Research Statement

Tefjol Pllaha

My research interests span across mathematics, computer science, and engineering. I have worked on algebraic coding theory [11, 12, 21, 25], quantum computation [22, 27, 29, 30], wireless communications [19, 26, 28, 36–38], and online privacy and security [1–5].

A portion of my PhD work is described in Sections 1 and 2.1. Section 2.2, although through the lenses of quantum computation, is in many ways a follow-up work. Section 3 describes my work in wireless communications. Section 4 describes the use of quantum computation in improving security and privacy of distributed data centers, whereas Section 5 deals with quantum error-correction. Finally, Section 6 describes two projects with undergraduate students.

The intent of this statement is to describe my current research interests in a broader sense. For more details about any of the research directions, feel free to email me at `tefjol.pllaha@unl.edu`.

1 Algebraic Coding Theory

Coding Theory deals with erroneously transmitted data over a noisy channel. Eliminating the noise is typically not an option. In fact the only efficient option is to make the data noise-proof, and this is done by adding redundancy. Coding Theory keeps under control the cost of the added redundancy, and this is achieved by efficient coding tools that also allow efficient decoding algorithms. Classically, a code $\mathcal{C}$ of length n is an additive subgroup of $\mathbb{F}_2^n$. The binary field $\mathbb{F}_2$ is the alphabet, and thus $\mathcal{C}$ is a binary code. Elements of $\mathcal{C}$ are called codewords. A code is endowed with the Hamming distance, which counts the number of coordinates in which two codewords differ.

Algebraic Coding Theory considers codes with additional structure. The alphabet is typically a finite field $\mathbb{F}_q$, and a code is an $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$, called a linear code. For a linear code we can talk about the Hamming weight of a codeword as the Hamming distance from the all-zero codeword. In other words, the Hamming weight counts the number of nonzero coordinates of a codeword. The main invariant of a code is the minimum distance — it characterizes the error-correcting capabilities of the code. Therefore, the goal is to find codes with large minimum distance while keeping the size of the code under control. The advantage of linear codes is that the minimum distance coincides with the minimum weight.

One can generalize the idea even further. The alphabet can be taken to be a finite left (or right) R-module A, where R is a finite ring. In this case, a linear code is just a left submodule of A^n. The first step toward this generalization is to take $A := \mathbb{Z}/d\mathbb{Z}$ viewed as a module over itself. Hence, linear codes over rings are an interesting special case of codes over modules. Another interesting special case is to consider field extensions E/F. In this context, the alphabet is E and codes consist of F-linear subspaces of E^n. In the case $\mathbb{F}_{p^n}/\mathbb{F}_p$ we get the so-called additive codes. Not only do they form an important class of codes on their own, but they also link with Quantum Information Theory and Quantum Error-Correcting Codes when $n = 2$. These generalizations are not merely a mathematical wonderment, but instead, they provide rather sophisticated tools for creating record-breaking codes.

An isometry is intended to capture the sameness of two codes. Thus, we would want an isometry to preserve the algebraic structure of the code as well as the weight function $\omega : A^n \to \mathbb{Q}$ with which the code is endowed. Along with the Hamming weight, other important weights include the homogeneous weight and the Lee weight. In [20], J. F. MacWilliams completely characterized isometries of binary linear codes with respect to the Hamming weight. It turned

out that the classification of codes is strongly connected to so-called **Frobenius** alphabets [17] and their rich character-theoretic duality [11, 39, 40].

Finite Frobenius rings are very close to finite fields [9], and similarly, finite Frobenius modules and bimodules are very similar to vector spaces [16, 24]. In fact, these algebraic structures can be characterized as those alphabets for which the work of MacWilliams holds true. The main insight here is Fourier analysis on finite abelian groups.

1.1 Equivalence of Codes

A notion of sameness is required for any structure. Consider block codes over some finite module alphabet endowed with a weight function ω. As mentioned, for a notion of sameness one would want the algebraic structure as well as the error-correcting capabilities to be preserved. Thus two codes $\mathcal{C}, \mathcal{C}'$ are "the same" if there exists an isomorphism between the two that also preserves the weight. We will refer to such a map as ω-**isometry** and to the codes as **isometric**. The latter may be decorated with adjectives that display properties of the weight. These ideas can also be approached with a categorical language, as in [6] and references therein, where objects are block codes and morphisms are the linear maps that don't increase the weight.

With a notion of sameness in place one considers the respective equivalence classes and seeks for canonical representatives. The first step in doing so is to understand the structure of ω-isometries, which it turns out to be a highly nontrivial task. One gains intuition by considering the (typically easy) extremal case $\mathcal{C} = A^n$. Namely, what is the structure of an ω-isometry $f : A^n \longrightarrow A^n$? This leads to two immediate followup questions. Is the structure of an ω-isometry $f : \mathcal{C} \subsetneq A^n \longrightarrow A^n$ the same as the extremal case for any code $\mathcal{C}$? And if not, how different is the structure? The former was first asked and answered affirmatively by MacWilliams [20] for binary linear codes with respect to the Hamming weight. Further generalizations led to MacWilliams Extension Theorem and the Extension Property of an alphabet [40]. However, the answer is not always affirmative; see [24, Chapter 5]. This fact, along with ideas discussed in [10], led Jay Wood to the notions of **isometry groups** [41]. The key insight is to think of a code as a set of **messages** M embedded in A^n via a linear injective map Λ, called **encoding**. Then one studies isometries of the code $\mathcal{C} := \Lambda(M)$ via automorphisms of the **information module** M. More specifically, given a code $\mathcal{C}$ along with an information module M and encoding Λ, one defines

$$\mathrm{Iso}_\omega(\mathcal{C}) = \{f \in \mathrm{Aut}(M) \mid \omega(\Lambda(f(m))) = \omega(\Lambda(m)) \text{ for all } m \in M\}. \tag{1}$$

