \otimes E_c[I_2] \end{array}\right),$$

$$D = \left(\begin{array}{c|c} E_{n_{j+1}} \otimes E_r & \\ \hline & E_{n'_j} \otimes E_c[I_2] \end{array}\right).$$

Clearly, any vector in the form $C'_{j+1}D\alpha^T$ will have all of its non-zero bits preserved after multiplication by F^T (which only affects the second block which is already projected by the lower-right block of D).

We also have $e'' = \bar{e}'F$. Since all non-zero bits in $\bar{e}'$ are preserved by this transformation, we have $(\bar{e}')^T = C'_{j+1}D\beta^T$, a linear combination of the columns of C'_{j+1}. Undoing the equivalence transformation from step 2, we get

$$(e')^T = \bar{e}'^T + C'_{j+1}(0|\beta_2)^T = C'_{j+1}\beta'^T,$$

where $\beta' = \beta D^T + (0|\beta_2)$. The transformation from step 1 gives us

$$(E[J_1])^T e^T = (E[J_1])^T C_{j+1} D_{J_1} \beta'^T.$$

As $(E[J_1])^T$ only trims zero positions for vectors involved on both sides, we conclude the original two-block vector $e = (e_1|e_2)$ is a linear combination of the columns of the original

matrix C_{j+1}, $e^T = C_{j+1} D_{J_1} \beta'^T$. Thus, any such e with block weights $w_1 < d_j$ and $w_2 < d_{j-1}\delta$ which satisfies $C_j e^T = 0$ is necessarily a linear combination of the columns of C_{j+1}. This guarantees $d'_j \geq \min(d_j, d_{j-1}\delta)$.

To complete the proof, consider the case (ii). Here, step 1 can be omitted; the matrices resulting from steps 2 and 3 alone would give trivial homology group, regardless of the weight $\mathrm{wgt}(e_1)$ of the first block. Thus, in this case we get the lower bound $d'_j \geq d_{j-1}\delta$.

■

This proof can be extended to nonbinary field, and may also leads to a proof for the distance of the tensor product of two arbitrary chain complexes.

Chapter 6

Quantum convolutional data-syndrome codes

Since measurements can be faulty as well, redundancy is required to eliminate measurement errors. Those redundancy can be viewed as a HQHP code formed by a quantum code and a classical code. The classical code implements redudancy into the quantum code. Although I haven't had a chance to study the performance of HQHP codes with D¿=4 in FT regime as DS codes, here I study much simpler codes based on quantum convolutional codes. In this chapter, we use a quantum conlutional code as the quantum code, use repetition code or a classical concolutional code as the classical code, hence construct the quantum concolutional code. We consider its performance in a FT regime using several syndrome measurement/decoding strategies and three different error models, including the circuit model.

6.1 Introduction

Quantum stabilizer codes are designed to be robust against qubit errors. However, syndrome measurement cannot be done perfectly: necessarily, there are some measurement errors whose probability grows with the weight of the checks (stabilizer generators). Furthermore, both the syndrome measurement protocol and the syndrome-based decoding have to operate in a fault-tolerant (FT) regime, to be robust against errors that happen during the measurement.

When all checks have relatively small weights, as in the case of the surface codes, one simple approach is to repeat syndrome measurement several times[13]. Then, FT syndrome-based decoding can be done in the assumption that the data errors accumulate while measurement errors be independently distributed. While there is always a non-vanishing probability to have some errors at the end of the cycle, what matters in practice is the ability to backtrack all errors after completion of several rounds of measurement.

Another approach is to measure an overcomplete set of stabilizer generators, using redundancy to recover the correct syndrome. Such an approach was used in the context of higher-dimensional toric and/or color codes[17, 69], the data-syndrome (DS) codes[58, 59, 60], and single-shot measurement protocols[70, 71, 61]. Here decoding is done in the assumption that data error remains the same during the measurement.

We note that with both approaches, the error models assumed for decoding do not exactly match the actual error probability distribution. In particular, any correlations between errors in different locations and/or different syndrome bits are typically ignored. Nevertheless, simulations with circuit-based error models which reproduce at least some of

the actual correlations show that both the repeated syndrome measurement protocol[72, 73] and the syndrome measurement protocols relying on an overcomplete set of generators[69] can result in competitive values of FT threshold.

The choice of the measurement protocol is typically dictated by the structure of the code, specifically, availability of an overcomplete set of stabilizer generators of the minimum weight. Such an approach is expected to be practical when typical gate infidelities are comparable with the probability of an incorrect qubit measurement. However, there is also a price to pay: codes with redundant sets of small-weight checks can be generally expected to have worse parameters.

On the other hand, if the physical one- and two-qubit gates are relatively accurate, it may turn out more practical to measure redundant sets of checks which include stabilizer generators of higher weights. Then, a DS code can be designed from any stabilizer code[58, 59, 60]. As a result, one faces a problem of constructing an optimal measurement protocol given the known gate fidelities and measurement errors.

In this work we compare several single-shot and repeated measurement/decoding protocols for a simple quantum convolutional code[74] with the parameters $[[24, 6, 3]]$ and syndrome generators of weight 6. We construct several computationally efficient schemes using the classical Viterbi algorithm[75, 76] to decode data and syndrome errors sequentially or simultaneously, and compare their effectiveness both with phenomenological and circuit-based depolarizing error models. In particular, we show that a DS code which requires measuring checks of weight up to $w_{\max} = 9$ has performance (successful decoding probability) exceeding that of the repeated measurement scheme when single-qubit mea-

surement error probability q_1 equals ten times the gate error probability p_1 (taken to be the same for Hadamard and CNOT gates).

6.2 Background

Let $\mathcal{P}_n = \{c\, M_1 \otimes \cdots \otimes M_n : M_j \in \{I, X, Y, Z\}\}$, with phase $c \in \{\pm 1, \pm i\}$ be the n-qubit Pauli group; elements with $c = \pm 1$ have eigenvalues ± 1. Any $G = c\, M_1 \otimes \cdots \otimes M_n \in \mathcal{P}_n$ can be represented, up to a phase, by length-n vector $\mathbf{g} = (g_1, \ldots, g_n) \in \mathbb{F}_4^n$, $\mathbb{F}_4 = \{0, 1, \omega, \bar{\omega}\}$, where $\omega^2 \equiv \bar{\omega} = \omega + 1$, and $g_j = 0, 1, \omega, \bar{\omega}$, if M_j is I, X, Z, or Y, respectively. The weight $\mathrm{wt}(\mathbf{g})$ of $\mathbf{g}$ is the number of its nonzero elements $g_j \neq 0$. A product of two Pauli operators X and Y is mapped into a sum of the corresponding vectors, $\mathbf{x} + \mathbf{y}$. Further, a pair of Pauli operators commute iff the trace inner product,

$$\mathbf{x} * \mathbf{y}^T \equiv \sum\nolimits_{i=1}^{n} \mathrm{Tr}(x_i \bar{y}_i), \tag{6.1}$$

of the corresponding vectors is zero, $\mathbf{x} * \mathbf{y}^T = 0$. Here $\mathrm{Tr}(x) = x + x^2$ is the trace map from $\mathbb{F}_4$ into $\mathbb{F}_2$, and $\bar{y}$ is the conjugation of $y \in \mathbb{F}_4$ which interchanges ω and $\bar{\omega}$.

