

Space–Time Codes from Sum-Rank Codes

Mohannad Shehadeh, *Graduate Student Member, IEEE* and Frank R. Kschischang, *Fellow, IEEE*

Abstract—Just as rank-metric or Gabidulin codes may be used to construct rate–diversity tradeoff optimal space–time codes, a recently introduced generalization for the sum-rank metric—linearized Reed–Solomon codes—accomplishes the same in the case of multiple fading blocks. In this paper, we provide the first explicit construction of minimal delay rate–diversity optimal multiblock space–time codes as an application of linearized Reed–Solomon codes. We also provide sequential decoders for these codes and, more generally, space–time codes constructed from finite field codes. Simulation results show that the proposed codes can outperform full diversity codes based on cyclic division algebras at low SNRs as well as utilize significantly smaller constellations.

Index Terms—Rank-metric codes, space–time codes, sum-rank codes, wireless communication.

I. INTRODUCTION

THIS paper builds upon a line of work which considers the design of space–time codes that optimally trade off diversity for rate at a fixed constellation size. Our primary contributions are as follows:

1) By replacing Gabidulin codes [2] in known rate–diversity optimal space–time code constructions [3]–[7] with *linearized Reed–Solomon codes* [8], we obtain the first explicit construction of minimal delay rate–diversity optimal *multiblock* space–time codes. This provides the first general solution to a problem first posed in [9] and [7].

2) We provide sequential maximum likelihood (ML) decoders for these codes. More generally, we show that many sequential decoding strategies for space–time codes [10]–[16] that are typically thought to be only applicable to codes with a linear dispersion form [17] can in some cases be effectively adapted for use with the proposed codes and similarly constructed codes [3]–[6].

3) Facilitated by these ML decoders, we provide an empirical study of the performance of the proposed codes in simulation as well as related codes [3]–[6] which had not been previously decoded for large codebook sizes. This demonstrates that these codes can outperform full diversity codes [18]–[21] based on cyclic division algebras (CDAs) [22] at low SNRs and using smaller constellations.

We emphasize that the latter two contributions cover new ground in the single-block setting as well. Apart from the primary contributions, we consolidate some results and observations occurring in some of the previous literature on the rate–diversity optimal space–time coding problem [3]–[7], [9] and attempt to situate these lines work within the

broader literature on space–time coding. We particularly note that this paper contains the first error performance comparison of codes designed for rate–diversity tradeoff optimality with codes designed for diversity–multiplexing tradeoff optimality.

The remainder of this paper is organized as follows: Section II establishes the setting, introduces the rate–diversity optimal multiblock space–time coding problem, and briefly surveys prior work on the problem. Section III discusses the relevance of the rate–diversity perspective and provides an alternative interpretation of the rate–diversity tradeoff to aid in comparing with codes designed from other perspectives. Section IV provides the proposed code construction after introducing the required technical ingredients which are *rank-metric-preserving maps* [3]–[7], [23] and *linearized Reed–Solomon codes* [8]. The error performance of the proposed codes is studied in simulation in Section V with the subject of their decoding deferred to Section VI. Section VII concludes the paper with some suggestions for future work.

II. SETTING, PROBLEM STATEMENT, AND BASIC RESULTS

A. Channel Model

Adopting the setting and conventions of [7], we consider a multiple-input multiple-output (MIMO) Rayleigh block-fading channel with n_t transmit antennas, n_r receive antennas, and L fading blocks per codeword each static for duration T . An L -block $n_t \times T$ space–time code \mathcal{X} is a finite subset of $\mathbb{C}^{n_t \times LT}$ of cardinality greater than or equal to two. A *codeword* $X \in \mathcal{X}$ is a complex $n_t \times LT$ matrix $X = [X_1 \ X_2 \ \dots \ X_L]$ which partitions into L sub-matrices X_1, X_2, \dots, X_L of dimensions $n_t \times T$ referred to as *sub-codewords*. For $\ell = 1, 2, \dots, L$, Y_ℓ is the $n_r \times T$ received matrix given by

$$Y_\ell = \rho H_\ell X_\ell + W_\ell \quad (1)$$

where H_ℓ is the $n_r \times n_t$ channel matrix and W_ℓ is the $n_r \times T$ noise matrix with both having iid circularly-symmetric complex Gaussian entries with unit variance. The codeword X is sampled uniformly at random from a code \mathcal{X} and the real scalar parameter ρ is chosen to satisfy

$$\mathbb{E}[\|\rho X\|_F^2] = \rho^2 \sum_{\ell=1}^L \mathbb{E}[\|X_\ell\|_F^2] = L \cdot T \cdot \text{SNR}. \quad (2)$$