Then, inside $\mathrm{Iso}_\omega(\mathcal{C})$ one identifies the subgroup $\mathrm{Mon}_\omega(\mathcal{C})$ of all automorphisms that are restrictions of ω-isometries of A^n. The terminology here stems from the fact that isometries of A^n are monomial maps. Whenever MacWilliams Extension Theorem is true the two groups are the same. Otherwise one wonders how big the gap could be and what subgroups of $\mathrm{Aut}(M)$ can be realized as isometry groups. It turns out that the gap can be as big as possible [41]. These considerations are closely related with the symmetries of the weight ω and tools from group theory, e.g., the *closure* of a group, play a central role.

2 Quantum Computation

Quantum computation emerged in early 80s when the first ideas of quantum computers started to develop. Ever since, the field has attracted interests from engineers, physicists, and mathematicians.

A quantum mechanical system is mathematically described by a two dimensional complex Hilbert space (typically taken to be $\mathbb{C}^2$) called quantum bit or qubit, and its time evolution

is described by unitary operators. In this computational model, a quantum circuit consists of a sequence of operations each of which is either a **quantum gate**, characterized by a unitary matrix, or a **quantum measurement**, characterized by a Hermitian matrix (i.e., an **observable**) [23]. Examples of simple but yet important gates are the **bit flip** and **phase flip** gates. The collection of these gates forms the well-known **Heisenberg-Weyl** group, which in turn plays a crucial role in quantum error-correction (QEC) [7, 32].

The Heisenberg-Weyl group, in fact, plays the role of an **error group** in quantum error-correction. The commutativity structure of this group can be described in terms of binary symplectic geometry. A large and useful class of QEC codes can be viewed as complex vector spaces fixed by **stabilizers**, that is, by projective abelian subgroups of the Heisenberg-Weyl group [13]. In this compact description, a stabilizer is precisely a self-orthogonal (totally isotropic) subspace, and thus much of the analysis can be done in finite arithmetic rather than complex/continuous arithmetic.

The computational model above can be generalized to **qudits**, which would be described by a d-dimensional complex Hilbert space, and corresponding generalized gates, measurements, and Heisenberg-Weyl group. Interestingly, it turns out that the natural finite arithmetic that realises the generalized Heisenberg-Weyl group as an error group is that of a finite Frobenius ring, and the associated symplectic geometry. We exploit this exciting connection to study generalized stabilizers and corresponding QEC codes in [12]. With the correct set-up, we show that, as expected, the error-correcting capabilities are determined by the Frobenius alphabet.

2.1 The Clifford Group

The **Clifford group** is defined as the automorphism group of the Heisenberg-Weyl group, and it turns out to coincide with the normalizer of the latter. Thus, an automorphism acts by conjugation. This simple observation is crucial in QEC because conjugation is well-behaved on stabilizers. Exploiting the connection with symplectic geometry, elements of the Clifford group (which are huge complex matrices) can be identified with binary (or d-ary in the generalized case) symplectic matrices. If $\mathcal{C}$ is a symplectic self-orthogonal subspace, in analogy with (1), we can define two isometry groups:

$$\begin{aligned} \mathrm{Mon}_{\mathrm{SL}}(\mathcal{C}) &:= \{f \in \mathrm{Aut}(\mathcal{C}) \mid f \text{ is the restriction of a symplectic monomial map}\}, \\ \mathrm{Symp}(\mathcal{C}) &:= \{f \in \mathrm{Aut}(\mathcal{C}) \mid f \text{ is a symplectic isometry}\}. \end{aligned} \tag{2}$$

In [25, Example 4.19] we give an explicit example that shows $\mathrm{Mon}_{\mathrm{SL}}(\mathcal{C}) \subsetneq \mathrm{Symp}(\mathcal{C})$. Moreover, using ideas from [41] and taking extra care of self-orthogonality, we show that this gap can be as big as possible. Namely, given two groups $H_1 \subsetneq H_2$, that satisfy some necessary conditions (see [25, Prop. 4.11]), then there exists a symplectic self-orthogonal subspace $\mathcal{C}$ such that $H_1 = \mathrm{Mon}_{\mathrm{SL}}(\mathcal{C})$ and $H_2 = \mathrm{Symp}(\mathcal{C})$.

It is worth mentioning that, in the background, we are dealing with stabilizers and their fixed spaces, which have their own notion of equivalence. Interestingly, all this work is strongly connected with [11] in which we also studied isometries of codes but in a classical setting.

