Research Statement

Tefjol Pllaha

My research interests are in applied algebra, very broadly defined. Currently I am focused on applications to algebraic coding theory [10,11,18,21], quantum computation [21–23,25], wireless communications [24,30–32], and online privacy and security [1–4]. This involves work with finite algebraic structures, which may be directly involved in said applications, or that may arise as discretized versions of continuous algebraic structures. I routinely use tools from finite field theory, Fourier analysis, representation theory, (finite or complex) Grassmannian geometry, and finite symplectic geometry.

My PhD work is described in Section 1 and part of Section 2. The reminder of this document describes my postdoctoral work. The intent of this statement is to describe my current research interests in a broader sense. For a detailed research statement 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 C of length n is an additive subgroup of $\mathbb{F}_2^n$. The binary field $\mathbb{F}_2$ is the alphabet, and thus, classically, C is a binary code. Elements of 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 more 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 ${}_FE$ 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 $\omega : A^n \to \mathbb{Q}$ which the code is endowed with. Along with the Hamming weight, other important weights include the homogeneous weight and the Lee weight. In [17], 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 the so-called **Frobenius** alphabets [15] and their rich character-theoretic duality [10, 33, 34].

Finite Frobenius rings are very close to finite fields [8], and similarly, finite Frobenius modules and bimodules are very similar to vector spaces [14, 20]. 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 C, 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 [5] 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 $C = A^n$. 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 $f : C \subsetneq A^n \longrightarrow A^n$ the same as the extremal case for any code C? And if not, how different is the structure? The former was first asked and answered affirmatively by MacWilliams [17] for binary linear codes with respect to the Hamming weight. Further generalizations led to MacWilliams Extension Theorem and the Extension Property of an alphabet [34]. However, the answer is not always affirmative; see Theorem [20, Thm. 5.3]. This fact, along with ideas discussed in [9], led Jay Wood to the notions of **isometry groups** [35]. 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 $C := \Lambda(M)$ via automorphisms of the **information module** M. More specifically, given a code C along with a information module M and encoding Λ, one defines

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

Then, inside $\mathrm{Iso}_\omega(C)$ one identifies the subgroup $\mathrm{Mon}_\omega(C)$ 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 [35]. 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**) [19]. 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) [6, 27].

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 [12]. 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 [11]. 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, which 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 C is a symplectic self-orthogonal subspace, in analogy with (1), we can define two isometry groups:

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

In [21, Example 4.19] we give an explicit example that shows $\mathrm{Mon}_{\mathrm{SL}}(C) \subsetneq \mathrm{Symp}(C)$. Moreover, using ideas from [35] 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 [21, Prop. 4.11]), then there exists a symplectic self-orthogonal subspace C such that $H_1 = \mathrm{Mon}_{\mathrm{SL}}(C)$ and $H_2 = \mathrm{Symp}(C)$.

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 [10] 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 [13]. 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 [22] 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 [22] 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, it is computationally expensive. In [25] 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 [26] 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 [23] 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 [16], 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 [24] 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 [32] 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 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 [32].

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 $i \neq j$.

The 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.

4 (Quantum) Private Information Retrieval

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 delivering. This is referred as Private Information Retrieval (PIR) and was first introduced in the seminal work [7]. 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. We are primarily interested in privacy.

In recent years, PIR has gained renewed interest in the setting of distributed storage systems (DSSs) where the servers are storing possibly large files. 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. 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 [28, 29] 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). The newly introduced scheme is somewhat ad-hoc. Currently, together with with the authors of [28, 29], we are working on implementing the stabilizer formalism [12] for coded storages. Preliminary work has appeared in [3] whereas the capacity is considered in [4].

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, 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. Submitted to JSAC. arXiv:2106.14719, June 2021.

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

[6] 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.

[7] 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.

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

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

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

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

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

[13] 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.

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

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

[16] 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.

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

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

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

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

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

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

[23] T. Pllaha, O. Tirkkonen, and R. Calderbank. Binary subspace chirps. Submitted to Transactions on Information Theory. arXiv:2102.12384, February 2021.

[24] 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.

[25] T. Pllaha, K. Volanto, and O. Tirkkonen. Decomposition of Clifford gates. To appear in GLOBECOM 2021. arXiv:2102.11380, January 2021.

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

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

[28] 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.

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

[30] 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.

[31] 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.

[32] 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.

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

[34] 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.

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