We further have ML decoding at the receiver with perfect channel knowledge in the sense that all channel matrix realizations are known and all channel model parameters are known. In particular, define the ML decision \hat{X} by

$$\hat{X} = \underset{X' \in \mathcal{X}}{\operatorname{argmin}} \sum_{\ell=1}^L \|Y_\ell - \rho H_\ell X'_\ell\|_F^2 \quad (3)$$

The authors are with the Edward S. Rogers Sr. Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S 3G4, Canada (emails: {mshehadeh, frank}@ece.utoronto.ca).

Parts of this work were presented at the 2020 IEEE International Symposium on Information Theory (ISIT) [1].

and define the probability of error P_e by

$$P_e = \Pr(\hat{X} \neq X). \quad (4)$$

The decoding problem to be considered in Section VI is that of solving (3) and each simulation curve in Section V provides the codeword error rate (CER) which is a Monte Carlo estimate of P_e as a function of SNR.

Throughout this paper, we will use \top for the matrix transpose, \dagger for the Hermitian transpose, and $(\cdot)_{ij}$ to denote the ij th entry of a matrix.

Definition 1 (Transmit Diversity Gain). An L -block $n_t \times T$ space-time code is said to achieve a *transmit diversity gain* of d if, for a channel with n_r receive antennas, we have

$$\lim_{\text{SNR} \rightarrow \infty} \frac{\log P_e(\text{SNR})}{\log \text{SNR}} = -n_r d. \quad (5)$$

Theorem 1 (Sum-Rank Criterion [7], [9], [24]–[28]). An L -block $n_t \times T$ space-time code \mathcal{X} achieves a transmit diversity gain of d if and only if

$$d = \min_{\substack{X, X' \in \mathcal{X} \\ X \neq X'}} \sum_{\ell=1}^L \text{rank}(X_\ell - X'_\ell). \quad (6)$$

Proof. This follows from combining the pairwise error probability upper bounds of [24], [26] with the lower bounds of [27], [28] and then sandwiching the probability of error via the union bound. For a detailed proof, see [29]. \square

Theorem 1 thus provides an equivalent definition of transmit diversity gain as a property of the code used. The recognition of the quantity (6) as a criterion for space-time code design first occurs in [24], [26] and the multiblock generalization which we adopt was first recognized in [7], [9], [25]. The equivalence to Definition 1 follows from [27], [28] which provide the required lower bound and state this equivalence.

From (6), we have that the transmit diversity gain d is an integer satisfying $1 \leq d \leq L \cdot \min\{n_t, T\}$. Codes for which $d = L \cdot \min\{n_t, T\}$ are referred to as being *full diversity*. Moreover, codes for which $T = n_t$ are referred to as being *minimal delay*.

A *constellation* \mathcal{A} is defined as a finite subset of \mathbb{C} of cardinality greater than or equal to two. Let \mathcal{A} be a constellation. An L -block $n_t \times T$ space-time code \mathcal{X} will be said to be *completely over* \mathcal{A} if \mathcal{X} is a subset of $\mathcal{A}^{n_t \times LT}$. The term *completely over* is adopted from [22] and emphasizes that codeword entries are constrained to belong to \mathcal{A} .

Definition 2 (Rate). For some fixed constellation \mathcal{A} , the *rate* R of an L -block $n_t \times T$ space-time code \mathcal{X} completely over \mathcal{A} is defined by

$$R = \frac{1}{LT} \log_{|\mathcal{A}|} |\mathcal{X}|. \quad (7)$$

The term *channel use* will refer to a use of the underlying MIMO channel so that a codeword is transmitted across LT channel uses and this rate is interpreted as the average information rate in symbols per channel use.

B. The Rate–Diversity Tradeoff and Some Consequences

The following theorem first appears in [7], [9] and is a generalization of the well-known tradeoff for the case of $L = 1$ appearing in [26], [30]. It follows from a Singleton bound [31] argument.

For the remainder of this section, we will let \mathcal{A} be some fixed but arbitrary constellation.