2.2 The Clifford Hierarchy

In 1999, Gottesman and Chuang demonstrated that universal quantum computing can be performed just by using the quantum teleportation protocol if one has access to certain standard resources — Bell-state preparation, Bell-basis measurements, and arbitrary single-qubit rotations [15]. They defined the **Clifford hierarchy** as part of their proof, and this has proven

to be a useful characterization of a large set of unitary operations both in theory and practice. In fact, in their teleportation model of computation, the level of a unitary in the hierarchy can be interpreted as a measure of complexity of implementing it. Furthermore, this model is closely related to the currently widespread scheme of distilling "magic" states and injecting them via teleportation-like methods in order to fault-tolerantly execute unitary operations on qubits encoded in a quantum error-correcting code. By definition, the Heisenberg-Weyl and Clifford groups are the first and second level of the hierarchy respectively. Then the kth level is defined recursively as those unitaries that conjugate the Heisenberg-Weyl group to the $(k-1)$st level.

The structure of the Clifford hierarchy remains still unknown. In [27] we make significant progress towards a complete characterization. We focus primarily on the third level and show that every third level element is supported on a maximal abelian group of the Heisenberg-Weyl group. Since the Clifford group is a subset of the third level, the result still applies and this can be leveraged in circuit design and significant complexity reduction. For this we use the notion of the **support** of a unitary matrix. First, the set of Hermitian matrices $\mathcal{E}_N$ ($N = 2^m$, where m is the number of qubits) in the Heisenberg-Weyl group $\mathcal{HW}_N$ forms an orthonormal basis for the vectors space $\mathcal{M}_N(\mathbb{C})$ of $N \times N$ complex matrices with respect to the Hermitian inner product

$$\langle \mathbf{M} \,|\, \mathbf{N} \rangle := \frac{1}{N} \mathrm{Tr}(\mathbf{M}^\dagger \mathbf{N}). \tag{3}$$

Thus, any matrix $\mathbf{M} \in \mathcal{M}_N(\mathbb{C})$ is a linear combination of elements in $\mathcal{E}_N$. The support of $\mathbf{M}$ consists of those basis matrices that show up on the linear combination, namely,

$$\mathrm{supp}(\mathbf{M}) := \{\mathbf{E} \in \mathcal{E}_N \mid \langle \mathbf{E} \,|\, \mathbf{M} \rangle \neq 0\}. \tag{4}$$

We show in [27] that, rather remarkably, the support of Clifford matrices is *always* a commutative subgroup of $\mathcal{HW}_N$, that is, a stabilizer. We also show that, up to a rotation, the same holds true for the third level of the Clifford hierarchy. This in turn implies several previously known structural results, such as the so-called semi-Clifford conjecture.

Finding the support of a matrix, while straightforward, is computationally expensive. In [30] we give a fast algorithm for computing the support of a Clifford matrix. For this we use a novel graphical approach on the binary symplectic group $\mathrm{Sp}(\mathbb{F}_2; 2m)$. We are currently working on implementing this new approach to achieve fault-tolerant quantum computation as well as exploring efficient algorithms for higher levels of the Clifford hierarchy (especially third level).

3 Fifth Generation (5G) Wireless Communications

One of the challenges/promises of 5G wireless communication is to enable massive machine-type communications (mMTC) in the Internet of Things (IoT), in which a massive number of low-cost devices sporadically and randomly access the network. In this scenario, users are assigned a unique **signature** sequence which they transmit whenever active. A twin use-case is unsourced multiple access where a large number of messages is transmitted infrequently. Polyanskiy [31] proposed a framework in which communication occurs in blocks of N channel uses, and the task of a receiver is to identify correctly L active users (messages) out of 2^B with one regime of interest being $N = 30,000$, $L = 250$, and $B = 100$.

The mathematical model of this use-case translates as follows. An active user u_ℓ transmits its unique signature $\mathbf{s}_{u_\ell}$. But, since there would be multiple simultaneous active users, the receiver will receive a superposition of these signatures, perturbed by some Gaussian noise, that is

$$\mathbf{s} = \left(\sum_{\ell=1}^{L} c_\ell \mathbf{s}_{u_\ell} \right) + \mathbf{n}, \quad c_\ell \in \mathbb{C}, \mathbf{n} \in \mathbb{C}^N. \tag{5}$$

The task is to discover the active users, that is, determine $\{u_1, \dots, u_L\}$ given $\mathbf{s}$.

Given the massive number of to-be-supported (to-be-encoded) users (messages), the design criteria are fundamentally different, and one simply cannot rely on classical multiple-access channel (MAC) solutions. For instance, interference is unavoidable since it is impossible to have orthogonal signatures/codewords. Thus the challenge becomes to design highly structured codebooks of large cardinality along with a reliable and low-complexity decoding algorithm. The performance of a collection of signatures $\mathcal{S} = \{\mathbf{s}_i\}_{i=1}^M \subset \mathbb{C}^N$ is governed by the **worst-case coherence** $\mu(\mathcal{S}) = \max_{i \neq j} |\mathbf{s}_i^\dagger \mathbf{s}_j|$, or equivalently by the **minimum chordal distance** $\delta_c(\mathcal{S}) = \sqrt{1 - \mu^2(\mathcal{S})}$. Thus, we are seeking for a large number of unit vectors in $\mathbb{C}^N$ that are sufficiently separated, and in the background we are dealing with Grassmannian packings.