For numerics in this chapter, we use the family of quantum convolutional codes (QCCs) of length $3(k+2)$, $k = 1, 2, \ldots$, based on linear $(3, 1)$ self-orthogonal convolutional codes whose generator matrces are constructed[74] by $k+1$ shifts of the row $\mathbf{g}_1 = (111|1\omega\bar{\omega})$. The actual generating matrix of the QCC $\mathcal{Q}_k$ with parameters $[[3(k+2), k, 3]]$ is obtained by adding a copy of the same rows multiplied by ω, and four additional rows for proper

termination. In the case $k = 2$, the stabilizer generating matrix has the form

$$\mathbf{G}(\mathcal{Q}_2) = \left(\begin{array}{ccc|ccc|ccc|ccc} 1 & \omega & \overline{\omega} & & & & & & & & & \\ \overline{\omega} & \omega & 1 & & & & & & & & & \\ 1 & 1 & 1 & 1 & \omega & \overline{\omega} & & & & & & \\ \omega & \omega & \omega & \omega & \overline{\omega} & 1 & & & & & & \\ & & & 1 & 1 & 1 & 1 & \omega & \overline{\omega} & & & \\ & & & \omega & \omega & \omega & \omega & \overline{\omega} & 1 & & & \\ & & & & & & 1 & 1 & 1 & 1 & \omega & \overline{\omega} \\ & & & & & & \omega & \omega & \omega & \omega & \overline{\omega} & 1 \\ & & & & & & & & & \overline{\omega} & \omega & 1 \\ & & & & & & & & & 1 & 1 & 1 \end{array}\right). \tag{6.2}$$

6.3 Error models and data-syndrome codes

Unlike with classical codes, extracting a syndrome for a quantum code involves a complicated quantum measurement which itself is prone to errors. To extract a syndrome bit corresponding to a row $\mathbf{g}$ of $\mathbf{G}$, one must execute a unitary which involves a non-trivial interaction [some single-qubit gate(s) and an entangling gate, e.g., a quantum `CNOT`] with each of the $w \equiv \mathrm{wt}(\mathbf{g})$ qubits in the support of $\mathbf{g}$, then do a quantum measurement of one or more auxiliary *ancilla* qubit(s). Data errors and measurement (ancilla) errors can happen at every step of the process; moreover, errors can propagate through measurement circuit unless it is designed using FT gadgets to prevent error multiplication[86]. Error propagation can be simulated efficiently for any circuit constructed from Clifford gates which map the Pauli group onto itself, which is sufficient to simulate the performance of

any stabilizer code[104]. In this work we simulated such a *circuit-based error* model (C), using depolarizing noise with probability p_1 (randomly chosen X, Y, or Z on every qubit in the interval between subsequent gates, including null gates for idle qubits), and additional ancilla measurement error with probability q_1 [72, 73].

While in principle it is possible to account for all correlations between the errors that may result from error propagation in a given circuit, and design a corresponding decoder, it would be a daunting task. Instead, one usually uses a decoder designed for some phenomenological error model, and uses circuit model (C) only to check the performance of such a decoder numerically. We consider two such error models.

Model (A) is a channel model where qubit errors (depolarizing noise with probability p) happen before the measurement, while each stabilizer generator (syndrome bit) is measured with independent error probability q. This model[59, 60] is an idealization of a situation where gate errors are small compared to qubit preparation and measurement errors. Clearly, model (A) can get unphysical, as here one can extract the syndrome perfectly with sufficient measurement redundancy.

This drawback is compensated somewhat in the phenomenological error model (B) which includes several rounds of syndrome measurement, and includes qubit errors that happen before each round (depolarizing noise with probability p; these errors accumulate between measurement rounds), and independent syndrome measurement errors with probability q. Both in the phenomenological model (B) and in the circuit model (C) some errors may remain after the last round of error correction; for simulations one includes an additional round with perfect syndrome measurement[72].

Phenomenological error models (A) and (B) can be used to construct DS codes dealing both with qubit (data) and syndrome errors. We start with an $r \times n$ stabilizer generator matrix $\mathbf{G}$, which may include additional linearly-dependent rows, thus $r \geq n-k$. In model (A), we have a qubit error vector $\mathbf{e} \in \mathbb{F}_2^n$, and a syndrome measurement error $\boldsymbol{\epsilon} \in \mathbb{F}_2^r$; the extracted syndrome vector is given by $\mathbf{s}^T = \mathbf{G} * \mathbf{e}^T + \boldsymbol{\epsilon}^T$. To characterize DS codes, it is convenient to consider mixed-field vector spaces, with elements $(\mathbf{e} \,|\, \boldsymbol{\epsilon})$, a pair of a quaternary and a binary vectors. For such pairs we define the inner product

$$(\mathbf{e}_1, \boldsymbol{\epsilon}_1) \star (\mathbf{e}_2, \boldsymbol{\epsilon}_2)^T \equiv \mathbf{e}_1 * \mathbf{e}_2^T + \boldsymbol{\epsilon}_1 \boldsymbol{\epsilon}_2^T. \tag{6.3}$$

By analogy with stabilizer codes, we define an additive code $\mathcal{C}_{\mathrm{DS}} \subseteq \mathbb{F}_4^n \oplus \mathbb{F}_2^r$ with the generator matrix

$$\mathbf{G}_{\mathrm{DS}} = \left(\begin{array}{c|c} \mathbf{G} & \mathbf{I} \end{array} \right), \tag{6.4}$$

and its dual with respect to the product (6.3), $\mathcal{C}_{\mathrm{DS}}^{\perp}$. The two orthogonal DS codes satisfy $|\mathcal{C}_{\mathrm{DS}}|\,|\mathcal{C}_{\mathrm{DS}}^{\perp}| = 2^{2n+r}$. Because the original code $\mathcal{C}$ is self orthogonal, $\mathbf{G} * \mathbf{G}^T = 0$, the code $\mathcal{C}_{\mathrm{DS}}^{\perp}$ includes vectors in the form $(\mathbf{e} \,|\, \mathbf{0})$, where $\mathbf{e} = \boldsymbol{\alpha}\mathbf{G}$ is an additive combination of the rows of $\mathbf{G}$, $\boldsymbol{\alpha} \in \mathbb{F}_2^r$. The distance d_{DS} of thus defined DS code is the minimum weight of a vector in $\mathcal{C}_{\mathrm{DS}}^{\perp} \setminus (\mathcal{C} \oplus \mathbf{0})$, it is upper bounded by the distance of the original quantum code $\mathcal{Q}$, $d_{\mathrm{DS}} \leq d$.

In phenomenological error model (B), with ℓ-times repeated syndrome measurement (including the final perfect measurement), we denote qubit errors that occur before the measurement t as $\mathbf{e}_t \in \mathbb{F}_4^n$, and the corresponding measurement errors as $\boldsymbol{\epsilon}_t \in \mathbb{F}_2^r$. The qubit errors accumulate, thus we can write for the syndrome $\mathbf{s}_t$ obtained in the t th round

of measurement:

$$\mathbf{G} * (\mathbf{e}_1 + \mathbf{e}_2 + \ldots + \mathbf{e}_t) + \boldsymbol{\epsilon}_t \quad = \quad \mathbf{s}_t.$$

In this work we do not attempt simultaneous decoding of data and syndrome errors over several rounds of measurement. Instead we decode them sequentially, using the accumulated errors $\hat{\mathbf{e}}_1 + \hat{\mathbf{e}}_2 + \ldots + \hat{\mathbf{e}}_{t-1}$ extracted at previous decoding rounds to offset the error at time t.