Theorem 2 (Rate–Diversity Tradeoff [7], [9]). Let \mathcal{X} be an L -block $n_t \times T$ space-time code completely over \mathcal{A} with rate R and achieving transmit diversity gain d . Then,

$$R \leq n_t - \frac{d-1}{L} \cdot \max\left\{\frac{n_t}{T}, 1\right\}. \quad (8)$$

A space-time code is said to be *rate–diversity optimal* if (8) holds with equality. A *rate–diversity pair* (R, d) for which (8) holds with equality (in which case specifying one of R or d specifies the other) will be said to be an *optimal rate–diversity pair*. The rate–diversity optimal multiblock space-time coding problem is that of constructing families of space-time codes capable of achieving *any* optimal rate–diversity pair (R, d) with d a positive integer satisfying $1 \leq d \leq L \cdot \min\{n_t, T\}$. We will be particularly interested in codes that are *not* full diversity. As will be seen shortly, the extremes of this tradeoff are relatively uninteresting.

The remainder of this section will consider what happens for some special cases of the parameters L , n_t , T , and d . The results which follow will not play a role in the main code construction to be provided in Section IV which will admit arbitrary values for these parameters. However, they are worth noting both as basic consequences of Theorem 2 and for the purposes of contextualizing the problem at hand.

Remark. Let $\mathcal{X} = \mathcal{A}^{n_t \times LT}$ be an L -block $n_t \times T$ space-time code completely over \mathcal{A} . It is easy to see that this code, which corresponds to uncoded signalling, achieves the optimal rate–diversity pair (R, d) corresponding to $d = 1$. Thus, restrictions to $d > 1$ are without elimination of interesting cases.

Solutions to the single-block, i.e., $L = 1$, rate–diversity optimal space-time coding problem are provided in [3]–[7], [30], [32], [33], hence we shift our attention to the multiblock, i.e., $L > 1$, problem. There are three special cases in which the multiblock problem is solved by a straightforward adaptation of a solution to the single-block problem. These cases are

- $d = L \cdot \min\{n_t, T\}$, full diversity;
- $T \geq Ln_t$, wide sub-codewords or very slow fading; and
- $n_t \geq LT$, tall sub-codewords or very fast fading.

These three special cases are hence implicitly solved. We show this in the next three propositions which deal with the construction of optimal multiblock codes *assuming that optimal single-block codes are at hand*.

In the case of $d = L \cdot \min\{n_t, T\}$, the only possibility admitted by (6) is that all sub-codeword differences corresponding to distinct codewords are full rank. Thus, as noted in [9] and as will be seen shortly, repetition of a full diversity single-block optimal code is optimal. On the other hand, in the case of $d < L \cdot \min\{n_t, T\}$, (6) admits a combinatorially vast

space of possibilities for the ranks of the differences of the sub-codewords and repetition of any single-block code only allows for the one where all the ranks in the sum in (6) are equal. Repetition in this case hence yields a lower rate than is possible and is suboptimal. More precisely, we have the following proposition:

Proposition 3 (Repetition Constructions). *Let $\tilde{\mathcal{X}}$ be a rate-diversity optimal 1-block $n_t \times T$ space-time code completely over \mathcal{A} achieving the (optimal) rate-diversity pair (\tilde{R}, \tilde{d}) . Let \mathcal{X} be the L -block $n_t \times T$ space-time code completely over \mathcal{A} with $L > 1$ obtained by horizontally concatenating L copies of each codeword of $\tilde{\mathcal{X}}$ and achieving rate-diversity pair (R, d) . Then, $R = \tilde{R}/L$, $d = L\tilde{d}$, and \mathcal{X} is rate-diversity optimal if and only if $\tilde{d} = \min\{n_t, T\}$.*

Proof. Since $|\mathcal{X}| = |\tilde{\mathcal{X}}|$, it is immediate from Definition 7 that $R = \tilde{R}/L$. Moreover, noting that the sub-codewords of \mathcal{X} are identical and are the codewords of $\tilde{\mathcal{X}}$, it is straightforwardly verified that $d = L\tilde{d}$. Next, note that by the rate-diversity optimality of $\tilde{\mathcal{X}}$, we have

$$\begin{aligned} \tilde{R} &= n_t - (\tilde{d} - 1) \cdot \max\left\{\frac{n_t}{T}, 1\right\} \\ &= n_t \cdot \left(1 - \frac{\tilde{d}}{\min\{n_t, T\}}\right) + \max\left\{\frac{n_t}{T}, 1\right\}. \end{aligned}$$