In [29] we introduce Binary Subspace Chirps, as a codebook of complex Grassmannian lines of large cardinality and good distance properties, which makes them good candidates for mMTC. This claim is backed up by the fact that the codebook is a natural extension of Binary Chirps [18], which have been proven very useful in various applications. Interestingly, the codebook can be characterized as a collection of Clifford matrices (discussed in Section 2). We fully exploit this connection in [28] to construct a fast and reliable decoding algorithm in a multi-user scenario. What remains to be seen is the reliability and stability of the algorithm in a massive setting as proposed by Polyanskiy.

As mentioned, the devices used in mMTC are low-cost. These are typically simple sensors with one transmit antenna and very little power available. However, there are important scenarios (such as industrial automation, intelligent transportation, and remote healthcare (surgery), to name a few) where Ultra-Reliable Low-Latency Communication (URLLC) is needed. It is obvious that errors in these applications can be fatal, and that is why extra power and complexity is traded for ultra reliability. In [38] we consider the case where users/devices have multiple transmit antennas and show that reliability can be improved significantly. Although this is a vastly different scenario from mMTC, our main insight still comes from there. Recall that in that case the devices had one transmit antenna and would transmit a sequence/signature which we modeled as a Grassmannian line. We model the multi-antenna transmission as a Grassmannian subspace of dimension equal to the number of transmit antennas. Namely, if the active user is transmitting with n_t antennas and the receiver receives with n_r antennas then (5) reads as

$$\mathbf{s} = \left(\sum_{\ell=1}^{L} \mathbf{s}_{u_\ell} \mathbf{c}_\ell \right) + \mathbf{n}, \quad \mathbf{c}_\ell \in \mathbb{C}^{n_t \times n_r}, \ \mathbf{s}_{u_\ell} \in \mathbb{C}^{N \times n_t}, \ \mathbf{n} \in \mathbb{C}^{N \times n_r}. \tag{6}$$

The goal is again to recover the active users $\{u_1, \dots, u_L\}$ given $\mathbf{s}$, and additionally, design signatures that *guarantee* full recovery. Statistical analysis of this use-case motivates the following definition [38].

Definition 1. A signature code $\mathcal{C} \subset M_{N \times n_t}(\mathbb{C})$ is called **well-balanced** if for every $\mathbf{s}_i \in \mathcal{C}$ we have $\mathbf{s}_i^\dagger \mathbf{s}_j = c_{i,j} \mathbf{x}_{i,j}$, where $\mathbf{x}_{i,j}$ is an $n_t \times n_t$ unitary matrix and $c_{i,j}$ is a scalar. The signature code will be called ε-**well-balanced** if $|c_{i,i}| = 1/n_t$ and $|c_{i,j}| \leq \varepsilon$ for $i \neq j$.

This newly introduced notion can be thought of as a generalization of *mutually unbiased bases*. In fact, using this intuition, we provide an explicit construction, which we then test in simulations. The performance is precisely as expected and we gain orders of magnitude in reliability.

3.1 Modular Quantization for mMIMO Communication

Massive Multiple-Input Multiple-Output (mMIMO) with a very large number of antennas at the transmission station is one of the key components in the 5G New Radio (NR). This type of

communication relies on the availability of high channel state information (CSI) that is fed back from the user to the station. However, with the large number of antennas N_t at the station, the complexity of reliable feedback becomes prohibitively high. The complexity continues to grow exponentially in a multi-user scenario. Each of the U users has their own channel $\mathbf{h}_u \in \mathbb{C}^{N_t \times 1}$, and collectively there is a channel matrix $\mathbf{H} \in \mathbb{C}^{N_t \times U}$. The transmission station will send *to all the users*

$$\mathbf{y} = \mathbf{H}\,\mathbf{Z}\,\mathbf{x} + \mathbf{n},$$

where $\mathbf{x} \in \mathbb{C}^{U \times 1}$ is the vector of information, $\mathbf{n}$ represents noise, and $\mathbf{Z}$ is a (to-be) designed *beam* so that each user u receivers the intended information $\mathbf{x}_u \in \mathbb{C}$. The beam $\mathbf{Z}$ is formed (a.k.a, *beamforming*) using real-time CSI feedback information from each user. The *covariance matrix* (and its eigenvalue decomposition)

$$\mathbf{R} = \mathbf{h}\mathbf{h}^\dagger = \mathbf{U}\,\mathbf{\Lambda}\,\mathbf{U}^\dagger$$

is used to handle complexity. The matrix $\mathbf{\Sigma} = \mathrm{diag}(\sigma_j)$ of the singular values of $\sqrt{\mathbf{R}}$ is used for complexity reduction. The key idea is that instead of working with the CSI vector $\mathbf{h}_u$, one works with

$$\mathbf{c}_u = \mathbf{\Sigma}^{-1}\,\mathbf{U}^\dagger\,\mathbf{h}_u.$$

The order induced by $\mathbf{\Sigma}$ selects the K dominant eigenvectors $\mathbf{U}_K$, and $\mathbf{c}_u$ can be reliably approximated by $\mathbf{\Sigma}_K^{-1}\,\mathbf{U}_K^\dagger\,\mathbf{h}_u \in \mathbb{C}^{K \times 1}$. To proceed with low-complexity feedback, one uses equidistant points in the Grassmannian $\mathcal{G}_{\mathbb{C}}(K, 1)$ of desired granularity.