6.4 Convolutional DS codes

Now, given an $[[n, k]]$ quantum code $\mathcal{Q}$ with the (full-row-rank) generating matrix $\mathbf{G}(\mathcal{Q})$ of size $(n-k) \times n$, we introduce redundant measurements by adding some linearly dependent rows. Without limiting generality, a set of r' additional rows $\mathbf{F} = \mathbf{AG}(\mathcal{Q})$ can be obtained by multiplying the original generating matrix by an $r' \times (n-k)$ binary matrix $\mathbf{A}$, so that the generating matrix 6.5 of the resulting DS code has the form

$$\mathbf{G}_{\mathrm{DS}} = \left(\begin{array}{c|cc} \mathbf{G}(\mathcal{Q}) & \mathbf{I}_{n-k} & \\ & & \\ \mathbf{AG}(\mathcal{Q}) & & \mathbf{I}_{r'} \end{array} \right). \tag{6.5}$$

This matrix has additive rank $r \equiv (n-k) + r'$ equal to the number of rows. It is convenient to rewrite this matrix in the following row-equivalent form,

$$\mathbf{G}'_{\mathrm{DS}} = \left(\begin{array}{c|cc} \mathbf{G}(\mathcal{Q}) & \mathbf{I}_{n-k} & \\ & & \\ & \mathbf{A} & \mathbf{I}_{r'} \end{array} \right). \tag{6.6}$$

Denote $[\mathbf{G}(\mathcal{Q})]^{\perp}$ the additive dual of $\mathbf{G}(\mathcal{Q})$ with additive rank $n+k$, and $\mathbf{M}$ a matrix such that $\mathbf{G}(\mathcal{Q})\,\mathbf{M}^T = \mathbf{I}_{n-k}$. It is then easy to see that the matrix

$$\mathbf{H}_{\mathrm{DS}} = \left(\begin{array}{c|cc} [\mathbf{G}(\mathcal{Q})]^{\perp} & & \\ \mathbf{M} & \mathbf{I}_{n-k} & \mathbf{A}^T \end{array}\right). \tag{6.7}$$

has additive rank $(n+k)+(n-k) = 2n$, while $\mathbf{G}'_{\mathrm{DS}} \star \mathbf{H}_{\mathrm{DS}}^T = 0$. Thus, $\mathbf{H}_{\mathrm{DS}}$ generates the code $\mathcal{C}_{DS}^{\perp}$.

We can now discuss the choice of the matrix $\mathbf{A}$. First, we obtain redundant syndrome bits by measuring operators F_j corresponding to the rows $\mathbf{f}_j$ of the matrix $\mathbf{F}$. Since the corresponding error grows with the operator weight, we want to choose matrix $\mathbf{A}$ to ensure that row weights of $\mathbf{F}$ be small. Second, we want to choose $\mathbf{A}$ so that the binary linear code generated by $(\mathbf{I}_{n-k}, \mathbf{A}^T)$ has a large minimum distance. Third important issue is the decoding complexity. Given the structure of the matrix $\mathbf{H}_{\mathrm{DS}}$, see Eq. (6.7), it is natural to choose $\mathbf{A}^T$ to form a generator matrix of a classical convolutional code. Quantum DS codes (6.5) obtained from a quantum convolutional code $\mathcal{Q}$ with such an $\mathbf{A}$ we call *convolutional DS codes*.

6.5 Decoding of Convolutional DS Codes

Big advantage of classical convolutional codes is that one can use the maximum-likelihood Viterbi decoding using a code trellis [76]. The "stripe" form of a generator matrix of a convolutional code (with small band width) ensures that its code trellis has relatively small number of states, which means that the Viterbi decoding has relatively small complexity.

In our case, it is not immediately obvious how to construct a code trellis with a manageable number of states, since neither $\mathbf{G}_{\mathrm{DS}}$ nor $\mathbf{H}_{\mathrm{DS}}$ has the "stripe" form. However, we show that $\mathbf{G}_{\mathrm{DS}}$ can be transformed into the stripe form.

Instead of presenting a general algorithm for this, we will consider a small example. Let $\mathbf{G}(\mathcal{Q})$ and $\mathbf{A}$ be generated by vectors $(\mathbf{v}_1|\mathbf{v}_2|\mathbf{v}_3)$ and $(\mathbf{u}_1|\mathbf{u}_2|\mathbf{u}_3)$, respectively, and assume that $\mathbf{v}_i$ and $\mathbf{u}_i$ have lengths n and n'. Then, in a particular case, the DS code generator (6.6) has the form

$$\mathbf{G}'_{\mathrm{DS}} = \begin{pmatrix}
\mathbf{v}_1 & \mathbf{v}_2 & \mathbf{v}_3 & & & 1 & & & & & & \\
 & \mathbf{v}_1 & \mathbf{v}_2 & \mathbf{v}_3 & & & 1 & & & & & \\
 & & \mathbf{v}_1 & \mathbf{v}_2 & \mathbf{v}_3 & & & 1 & & & & \\
 & & & & & \mathbf{u}_1^T & & & \mathbf{I} & & & \\
 & & & & & \mathbf{u}_2^T & \mathbf{u}_1^T & & & \mathbf{I} & & \\
 & & & & & \mathbf{u}_3^T & \mathbf{u}_2^T & \mathbf{u}_1^T & & & \mathbf{I} & \\
 & & & & & & \mathbf{u}_3^T & \mathbf{u}_2^T & & & & \mathbf{I} \\
 & & & & & & & \mathbf{u}_3^T & & & &
\end{pmatrix},$$

where $\mathbf{I}$ is the $n' \times n'$ identity matrix. With an appropriate permutation of columns and rows, we can transform the above matrix into the form

$$\mathbf{G}''_{\mathrm{DS}} = \left(\begin{array}{cccc|cccccccc}
\mathbf{v}_1 & \mathbf{v}_2 & & & \mathbf{v}_3 & 1 & & & & & & \\
 & & \mathbf{I} & & & \mathbf{u}_1^T & & & & & & \\
 & \mathbf{v}_1 & & & \mathbf{v}_2 & & \mathbf{v}_3 & 1 & & & & \\
 & & & \mathbf{I} & & \mathbf{u}_2^T & & \mathbf{u}_1^T & & & & \\
 & & & & \mathbf{v}_1 & & \mathbf{v}_2 & & \mathbf{v}_3 & 1 & & \\
 & & & & & \mathbf{u}_3^T \quad \mathbf{I} & & \mathbf{u}_2^T & & & \mathbf{u}_1^T & \\
\hline
 & & & & & & & \mathbf{u}_3^T & \mathbf{I} & & \mathbf{u}_2^T & \\
 & & & & & & & & & & \mathbf{u}_3^T & \mathbf{I}
\end{array}\right),$$

where we marked the small matrix block that defines the repeating section of the syndrome trellis. Now, the method in Ref. [105] gives the syndrome trellis, a particular form of the code trellis.