We then have by (8)

$$\begin{aligned} R &= \frac{\tilde{R}}{L} = \frac{n_t}{L} \cdot \left(1 - \frac{\tilde{d}}{\min\{n_t, T\}}\right) + \frac{1}{L} \cdot \max\left\{\frac{n_t}{T}, 1\right\} \\ &\leq \frac{n_t}{1} \cdot \left(1 - \frac{\tilde{d}}{\min\{n_t, T\}}\right) + \frac{1}{L} \cdot \max\left\{\frac{n_t}{T}, 1\right\} \\ &= n_t - \frac{d-1}{L} \cdot \max\left\{\frac{n_t}{T}, 1\right\} \end{aligned}$$

with equality if $\tilde{d} = \min\{n_t, T\}$. Conversely, equality implies that $\tilde{d} = \min\{n_t, T\}$ by the $L > 1$ assumption. \square

We now proceed to the cases of $T \geq Ln_t$ and $n_t \geq LT$ which can be addressed with what we term *slicing constructions* to be described in the next two propositions. The first slicing construction to be described in Proposition 4 first occurs in [7], [25]. Proposition 5 is a space-time coding analogue of a result in [34]. Both are based on the simple fact that

$$\text{rank}\left(\begin{bmatrix} A \\ B \end{bmatrix}\right) \leq \text{rank}(A) + \text{rank}(B)$$

for arbitrary matrices A and B over any field having the same number of columns. Similarly, we have

$$\text{rank}([A \quad B]) \leq \text{rank}(A) + \text{rank}(B) \quad (9)$$

for matrices A and B with the same number of rows.

Proposition 4 (Horizontal Slicing Construction [7], [25]). *Let $\tilde{\mathcal{X}}$ be a rate-diversity optimal 1-block $Ln_t \times T$ space-time code completely over \mathcal{A} with $L > 1$ and let \mathcal{X} be the L -block $n_t \times T$ space-time code completely over \mathcal{A} obtained by horizontally slicing the codewords of $\tilde{\mathcal{X}}$ into L sub-codewords*

of dimensions $n_t \times T$. If $T \geq Ln_t$, then \mathcal{X} is rate-diversity optimal.

Proof. Let (\tilde{R}, \tilde{d}) be the rate-diversity pair achieved by $\tilde{\mathcal{X}}$ and (R, d) be the rate-diversity pair achieved by \mathcal{X} . By the rate-diversity optimality of $\tilde{\mathcal{X}}$, we have $\tilde{R} = Ln_t - \tilde{d} + 1$ and since $|\mathcal{X}| = |\tilde{\mathcal{X}}|$, we have $R = \tilde{R}/L = n_t - (\tilde{d} - 1)/L$. Noting that $T \geq Ln_t \geq n_t$, it suffices to show that $d = \tilde{d}$. Rearranging the rate-diversity tradeoff (8) for \mathcal{X} , we have $d \leq Ln_t - LR + 1 = \tilde{d}$. Let $X, X' \in \mathcal{X}$ be a codeword pair such that $d = \sum_{\ell=1}^L \text{rank}(X_\ell - X'_\ell)$. Then,

$$\begin{aligned} d &= \sum_{\ell=1}^L \text{rank}(X_\ell - X'_\ell) \\ &\geq \text{rank}\left(\begin{bmatrix} X_1 - X'_1 \\ X_2 - X'_2 \\ \vdots \\ X_L - X'_L \end{bmatrix}\right) \\ &\geq \tilde{d} \end{aligned}$$

since the vertically concatenated sub-codewords of \mathcal{X} are a codeword of $\tilde{\mathcal{X}}$ by definition. \square

We can similarly show the following:

Proposition 5 (Vertical Slicing Construction). *Let $\tilde{\mathcal{X}}$ be a rate-diversity optimal 1-block $n_t \times LT$ space-time code completely over \mathcal{A} with $L > 1$ and let \mathcal{X} be the L -block $n_t \times T$ space-time code completely over \mathcal{A} obtained by vertically slicing the codewords of $\tilde{\mathcal{X}}$ into L sub-codewords of dimensions $n_t \times T$. If $n_t \geq LT$, then \mathcal{X} is rate-diversity optimal.*

We conjecture that the converses of Propositions 4 and 5 are also true. Weaker versions of the converse statements can be found in [29]. Essentially, we cannot expect slicing to work beyond the special cases of $T \geq Ln_t$ and $n_t \geq LT$ because this technique inherently relies on the unnecessarily strong requirement of linear independence *across* different sub-codeword matrices. As a result, sub-codewords must be sufficiently wide or sufficiently tall so that linear independence across them can be imposed without a rate penalty.