In [19], we propose a novel approach where the eigenvectors $\{\mathbf{u}_1, \ldots, \mathbf{u}_K\}$ are sequentially quantized (from the dominant to Kth dominant) with an *adaptive* granularity based both on dominance as well as on K. Simulations have shown that this approach yields considerable performance improvement. Further improvements can be achieved by using an orthonormalized version of $\mathbf{U}_K$ instead of $\mathbf{U}_K$ itself.

4 Security and Privacy with Quantum Resources

Online activity and digital footprints are increasing exponentially, and this comes along with significant risks. Luckily, there is also an increasing awareness, and tech companies are stepping up to address these issues. A step in the right direction is the introduction of anonymization and differential privacy. Another important step in the right direction are data protection laws.

In a typical online activity, there is a user that sends a request through a network to a server about certain information. The server recognizes the request and replies with the relevant information. In this scenario, there are two main risks: one from the user prospective and another from the server prospective. In the former, the user would want **privacy**, meaning that the information requested remains unknown to the server. Yet somehow, the server should be able to reply with the relevant information without knowing what information is being delivered. This is referred as Private Information Retrieval (PIR) and was first introduced in the seminal work [8]. Additionally, the user may want **anonymity**, meaning that the server doesn't know the identity of the user during the exchange. In the latter type of risk, the server (but also the user) would want **security**, meaning that the information delivered is robust against malicious third parties.

In recent years, PIR has gained renewed interest in the setting of distributed storage systems (DSSs) where the servers are storing possibly large files $x^i \in \mathbb{F}_q^{\beta \times k}, i = 1, \ldots, m$. To protect from data loss in the case of the failure of some number of servers, such systems commonly employ

either replication, where all servers store all files completely, or erasure-correcting codes, where each server stores specific linear combinations of symbols of each file, as depicted below. A $k \times n$ generator matrix $\mathbf{G}_{\mathcal{C}}$ of an $[n, k]$ error-correcting code $\mathcal{C}$ determines what linear combinations of symbols from each file are stored in each server.

$$\begin{matrix} \text{file } 1 \\ \\ \\ \\ \text{file } m \end{matrix} \begin{pmatrix} x_{1,1}^1 & \cdots & x_{1,k}^1 \\ \vdots & \ddots & \vdots \\ x_{\beta,1}^1 & \cdots & x_{\beta,k}^1 \\ \vdots & \vdots & \vdots \\ x_{1,1}^m & \cdots & x_{1,k}^m \\ \vdots & \ddots & \vdots \\ x_{\beta,1}^m & \cdots & x_{\beta,k}^m \end{pmatrix} \cdot \mathbf{G}_{\mathcal{C}} = \begin{pmatrix} y_{1,1}^1 & \cdots & y_{1,n}^1 \\ \vdots & \ddots & \vdots \\ y_{\beta,1}^1 & \cdots & y_{\beta,n}^1 \\ \vdots & \vdots & \vdots \\ y_{1,1}^m & \cdots & y_{1,n}^m \\ \vdots & \ddots & \vdots \\ y_{\beta,1}^m & \cdots & y_{\beta,n}^m \end{pmatrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \text{SERVER}_1 \end{matrix} \quad \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \text{SERVER}_n \end{matrix}$$

Not only is this new setting commercially important, but it is also mathematically challenging and interesting. There exist many PIR schemes for various scenarios, but most of them are not capacity-achieving in the sense that they are not the best possible. More importantly, in many cases the capacity is not even known.

We consider PIR in a scenario where servers share some quantum resources and use them collaboratively to improve the capacity. We refer to this scenario as quantum PIR (QPIR). This was first introduced and studied in [33,34] for replicated storage (meaning that every server stores a copy of each file). It should be stressed that replicated storages have a massive overhead in the sense that it is absolutely not necessary that each server stores a copy of each file. For this reason replicated storages are impractical and are substituted with coded (erasure-correcting) storages. In [1, 2] we construct a QPIR scheme for a coded storage. Additionally, the scheme allows even **colluding** servers (where some servers may exchange information as an attempt to threaten privacy). Using the stabilizer formalism [13], we generalized the scheme for distributed/coded storages in [3] and computed the capacity in [5].

4.1 A New Approach: N-Sum Protocol

This new approach leverages the extremely simple 2-sum protocol [33] to first construct an N-sum box, which we then further leverage in distributed computing [4]. It is worth pointing out immediately that the technical foundations of the N-sum box are not new, indeed the construction draws upon the well-understood stabilizer formalism in quantum coding theory, and most of the technical details of the generalization from 2-sum to N-sum are also contained in the works of Song and Hayashi on Quantum Private Information Retrieval. Nevertheless, the crystallization of the black-box abstraction holds significant promise for researchers in the classical information and coding theory domains. These researchers, though less acquainted with stabilizer codes and quantum coding theory, can still make valuable contributions to comprehending the fundamental boundaries of transmitter-side entanglement-assisted distributed classical computation over quantum multiple access (QMAC) networks. This is achieved through the utilization of the aforementioned classical abstraction, which effectively conceals the intricate details of the underlying quantum circuitry. For example, wireless researchers with little background in quantum codes may recognize the N-sum box as the familiar MIMO MAC setting illustrated via an example in Figure 1. The main distinctions from the multiple antenna wireless setting are 1) that the channel is deterministic (noise-free), defined over a finite field ($\mathbb{F}_q$) rather than complex numbers, and 2) that instead of being generated randomly by nature, the channel matrix can be freely designed as