Let $(\mathbf{v}, \mathbf{s}) \in C_{\mathrm{DS}}^{\perp}$ and define the received vectors $\mathbf{x} = \mathbf{v} + \mathbf{e} \in \mathbb{F}_4^n$, $\mathbf{y} = \mathbf{s} + \boldsymbol{\epsilon} \in \mathbb{F}_2^{n-k+r'}$, where $\mathbf{e}$ and $\boldsymbol{\epsilon}$ are qubit and syndrome errors, respectively. The syndrome allows us to efficiently conduct the Viterbi minimum distance decoding (MDD) using $(\mathbf{x}, \mathbf{y})$ as an input:

$$\mathrm{MDD}(\mathbf{x}, \mathbf{y}) = \arg \min_{(\mathbf{a},\mathbf{b}) \in C_{\mathrm{DS}}^{\perp}} \mathrm{wt}(\mathbf{a} - \mathbf{x}) + \mathrm{wt}(\mathbf{y} - \mathbf{b}).$$

However, unlike in the classical case where we receive $(\mathbf{x}, \mathbf{y})$ from a channel, in the quantum case we have only $\mathbf{y} = \mathbf{s} + \mathbf{e}$, and we do not have $\mathbf{x}$. It is easy to check that in this case the correct minimum distance decoding corresponds to $\mathrm{MDD}(\mathbf{0}, \mathbf{y})$. For simulations in this work we implemented a version of Viterbi decoding for non-binary classical codes with known

symbol error probabilities. For DS decoding with phenomenological noise parameters p and q, we used

$$\Pr(X) = \Pr(Y) = \Pr(Z) = p/3 \text{ and } \Pr(\epsilon_j = 1) = q.$$

In addition, one can use several suboptimal decoders with significantly smaller complexity. In particular, one may use the following *2 step algorithm*

1. Construct the syndrome trellis, say T, for the DS code with $\mathbf{G}_{\rm DS} = (\mathbf{G}|\mathbf{I}_r)$. It will have much smaller number of states compared with the trellis for Eq. (6.7).

2. Decode $\mathbf{y}$ by the Viterbi decoding of the code with generator $(\mathbf{I}_{n-k}, \mathbf{A}^T)$, to get a tentative syndrome $\widehat{\mathbf{s}} = (\widehat{s}_1, \ldots, \widehat{s}_{n-k})$. Typically $\widehat{\mathbf{s}}$ would have significantly smaller number of errors than the measured syndrome.

3. Decode $(\mathbf{0}, \widehat{\mathbf{s}})$ by the Viterbi decoding using trellis T.

Several variations of this algorithm are possible. For example we may decode $\mathbf{y}$ using a list decoding of size L, get several tentative syndromes $\widehat{\mathbf{s}}_i, i = 1, \ldots, L$, and use them in turn in step 3 of the above algorithm, and choose the best result.

Another possibility is to use BCJR decoding for computing the tentative syndrome $\widehat{\mathbf{s}} = (\widehat{s}_1, \ldots, \widehat{s}_{n-k})$.

6.6 Numerical results

We constructed the trellises and numerically analyzed the performance of several quantum convolutional DS codes differing by the structure of the binary generating matrix $\mathbf{A}$. In all cases, we used as the starting code the code $\mathbf{Q}_6$ with parameters $[[24, 6, 3]]$

constructed from a linear $\mathbb{F}_4$ convolutional code with generator $\mathbf{g} = (111|1\omega\bar{\omega})$, one of the many QCCs constructed in Ref. [74]. As discussed in Sec. 6.2, the stabilizer generators for codes in this family have weights $\mathrm{wt}(\mathbf{g}_j) \in \{3, 6\}$, see Eq. (6.2).

Specifically, we used the following choices. (**i**) Code "GA", a quantum DS CC (6.5) with the 16×18 matrix $\mathbf{A}^T$ chosen as the generating matrix of the binary convolutional code (CC) with the generator row $\mathbf{g} = (11|01|11)$. Explicitly,

$$\mathbf{A}^T_{\mathrm{GA}} = \begin{pmatrix} 1\,1 & 0\,1 & 1\,1 & & \\ & 1\,1 & 0\,1 & 1\,1 & \\ & & \cdots & \cdots & \cdots \end{pmatrix}. \tag{6.8}$$

Matrix $\mathbf{F} = \mathbf{A}_{\mathrm{GA}}\mathbf{G}(\mathcal{Q}_k)$ has row weights $\mathrm{wt}(\mathbf{f}_j) \in \{6, 9\}$.

(**ii**) Code "GR" (here R stands for "repetition") is constructed similarly, except the matrix $\mathbf{A}^T$ is formed by a trivial CC code with $\mathbf{g} = (11)$. Explicitly, it has the form

$$\mathbf{A}^T_{\mathrm{GR}} = \begin{pmatrix} 1\,1 & & \\ & 1\,1 & \\ & & \cdots \end{pmatrix}. \tag{6.9}$$

It is easy to see that such a matrix results from three-times repeated measurement of the original set of generators in the 18 rows of $\mathbf{G}(\mathcal{Q}_6)$. Respectively, only the original stabilizer generators of weights 3 and 6 need to be measured here.

(**iii**) Code "GI" is a trivial DS code with $\mathbf{A}_{\mathrm{GI}} = \mathbf{0}$. The name is due to the structure of the matrix (6.5): in this case it has the form $\mathbf{G}_{\mathrm{DS}} = (\mathbf{G}(\mathcal{Q}_6)\,|\,\mathbf{I}_{18})$. With phenomenological error model (A) [Sec. 6.3] and three-times repeated measurement, we use this code as a simpler alternative to code "GR". Namely, we first perform majority vote on every bit of the syndrome, then use the DS code GI for actual decoding.

(**iv**) Finally, the code "G" stands for yet another simple DS decoding protocol for three-time repeated measurements. Again, the syndrome bits are obtained using majority vote, but the resulting syndrome is considered as error-free, and the decoding is done directly using the QCC $\mathcal{Q}_6$. Main difference with the previous case is that here a single-bit syndrome error after majority vote necessarily results in a decoding fault.

Results of simulations with phenomenological error model (A) are shown in Fig. 6.1, along with a break-even line $P_{\rm BLER} = 6p$ ($k = 6$ unprotected qubits). We did not attempt to account for larger weight of measured operators in the case of code GA. Single-shot block error probabilities $P_{\rm BLER}$ for four decoders as indicated in the caption are shown. For each point, simulations were done until $N = 100$ decoder failures. The slope is consistent with the distance $d = 3$ of the quantum code. Results indicate that (with the exception of the simplest decoder G) all decoders are able to correct most syndrome measurement errors with $q = p$, and also for $q = 10p$ in the interval $p \lesssim 10^{-3}$. With larger error rates, code GA works best, consistent with its larger distance for syndrome errors.

In simulations with phenomenological error model (B) we measured the average fail time of the code[72]. Namely, in each simulation round j repeated decoding cycles are done until decoding failure after round t_j; the corresponding average after $N \geq 100$ simulation rounds was recorded. Effective block error rate $P_{\rm BLER} = 1/(\bar{t} - 1)$ was then extracted from the average fail time $\bar{t}$ assuming Poisson distribution of life times $t'_j = t_j - 1$ with parameter $\lambda = P_{\rm BLER}$. We decoded every cycle t separately, using the accumulated data error $\hat{\mathbf{e}}_1 + \hat{\mathbf{e}}_2 + \ldots + \hat{\mathbf{e}}_{t-1}$ found in the previous cycles as an offset. Consistent with the standard protocol for quantum LDPC codes[72], a failure would be recorded if at time