long as it satisfies some *weak* necessary conditions. This is because it is shown in this work that feasible N-sum box transfer functions are precisely those matrices $\mathbf{M} \in \mathbb{F}_q^{N\times 2N}$ that satisfy the said conditions. Thus, from a wireless perspective, the problem of coding for the QMAC becomes conceptually equivalent to that of designing a coding scheme as well as the channel matrix for a MIMO MAC subject to given structural constraints imposed by the N-sum box abstraction, such that the resulting MIMO MAC is able to efficiently achieve the desired linear computation 'over-the-air' (actually, through quantum entanglement). The efficiency gained by 'over-the-air' computation in this (constrained) MIMO MAC translates into superdense coding gain over the QMAC.

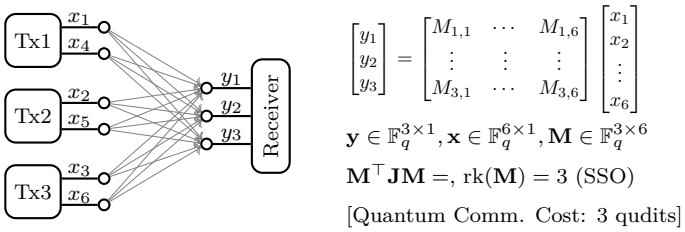

Figure 1: The N-sum box is illustrated as a MIMO MAC for $N = 3$.

The N-sum box is intended to be useful primarily as a tool for exploring the information-theoretic capacity of $\mathbb{F}_q$-linear classical computations over an ideal QMAC, with the potential to shed new light into the fundamental limitations of superdense coding and quantum entanglement. As with other tools that information theorists have at their disposal, it is difficult to predict in advance if the N-sum box abstraction will turn out to be sufficient to construct capacity achieving schemes. Indeed the linear computation capacity of a MAC is a challenging problem even in the classical setting, especially for *vector* linear computations. Nevertheless, we are cautiously optimistic that the stabilizer-based construction exhausts the scope of the N-sum box functionality for $\mathbb{F}_q$-linear computations. The optimistic outlook is supported by our prior works on capacity of QPIR [1,5] where N-sum boxes have been implicitly employed for capacity-achieving schemes, as well as a recent follow-up work that utilizes the N-sum-box abstraction from this work, to find the capacity of sum-computation over the QMAC [42].

Last but not the least, even when an exact capacity characterization is beyond reach, a fruitful strategy is to utilize the N-sum box to design the best possible schemes allowed by the abstraction. In general the constraints of the abstraction may lead to entirely new schemes. However, certain applications of interest, of which QPIR is a prime example, have classical solutions with specialized structures that naturally resonate with the constraints of the N-sum boxes. For such applications, it can be particularly insightful to find ways to efficiently *quantumize* the classical solutions, leading not only to good quantum coding schemes but also a better understanding of the role of these constraints for linear computations. Notably, we introduced such quantumization in [1] by blending the existing classical schemes with the 2-sum protocol. In this work, to further illustrate this aspect, we provide another instance by quantumizing classical cross-subspace alignment (CSA) codes into QCSA codes. CSA codes have been used in a variety of schemes ranging from PIR to secure distributed batch matrix multiplication (SDBMM). Therefore, QCSA codes naturally open the door for the general quantum MDS-coded PIR setting as well as quantum SDBMM.

5 Quantum Low-Density Parity-Check Codes

Since the discovery of the first quantum error correction code [32], there has been tremendous progress in code design. Many of the existing quantum codes leverage the vast existing literature in classical coding theory. Low-density parity-check (LDPC) codes are well-established in classical coding theory. Their quantum analogues, quantum LDPC (QLDPC) codes, gained popularity due to Gottesman's breakthrough discovery [14], showing that constant overhead can be achieved with constant encoding rate. For this reason, QLDPC codes are current candidates for realizing scalable fault-tolerant quantum computation. Like their classical counterparts, QLDPC codes are amenable to low-complexity iterative decoding algorithms, such as syndrome-based iterative decoding.

An important class of stabilizer codes are the Calderbank-Shor-Steane (CSS) codes [7, 35], defined by a pair of classical linear codes $\mathcal{C}_{\mathsf{X}}, \mathcal{C}_{\mathsf{Z}} \subset \mathbb{F}_q^n$ such that $\mathcal{C}_{\mathsf{X}}^{\perp} \subset \mathcal{C}_{\mathsf{Z}}$. This condition forces two respective parity check matrices H_{X} and H_{Z} to satisfy $H_{\mathsf{Z}} H_{\mathsf{X}}^T = 0$ and thus the matrix

$$H = \left(\begin{array}{c|c} H_{\mathsf{X}} & 0 \\ 0 & H_{\mathsf{Z}} \end{array}\right)$$

satisfies the necessary condition $H_{\mathsf{X}} H_{\mathsf{Z}}^T + H_{\mathsf{Z}} H_{\mathsf{X}}^T = 0$, and it defines a stabilizer code. A Pauli error acting on n qubits can be represented as $e = (e_{\mathsf{X}}, e_{\mathsf{Z}})$. The corresponding error syndrome is

$$\sigma_e = (\sigma_{\mathsf{X}}, \sigma_{\mathsf{Z}}) = \left(\begin{array}{c|c} H_{\mathsf{X}} & 0 \\ 0 & H_{\mathsf{Z}} \end{array}\right) \odot e = (H_{\mathsf{Z}} e_{\mathsf{X}}^T, H_{\mathsf{X}} e_{\mathsf{Z}}^T).$$

The goal of a syndrome-based decoder is to estimate an error $\hat{e}$ whose syndrome $\sigma_{\hat{e}}$ matches the input syndrome σ_e.