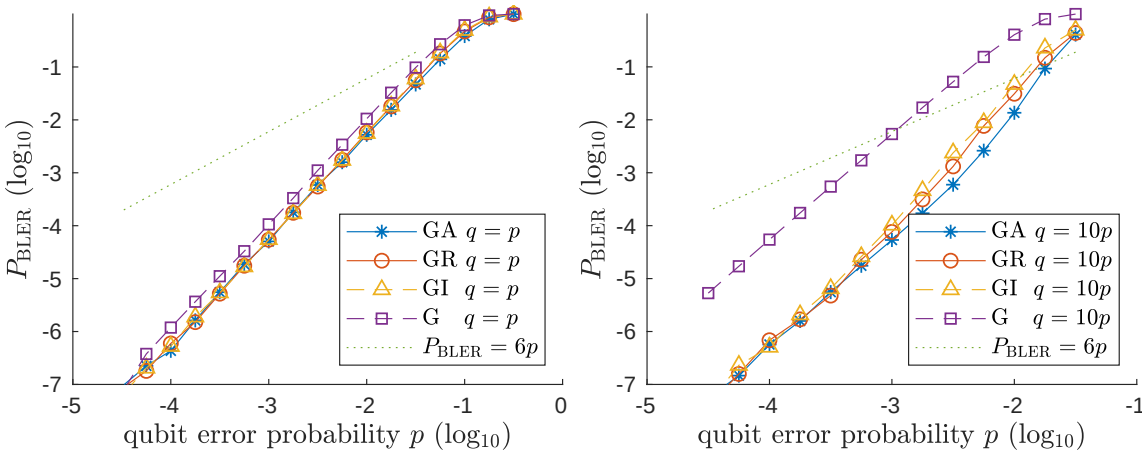

Figure 6.1: Phenomenological noise model (A) with depolarizing errors (probability p) and syndrome bit measurement error probability $q = p$ (left) and $q = 10p$ (right). Symbols show the block error probability P_{BLER} for four decoders as indicated, see text for details. Dotted lines give the nominal single-qubit break-even threshold, $P_{\mathrm{BLER}} = 6p$.

step t decoding with zero syndrome error $\boldsymbol{\epsilon}_t = \mathbf{0}$ gives a logical error. Otherwise, a new estimated error $\hat{\mathbf{e}}_t$ would be computed with the syndrome error $\boldsymbol{\epsilon}_t$ present, and calculation repeated at $t = t + 1$. The results are shown in Fig. 6.2; they are largely consistent with those for phenomenological error model (A).

In simulations with circuit error model (C) we constructed the actual circuits for measuring quantum operators corresponding to rows of $\mathbf{G}$, including the redundant rows for code GA, with the attempt to maximally parallelize the measurements. We then used a separate program to generate random Pauli errors with probability p_1 per interval between the gates, propagated the errors through the circuit, and recorded the actual accumulated error $\underline{\mathbf{e}}_t$ and the measured syndrome $\mathbf{s}_t$ at the end of each measurement cycle $t = 1, 2, \ldots$. Additional syndrome measurement error q_1 was added at the time of subsequent processing. These data then have been used with the decoders identical to those for model B.

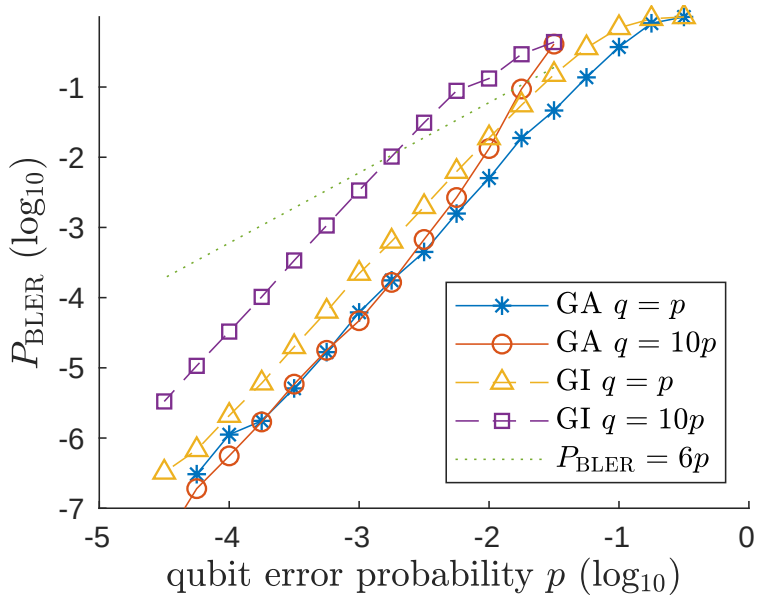

Figure 6.2: Effective block error rate P_{BLER} with phenomenological error model B. Only results for GA and single-interval GI decoders as indicated are shown.

The obtained effective block error rates are plotted in Fig. 6.3. One striking difference with phenomenological error models A and B is that the calculated curves no longer have quadratic dependence on BER, as would be expected for a code with distance $d = 3$. The reason is that we have used non-FT circuits in simulations. As a result, e.g., a single ancilla error can propagate and multiply through the circuit, resulting in a higher-weight error which cannot be corrected by the code.

6.7 Discussion and Future Work

In conclusion, in this work we introduced quantum convolutional data-syndrome codes, constructed an efficient decoder for this class of codes, and analyzed numerically the performance of a family of DS codes based on a single QCC with parameters $[[24, 6, 3]]$

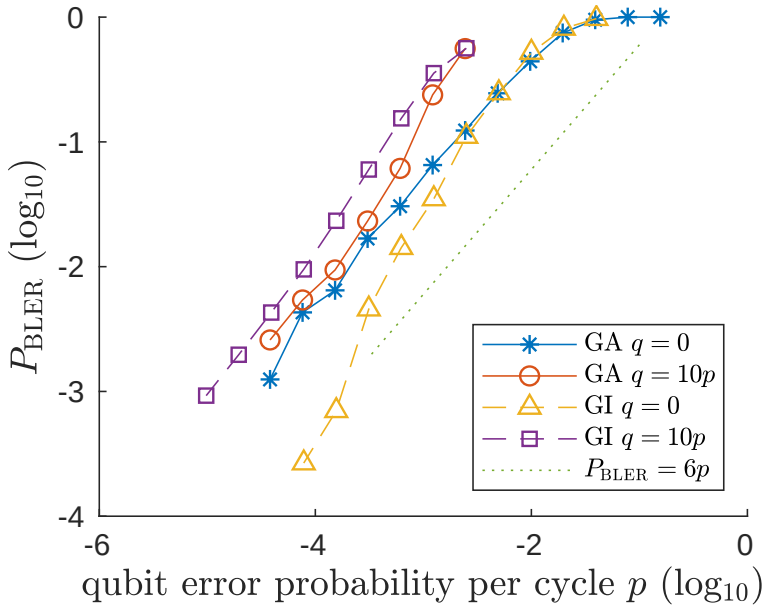

Figure 6.3: Effective block error rate (per gate) for phenomenological error model C as a function of gate error probability p_1 scaled by cycle duration.

using three distinct error models. In particular, this was the first time a DS code has been simulated with the circuit error model.

Here we exclusively relied on the QCCs designed in Ref. [74]. These codes have relatively high weights of stabilizer generators. It is an open question whether degenerate QCCs exist, with small-weight generators, large distances, and trellises with reasonably small memory sizes. For the purpose of constructing convolutional DS codes, one would further like to have a QCC with a redundant set of minimum-weight stabilizer generators. For such codes, degenerate Viterbi decoding algorithm[106] would be particularly useful.

Our limited simulation results indicate that a DS code with large-distance classical syndrome code may show competitive performance in the regime where measurement errors are significant, even though the corresponding generators may have larger weights. This regime is experimentally relevant, e.g., for superconducting transmon qubits with dispersive

readout, where measurement time can be as large as 500ns, compared to under 50ns two-qubit gates, with the error probabilities scaling accordingly. It is an open question whether similarly constructed non-convolutional DS codes could be useful in this regime, e.g., for optimizing the performance of surface codes in the current or near-future generation of quantum computers.

One obvious way to improve the practical performance of DS codes is by using FT gadgets for generator measurements, to control error propagation. In particular, we intend to try flag measurement circuits[107], as this technique has relatively small overhead in the number of qubits.

Chapter 7

Conclusions

Our main work on the HQHP code focuses on the Hamming distance. This algebraic construction of LDPC codes with explicit parameters helps to answer the key question in developing quantum LDPC codes, that is, the trade-off among n, k, d, w. Here w stands for sparsity, the maximum row and column weight of the parity-check matrix. What is the optimal code one can find, since there is no constraint saying that we can only get $d = \mathcal{O}(\sqrt{n})$? Our approach to tackling this problem is by generalizing known codes and discovering what is more fundamental and achievable. The HQHP codes[38] generalize both QHP codes and toric codes in all dimensions. The subsystem product codes, obtained by projecting the HQHP codes, can be gauge fixed to concatenated codes and homological product codes. Those include the famous Shor's code and Bacon-Shor code as special cases. Meanwhile, HQHP codes can be mapped to tensor products of chain complexes, which provides an algebraic framework to construct quantum LDPC codes with finite code rates, square root distances, FT thresholds, and single-shot properties with redundant checks.

Those code parameters can be even further improved after those generalizations by HQHP codes. For example, the fiber bundle codes[45] break the square root distance record and lifting it to $n^{3/5}/\text{polylog}(n)$. The construction implements a twist to the chain complex, hence cannot be mapped to a product of two manifolds. If this twisting technique can be generalized to HQHP codes, one can get a larger distance that is favored by FT threshold. There are also other candidates like rotated HQHP codes which may increase the code rates. Since toric code and its variants are always included in those constructions, it is necessary to understand the trade-off between the FT threshold and locality in the case of toric code and large code rates and distances in other cases.

Another designing goal of QECCs is the implementation of universal FT gates. Among various qLDPC codes, it has been demonstrated for QHP codes[108] and homological product codes[109]. Those are done by accommodating various initial states according to the structure of the codes. The HQHP codes have similar structures, which make it possible to design a protocol for HQHP codes, hence complete the puzzle for FT quantum computation.

In Chapter 6, we introduced quantum convolutional data-syndrome codes, constructed an efficient decoder for this class of codes, and analyzed numerically the performance of a family of DS codes based on a single QCC with parameters $[[24, 6, 3]]$ using three distinct error models. In particular, this was the first time a DS code has been simulated with the circuit error model.

Here we exclusively relied on the QCCs designed in Ref. [74]. These codes have relatively high weights of stabilizer generators. It is an open question whether degenerate QCCs exist, with small-weight generators, large distances, and trellises with reasonably

small memory sizes. For the purpose of constructing convolutional DS codes, one would further like to have a QCC with a redundant set of minimum-weight stabilizer generators. For such codes, degenerate Viterbi decoding algorithm[106] would be particularly useful.

Our limited simulation results indicate that a DS code with large-distance classical syndrome code may show competitive performance in the regime where measurement errors are significant, even though the corresponding generators may have larger weights. This regime is experimentally relevant, e.g., for superconducting transmon qubits with dispersive readout, where measurement time can be as large as 500ns, compared to under 50ns two-qubit gates, with the error probabilities scaling accordingly. It is an open question whether similarly constructed non-convolutional DS codes could be useful in this regime, e.g., for optimizing the performance of surface codes in the current or near-future generation of quantum computers.

One obvious way to improve the practical performance of DS codes is by using FT gadgets for generator measurements, to control error propagation. In particular, it would be interesting to try flag measurement circuits[107], as this technique has relatively small overhead in the number of qubits.

Bibliography

[1] Yuri Manin. Computable and uncomputable. *Sovetskoye Radio, Moscow*, 128, 1980.

[2] Richard P Feynman. Simulating physics with computers. *Int. J. Theor. Phys*, 21(6/7), 1982.

[3] Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.

[4] Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219, 1996.

[5] David P DiVincenzo. The physical implementation of quantum computation. *Fortschritte der Physik: Progress of Physics*, 48(9-11):771–783, 2000.

[6] John Preskill. Quantum computing in the nisq era and beyond. *Quantum*, 2:79, 2018.

[7] Seth Lloyd. Universal quantum simulators. *Science*, pages 1073–1078, 1996.

[8] Jarrod R McClean, Jonathan Romero, Ryan Babbush, and Alán Aspuru-Guzik. The theory of variational hybrid quantum-classical algorithms. *New Journal of Physics*, 18(2):023023, 2016.

[9] Tameem Albash and Daniel A Lidar. Adiabatic quantum computation. *Reviews of Modern Physics*, 90(1):015002, 2018.

[10] Jacob Biamonte, Peter Wittek, Nicola Pancotti, Patrick Rebentrost, Nathan Wiebe, and Seth Lloyd. Quantum machine learning. *Nature*, 549(7671):195–202, 2017.

[11] S. B. Bravyi and A. Yu. Kitaev. Quantum codes on a lattice with boundary. *Quantum Computers and Computing*, 2(1):43–48, 2001.

[12] M. H. Freedman and D. A. Meyer. Projective plane and planar quantum codes. *Foundations of Computational Mathematics*, 1:325–332, 2001.

[13] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill. Topological quantum memory. *J. Math. Phys.*, 43:4452, 2002.

[14] H. Bombin and M. A. Martin-Delgado. Homological error correction: Classical and quantum codes. *Journal of Mathematical Physics*, 48(5):052105, 2007.

[15] C. Castelnovo and C. Chamon. Topological order in a three-dimensional toric code at finite temperature. *Phys. Rev. B*, 78:155120, Oct 2008.

[16] D. Mazáč and A. Hamma. Topological order, entanglement, and quantum memory at finite temperature. *Annals of Physics*, 327(9):2096 – 2111, 2012.

[17] H. Bombin, R. W. Chhajlany, M. Horodecki, and M. A. Martin-Delgado. Self-correcting quantum computers. *New Journal of Physics*, 15(5):055023, 2013.

[18] A. Yu. Kitaev. Fault-tolerant quantum computation by anyons. *Ann. Phys.*, 303:2, 2003.

[19] S. Bravyi and B. Terhal. A no-go theorem for a two-dimensional self-correcting quantum memory based on stabilizer codes. *New Journal of Physics*, 11(4):043029, 2009.

[20] S. Bravyi, D. Poulin, and B. Terhal. Tradeoffs for reliable quantum information storage in 2D systems. *Phys. Rev. Lett.*, 104:050503, Feb 2010.

[21] N. Delfosse. Tradeoffs for reliable quantum information storage in surface codes and color codes. In *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on*, pages 917–921, Istanbul, Turkey, 2013. IEEE.

[22] S. T. Flammia, J. Haah, M. J. Kastoryano, and I. H. Kim. Limits on the storage of quantum information in a volume of space. *Quantum*, 1:4, 2017.

[23] A. A. Kovalev and L. P. Pryadko. Fault tolerance of quantum low-density parity check codes with sublinear distance scaling. *Phys. Rev. A*, 87:020304(R), Feb 2013.

[24] I. Dumer, A. A. Kovalev, and L. P. Pryadko. Thresholds for correcting errors, erasures, and faulty syndrome measurements in degenerate quantum codes. *Phys. Rev. Lett.*, 115:050502, Jul 2015.

[25] D. Gottesman. Fault-tolerant quantum computation with constant overhead. *Quant. Information and Computation*, 14:1338–1371, 2014.

[26] R. Gallager. Low-density parity-check codes. *IRE Trans. Inf. Theory*, 8(1):21–28, Jan 1962.