While most work on decoder failure of QLDPC codes has focused on defining and identifying trapping sets (that is, structures that force the decoder to diverge) of QLDPC codes, less have characterized problematic graphical structures in trapping sets. Our work [22] aims to identify classes of said structures.

Definition 2. An (a, b)-*absorbing set* $\mathcal{A}$ in the Tanner graph $\mathcal{G}$ of the code $\mathcal{C}$ is a subset of variable nodes such that $|\mathcal{A}| = a$, there are b odd degree vertices in the induced subgraph $W_{\mathcal{A}}$, and every variable node $v \in \mathcal{A}$ has more even degree than odd degree neighbors in $\mathcal{G}_{\mathcal{A}}$.

We show that for absorbing sets with $b > 0$, that is, when there exists at least one odd degree node, the decoder will always get trapped. The more interesting case is when $b = 0$, and we connect this case with *degenerate errors*, which constitute a unique feature of quantum coding.

6 Undergraduate Research

By its very nature, my research is highly accessible for a wide range of undergraduate students. Most of my intended projects require little to no background which in turn allows students to tackle core problems almost immediately. Additionally, part of my research deals with real life applications, and this can be attractive to students with different research interests (e.g., pure math versus applied math, algebra versus combinatorics). As usual, to come up with a solution to a real life problem one would not only need to "construct" a solution but also implement it. This is a green light for students that would rather prefer a more computational or programming approach, as well as for interdisciplinary research with computer science majors and/or engineering majors.

In Summer 2020, I supervised a research project for Kalle Volanto at Aalto University, who at that time was an electrical engineering senior, while also working for a math major. The problem we tackled was at a first glance very theoretical in nature – decomposition of certain binary symplectic matrices, uniqueness of the decomposition and other related considerations – which in turn has important connections with quantum computation. Despite this, the problem in hand can be translated to simple graph theory language which is very accessible and visual. This helped in gaining intuition, and eventually we not only solved the problem but also implemented a fast algorithm [30].

In Summer 2022, I supervised a research project for Kolton O'Neal at UNL, who at the time was a freshman math major. The problem we studied involved distributed matrix multiplication. When the multiplications are carried across many distributed servers, security is a concern as the servers might be curious about the matrix contents. Our goal was to improve the security of current protocols by leveraging/utilizing quantum resources. We made significant progress by coming up with relevant protocols, and Kolton is scheduled to disseminate the results in upcoming conferences. While utilizing quantum resources helps improving and achieving security, it comes with its own costs, and trade-offs remain to be explored in future projects.

References

[1] M. Allaix, L. Holzbaur, T. Pllaha, and C. Hollanti. Quantum private information retrieval from coded and colluding servers. *IEEE Journal on Selected Areas in Information Theory*, 1(2):599–610, 2020.

[2] M. Allaix, L. Holzbaur, T. Pllaha, and C. Hollanti. Quantum private information retrieval from MDS-coded and colluding servers. In *2020 IEEE International Symposium on Information Theory (ISIT)*, pages 1059–1064, 2020.

[3] M. Allaix, L. Holzbaur, T. Pllaha, and C. Hollanti. High-rate quantum private information retrieval with weakly self-dual star product codes. In *2021 IEEE International Symposium on Information Theory (ISIT)*, pages 1046–1051, 2021.

[4] M. Allaix, Y. Lu, Y. Yao, T. Pllaha, C. Hollanti, and S. Jafar. N-sum box: An abstraction for linear computation over many-to-one quantum networks. In *2023 IEEE Global Communications Conference*, pages 5457–5462, 2023.

[5] M. Allaix, S. Song, L. Holzbaur, T. Pllaha, M. Hayashi, and C. Hollanti. On the capacity of quantum private information retrieval from mds-coded and colluding servers. *IEEE Journal on Selected Areas in Communications*, 40(3):885–898, 2022.

[6] E. F. Assmus, Jr. The category of linear codes. *IEEE Trans. Inform. Theory*, 44(2):612–629, 1998.

[7] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over GF(4). *IEEE Trans. Inform. Theory*, 44(4):1369–1387, 1998.

[8] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan. Private information retrieval. In *Proceedings of IEEE 36th Annual Foundations of Computer Science*, pages 41–50. IEEE, 1995.

[9] H. L. Claasen and R. W. Goldbach. A field-like property of finite rings. *Indag. Math. (N.S.)*, 3(1):11–26, 1992.

[10] S. Dyshko. On extendability of additive code isometries. *Adv. Math. Commun.*, 10(1):45–52, 2016.