[27] R. G. Gallager. *Low-Density Parity-Check Codes*. M.I.T. Press, Cambridge, Mass., 1963.

[28] S. Litsyn and V. Shevelev. On ensembles of low-density parity-check codes: asymptotic distance distributions. *IEEE Trans. Inf. Theory*, 48(4):887–908, Apr 2002.

[29] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke. Design of capacity-approaching irregular low-density parity-check codes. *Information Theory, IEEE Transactions on*, 47(2):619–637, 2001.

[30] G. Zémor. On Cayley graphs, surface codes, and the limits of homological coding for quantum error correction. In Y. M. Chee, C. Li, S. Ling, H. Wang, and C. Xing, editors, *Coding and Cryptology: Second International Workshop, IWCC 2009, Proc.*, pages 259–273. Springer, Berlin, Heidelberg, 2009.

[31] N. Delfosse and G. Zémor. Quantum erasure-correcting codes and percolation on regular tilings of the hyperbolic plane. In *Information Theory Workshop (ITW), 2010 IEEE*, pages 1–5, Aug 2010.

[32] N. P. Breuckmann and B. M. Terhal. Constructions and noise threshold of hyperbolic surface codes. *IEEE Trans. on Inf. Th.*, 62(6):3731–3744, June 2016.

[33] N. P. Breuckmann, C. Vuillot, E. Campbell, A. Krishna, and B. M. Terhal. Hyperbolic and semi-hyperbolic surface codes for quantum storage. *Quantum Science and Technology*, 2(3):035007, 2017.

[34] L. Guth and A. Lubotzky. Quantum error correcting codes and 4-dimensional arithmetic hyperbolic manifolds. *Journal of Mathematical Physics*, 55(8):082202, 2014.

[35] J.-P. Tillich and G. Zémor. Quantum LDPC codes with positive rate and minimum distance proportional to $\sqrt{n}$. In *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, pages 799–803, Seoul, Korea, June 2009.

[36] J.-P. Tillich and G. Zémor. Quantum LDPC codes with positive rate and minimum distance proportional to the square root of the blocklength. *IEEE Transactions on Information Theory*, 60(2):1193–1202, 2014.

[37] A. A. Kovalev and L. P. Pryadko. Quantum Kronecker sum-product low-density parity-check codes with finite rate. *Phys. Rev. A*, 88:012311, July 2013.

[38] Weilei Zeng and Leonid P. Pryadko. Higher-dimensional quantum hypergraph-product codes with finite rates. *Phys. Rev. Lett.*, 122:230501, Jun 2019.

[39] Alain Couvreur, Nicolas Delfosse, and Gilles Zémor. A construction of quantum ldpc codes from cayley graphs. *IEEE transactions on information theory*, 59(9):6087–6098, 2013.

[40] Sergey Bravyi and Matthew B Hastings. Homological product codes. In *Proceedings of the forty-sixth annual ACM symposium on Theory of computing*, pages 273–282, New York, 2014.

[41] B. Audoux. An application of Khovanov homology to quantum codes. *Ann. Inst. Henri Poincare*, 1:185223, 2014.

[42] B. Audoux and A. Couvreur. On tensor products of CSS codes. *Ann. Inst. Henri Poincaré Comb. Phys. Interact.*, 6:239–287, 2019.

[43] M. B. Hastings. Quantum codes from high-dimensional manifolds. unpublished, 2016.

[44] Mathew B Hastings. Weight reduction for quantum codes. *Quantum Information & Computation*, 17(15-16):1307–1334, 2017.

[45] Matthew B. Hastings, Jeongwan Haah, and Ryan O'Donnell. Fiber bundle codes: Breaking the $N^{1/2}$ polylog(N) barrier for quantum LDPC codes. unpublished, 2020.

[46] Tomasz Kaczynski, Konstantin Mischaikow, and Marian Mrozek. Computing homology. *Homology, Homotopy and Applications*, 5:233–256, 2003.

[47] Tomasz Kaczynski, Konstantin Mischaikow, and Marian Mrozek. *Computational homology*, volume 157 of *Applied Mathematical Sciences*. Springer-Verlag, New York, 2004.

[48] Aldo Gonzalez-Lorenzo, Alexandra Bac, Jean-Luc Mari, and Pedro Real. Two Measures for the Homology Groups of Binary Volumes. In Springer, editor, *19th IAPR International Conference on Discrete Geometry for Computer Imagery (DGCI 2016)*, volume 9647 of *Discrete Geometry for Computer Imagery*, pages 154–165, Nantes, France, April 2016.

[49] Tamal K. Dey, Tianqi Li, and Yusu Wang. Efficient algorithms for computing a minimal homology basis. In Michael A. Bender, Martín Farach-Colton, and Miguel A. Mosteiro, editors, *LATIN 2018: Theoretical Informatics*, pages 376–398, Cham, 2018. Springer International Publishing.

[50] Stephen S. Bullock and Gavin K. Brennen. Qudit surface codes and gauge theory with finite cyclic groups. *Journal of Physics A: Mathematical and Theoretical*, 40(13):3481, 2007.

[51] A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54(2):1098–1105, Aug 1996.

[52] A. M. Steane. Simple quantum error-correcting codes. *Phys. Rev. A*, 54:4741–4751, 1996.

[53] H. Künneth. Ueber die bettische zahlen einer produktmannigfaltigkeit. *Math. Ann.*, 90:65–85, 1923.

[54] H. Künneth. Ueber die torsionszahlen von produktmannigfaltigkeiten. *Math. Ann.*, 91:125–134, 1923.

[55] Weilei Zeng and Leonid P Pryadko. K\" unneth theorem with a distance. *arXiv preprint arXiv:2007.12152*, 2020.

[56] C. Wang, J. Harrington, and J. Preskill. Confinement-Higgs transition in a disordered gauge theory and the accuracy threshold for quantum memory. *Annals of Physics*, 303(1):31 – 58, 2003.

[57] Ruben S. Andrist. *Understanding topological quantum error-correction codes using classical spin models*. PhD thesis, ETH Zürich, Dep. of Physics, ETH Zürich, 2012.

[58] Y. Fujiwara. Ability of stabilizer quantum error correction to protect itself from its own imperfection. *Phys. Rev. A*, 90:062304, Dec 2014.

[59] A. Ashikhmin, C. Y. Lai, and T. A. Brun. Robust quantum error syndrome extraction by classical coding. In *2014 IEEE International Symposium on Information Theory*, pages 546–550, Honolulu, Hawaii, 2014.

[60] A. Ashikhmin, C. Y. Lai, and T. A. Brun. Correction of data and syndrome errors by stabilizer codes. In *2016 IEEE International Symposium on Information Theory (ISIT)*, pages 2274–2278, Barcelona, Spain, 2016.

[61] Earl T. Campbell. A theory of single-shot error correction for adversarial noise. *Quantum Science and Technology*, 4:025006, 2019.

[62] Lev Ioffe and Marc Mézard. Asymmetric quantum error-correcting codes. *Phys. Rev. A*, 75:032345, 2007.

[63] Z. W. E. Evans, A. M. Stephens, J. H. Cole, and L. C. L. Hollenberg. Error correction optimisation in the presence of x/z asymmetry. arXiv:0709.3875, 2007.

[64] A. M. Stephens, Z. W. E. Evans, S. J. Devitt, and L. C. L. Hollenberg. Asymmetric quantum error correction via code conversion. *Phys. Rev. A*, 77:062335, 2008.

[65] P. Aliferis and J. Preskill. Fault-tolerant quantum computation against biased noise. *Phys. Rev. A*, 78:052331, 2008.

[66] P. K. Sarvepalli, A. Klappenecker, and M. Rötteler. Asymmetric quantum codes: constructions, bounds and performance. *Proc. R. Soc. A*, 465:1645–72, 2009.

[67] D. K. Tuckett, S. D. Bartlett, and S. T. Flammia. Ultrahigh error threshold for surface codes with biased noise. *Phys. Rev. Lett.*, 120:050505, Jan 2018.

[68] Charles A. Weibel. *An introduction to homological algebra*, volume 38 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1994.

[69] Kasper Duivenvoorden, Nikolas P. Breuckmann, and Barbara M. Terhal. Renormalization group decoder for a four-dimensional toric code. unpublished.

[70] Héctor Bombín. Single-shot fault-tolerant quantum error correction. *Phys. Rev. X*, 5:031043, Sep 2015.

[71] Benjamin J. Brown, Naomi H. Nickerson, and Dan E. Browne. Fault-tolerant error correction with the gauge color code. *Nature Communications*, 7:12302, 2016.

[72] David S. Wang, Austin G. Fowler, and Lloyd C. L. Hollenberg. Surface code quantum computing with error rates over 1%. *Phys. Rev. A*, 83:020302, Feb 2011.

[73] A. J. Landahl, J. T. Anderson, and P. R. Rice. Fault-tolerant quantum computing with color codes. Presented at QIP 2012, December 12 to December 16, 2011.

[74] G. D. Forney, M. Grassl, and S. Guha. Convolutional and tail-biting quantum error-correcting codes. *IEEE Transactions on Information Theory*, 53(3):865–880, 2007.

[75] Andrew J. Viterbi. Error bounds for convolutional codes and an asymptotically optimum decoding algorithm. *IEEE Transactions on Information Theory*, 13:260–269, 1967.

[76] Rolf Johannesson and Kamil Sh Zigangirov. *Fundamentals of convolutional coding*, volume 15. John Wiley & Sons, 2015.

[77] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 1981.

[78] E. M. Rains and N. J. A. Sloane. Self-dual codes. In V. S. Pless and. W. C. Huffman, editor, *Handbook of coding theory*, volume I, pages 177–294. North-Holland, Amsterdam, 1998.

[79] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli. Nonbinary stabilizer codes over finite fields. *IEEE Trans. Info. Th.*, 52(11):4892–4914, Nov 2006.

[80] Yun Fan and Liang Zgang. Galois self-dual constacyclic codes. *Designs, Codes and Cryptography*, 84:473–492, 2017.

[81] A. Ashikhmin and E. Knill. Nonbinary quantum stabilizer codes. *IEEE Trans. Info. Th.*, 47(7):3065–3072, Nov 2001.

[82] Daniel Gottesman. Stabilizer codes with prime power qudits. Invited talk at QEC 2014 (ETH Zurich), 2014.

[83] David Poulin. Stabilizer formalism for operator quantum error correction. *Phys. Rev. Lett.*, 95:230504, Dec 2005.

[84] Dave Bacon. Operator quantum error-correcting subsystems for self-correcting quantum memories. *Phys. Rev. A*, 73:012340, Jan 2006.

[85] Muyuan Li and Theodore J. Yoder. A numerical study of Bravyi-Bacon-Shor and subsystem hypergraph product codes. unpublished, 2020.

[86] P. W. Shor. Fault-tolerant quantum computation. In *Proc. 37th Ann. Symp. on Fundamentals of Comp. Sci.*, pages 56–65, Los Alamitos, 1996. IEEE, IEEE Comp. Soc. Press.

[87] Muyuan Li, Daniel Miller, Michael Newman, Yukai Wu, and Kenneth R. Brown. 2-D compass codes. unpublished, 2018.

[88] Theodore J. Yoder. Optimal quantum subsystem codes in 2-dimensions. unpublished, 2019.

[89] John Napp and John Preskill. Optimal Bacon-Shor codes. *Quant. Inf. & Comp.*, Vol.13 2013:0490–0510, 2013.

[90] E. Prange. The use of information sets in decoding cyclic codes. *Information Theory, IRE Transactions on*, 8(5):5–9, 1962.

[91] L. O. Chua and L. Yang. Cellular neural networks: theory. *IEEE Transactions on Circuits and Systems*, 35(10):1257–1272, 1988.

[92] I. Dumer, A. A. Kovalev, and L. P. Pryadko. Distance verification for classical and quantum LDPC codes. *IEEE Trans. Inf. Th.*, 63(7):4675–4686, July 2017.

[93] S. T. Hedetniemi. Homomorphisms of graphs and automata. Technical Report 03105-44-T, University of Michigan, (1966).

[94] S. T. Hedetniemi. *Homomorphisms of graphs and automata*. PhD thesis, The University of Michigan, 1966.

[95] Yaroslav Shitov. Counterexamples to Hedetniemi's conjecture. *Annals of Mathematics*, 190(2):663–667, 2019.

[96] Gil Kalai. A sensation in the morning news—Yaroslav Shitov: Counterexamples to Hedetniemi's conjecture. *Combinatorics and More*, 2019.

[97] Xuding Zhu. Relatively small counterexamples to Hedetniemi's conjecture. *Journal of Combinatorial Theory, Series B*, 146:141 – 150, 2021.

[98] A. A. Frolov and V. V. Zyablov. Bounds on the minimum code distance for nonbinary codes based on bipartite graphs. *Problems of Information Transmission*, 47:327–341, 2011.

[99] A. Frolov. An upper bound on the minimum distance of LDPC codes over GF(q). In *2015 IEEE International Symposium on Information Theory (ISIT)*, pages 2885–2888, Hong Kong, 2015.

[100] N. P. Breuckmann, K. Duivenvoorden, D. Michels, and B. M. Terhal. Local decoders for the 2D and 4D toric code. *Quantum Inf. Comput.*, 17:0181, 2017.

[101] Tommaso Pacini. Extremal length in higher dimensions and complex systolic inequalities. *The Journal of Geometric Analysis*, pages 1–21, 2020.

[102] James Pierpont. Area of curved surfaces. *Transactions of the American Mathematical Society*, 7:489–498, 1906.

[103] Yi Jiang, Alexei A. Kovalev, Weilei Zeng, and Leonid P. Pryadko. Quantum codes over $\mathbb{Z}_q$ and q-state Potts models. unpublished, 2020.

[104] D. Gottesman. The Heisenberg representation of quantum computers. In S. P. Corney, R. Delbourgo, and P. D. Jarvis, editors, *Group22: Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics*, pages 32–43, Cambridge,

MA, 1998. International Press. Expanded version of a plenary speech at the 1998 International Conference on Group Theoretic Methods in Physics.

[105] Vladimir Sidorenko and V Zyablov. Decoding of convolutional codes using a syndrome trellis. *IEEE Transactions on Information Theory*, 40(5):1663–1666, 1994.

[106] Emilie Pelchat and David Poulin. Degenerate Viterbi decoding. *IEEE Trans. Information Theory*, 59(6):3915–3921, 2013.

[107] Christopher Chamberland and Michael E. Beverland. Flag fault-tolerant error correction with arbitrary distance codes. *Quantum*, 2:53, 2018.

[108] Anirudh Krishna and David Poulin. Fault-tolerant gates on hypergraph product codes. *arXiv preprint arXiv:1909.07424*, 2019.

[109] Tomas Jochym-O'Connor. Fault-tolerant gates via homological product codes. *Quantum*, 3:120, 2019.