[11] H. Gluesing-Luerssen and T. Pllaha. Extension theorems for various weight functions over Frobenius bimodules. *J. Algebra Appl.*, 17(3):1850052, 28, 2018.

[12] H. Gluesing-Luerssen and T. Pllaha. On quantum stabilizer codes derived from local frobenius rings. *Finite Fields and Their Applications*, 58:145 – 173, 2019.

[13] D. Gottesman. Class of quantum error-correcting codes saturating the quantum Hamming bound. *Phys. Rev. A (3)*, 54(3):1862–1868, 1996.

[14] D. Gottesman. Fault-tolerant quantum computation with constant overhead. *Quantum Inform. and Computation*, 14:1338–1372, Nov 2014.

[15] D. Gottesman and I. L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402(6760):390–393, 1999.

[16] M. Greferath, A. Nechaev, and R. Wisbauer. Finite quasi-Frobenius modules and linear codes. *J. Algebra Appl.*, 3(3):247–272, 2004.

[17] T. Honold. Characterization of finite Frobenius rings. *Arch. Math. (Basel)*, 76(6):406–415, 2001.

[18] S. D. Howard, A. R. Calderbank, and S. J. Searle. A fast reconstruction algorithm for deterministic compressive sensing using second order Reed-Muller codes. In *Conference on Information Sciences and Systems*, pages 11–15, March 2008.

[19] J. Liao, R. Vehkalahti, T. Pllaha, W. Han, and O. Tirkkonen. Modular csi quantization for fdd massive mimo communication. *IEEE Transactions on Wireless Communications*, pages 1–1, 2023.

[20] F. J. MacWilliams. *Combinatorial problems of elementary abelian groups*. ProQuest LLC, Ann Arbor, MI, 1962. Thesis (Ph.D.)–Radcliffe College.

[21] M. Meyer and T. Pllaha. Laplacian simplices II: A coding theoretic approach. Submitted to The Electronic Journal of Combinatorics. arXiv:1809.02960, 2018.

[22] K. D. Morris, T. Pllaha, and C. A. Kelley. Analysis of syndrome-based iterative decoder failure of qldpc codes. In *2023 12th International Symposium on Topics in Coding (ISTC)*, pages 1–5, 2023.

[23] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, Cambridge, 2000.

[24] T. Pllaha. *Equivalence of Classical and Quantum Codes*. 2019. Thesis (Ph.D.)–University of Kentucky.

[25] T. Pllaha. Symplectic isometries of stabilizer codes. *J. Algebra Appl.*, 19(2):2050021, 22, 2020.

[26] T. Pllaha, E. Heikkila, R. Calderbank, and O. Tirkkonen. Low-complexity grassmannian quantization based on binary chirps. In *2022 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1105–1110, 2022.

[27] T. Pllaha, N. Rengaswamy, O. Tirkkonen, and R. Calderbank. Un-Weyl-ing the Clifford Hierarchy. *Quantum*, 4:370, Dec. 2020.

[28] T. Pllaha, O. Tirkkonen, and R. Calderbank. Reconstruction of multi-user binary subspace chirps. In *2020 IEEE International Symposium on Information Theory (ISIT)*, pages 531–536, 2020.

[29] T. Pllaha, O. Tirkkonen, and R. Calderbank. Binary subspace chirps. *IEEE Transactions on Information Theory*, 68(12):7735–7752, 2022.

[30] T. Pllaha, K. Volanto, and O. Tirkkonen. Decomposition of Clifford gates. In *2021 IEEE Global Communications Conference (GLOBECOM)*, pages 01–06, 2021.

[31] Y. Polyanskiy. A perspective on massive random-access. In *2017 IEEE International Symposium on Information Theory (ISIT)*, pages 2523–2527, 2017.

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

[33] S. Song and M. Hayashi. Capacity of quantum private information retrieval with collusion of all but one of servers. *arXiv preprint arXiv:1903.12556*, 2019.

[34] S. Song and M. Hayashi. Capacity of quantum private information retrieval with multiple servers. *arXiv preprint arXiv:1903.10209*, 2019.

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

[36] R. Vehkalahti, J. Liao, T. Pllaha, W. Han, and O. Tirkkonen. CSI quantization for FDD massive MIMO communication. In *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*, pages 1–5, 2021.

[37] R. Vehkalahti, T. Pllaha, and O. Tirkkonen. Signature code design for fast fading channels. In *2021 IEEE International Symposium on Information Theory (ISIT)*, pages 2936–2941, 2021.

[38] R. Vehkalahti, T. Pllaha, and O. Tirkkonen. Towards ultra-reliable signature coding with multiple transmit antennas. In *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*, pages 1–5, 2021.

[39] J. A. Wood. Duality for modules over finite rings and applications to coding theory. *Amer. J. Math.*, 121(3):555–575, 1999.

[40] J. A. Wood. Foundations of linear codes defined over finite modules: the extension theorem and the MacWilliams identities. In *Codes over rings*, volume 6 of *Ser. Coding Theory Cryptol.*, pages 124–190. World Sci. Publ., Hackensack, NJ, 2009.

[41] J. A. Wood. Isometry groups of additive codes over finite fields. *J. Algebra Appl.*, 17(10):1850198, 39, 2018.

[42] Y. Yao and S. A. Jafar. The capacity of classical summation over a quantum MAC with arbitrarily replicated inputs. 2023.