We seek a rate-diversity optimal family of multi-block space-time codes capable of achieving any optimal rate-diversity pair (R, d) with d an integer satisfying $1 \leq d \leq L \cdot \min\{n_t, T\}$ for any L, T , and n_t . To the best of the authors' knowledge, no such codes exist in the prior literature; existing constructions are either non-explicit or by slicing, thus requiring $T \geq Ln_t$ or $n_t \geq LT$.

C. Existing Rate-Diversity Optimal Constructions

In [7], Lu and Kumar provide for $L = 1$ and $T \geq n_t$ a rate-diversity optimal family for any optimal rate-diversity pair. The construction is based on a mapping which takes a collection of maximum rank distance codes over finite fields, namely Gabidulin codes [2], to a space-time code which inherits the rank of differences properties of the underlying finite field codes. In the case of $L > 1$ and $T \geq Ln_t$, Lu and

Kumar further provide a rate–diversity optimal family for any optimal rate–diversity pair by horizontal slicing as described in Proposition 4. We digress briefly to outline the connection to this paper. Looking at the slicing as being done for the underlying finite field code, the need for $T \geq Ln_t$ occurs precisely due to a limitation of rank-metric or Gabidulin codes which is overcome by sum-rank or linearized Reed–Solomon codes [8]. Once linearized Reed–Solomon codes are at hand, tools in the literature for obtaining space–time codes from codes over finite fields can be adopted and a multiblock rate–diversity optimal family allowing for $T < Ln_t$ will follow. Analogous results hold for the case of $T < n_t$ and $n_t < LT$ by applying the appropriate matrix transpositions.

Single-block rate–diversity optimal families are also described in [3]–[6], [30], [32], [33]. These are again based on starting with rank-metric or Gabidulin codes and using different mappings from finite fields to constellations that are rank-metric-preserving in some sense. By Propositions 3, 4, and 5, these can be used readily to obtain multiblock rate–diversity optimal codes in the three special cases to which they pertain. Moreover, a large number of single-block constructions are available in the literature some of which may be rate–diversity optimal for some specific points on the tradeoff curve, usually the point of full diversity. They can therefore potentially be used to construct rate–diversity optimal multiblock codes in the aforementioned special cases. The reader is referred to the summary of prior constructions in [7] for details. Nonetheless, our focus shall be the unexplored case of $n_t \leq T < Ln_t$ and $1 < d < Ln_t$ where the methods for adapting single-block constructions fail.

Additionally, other lines of work provide non-explicit constructions of space–time codes via design criteria that are more amenable to algebraic constructions or computer search constructions. In [35] and [36], translations of the rank distance over complex field criterion of (6) to rank criteria over finite fields or finite rings are considered in the single-block case. In [9], the work of [35] is extended to provide algebraic criteria for the design of rate–diversity optimal multiblock codes with BPSK and QPSK constellations and a few examples found by exhaustive or empirical searches are provided.

III. OTHER PERSPECTIVES

In this section, we examine the relevance of the rate–diversity perspective and provide a framework for comparing the codes to be constructed with other codes in the space–time coding literature. For the purposes of comparing different space–time codes constructed in different manners and designed for different criteria, we will define some more meaningful notions of rate. The *bits per channel use (bpcu) rate* R_b of an L -block $n_t \times T$ space–time code \mathcal{X} is defined by

$$R_b = \frac{1}{LT} \log_2 |\mathcal{X}|. \quad (10)$$

The *bits per channel use per transmit antenna (bpcu/tx) rate* $R_{b/tx}$ of an L -block $n_t \times T$ space–time code \mathcal{X} is defined by

$$R_{b/tx} = \frac{1}{n_t LT} \log_2 |\mathcal{X}| = \frac{R_b}{n_t}. \quad (11)$$

A. Unconstrained Transmission Alphabets

An L -block $n_t \times T$ space–time code \mathcal{X} is said to be a *linear dispersion code* [17]¹ if it can be expressed as

$$\mathcal{X} = \left\{ \sum_{i=1}^{n_t LT} a_i A_i \mid a_1, a_2, \dots, a_{n_t LT} \in \mathcal{A}_{in} \right\} \quad (12)$$

where $A_1, A_2, \dots, A_{n_t LT} \in \mathbb{C}^{n_t \times LT}$ are referred to as *dispersion matrices* and \mathcal{A}_{in} is a constellation which we refer to as the *input constellation*. The significance of such codes is that the detection problem (3) can be converted into an equivalent standard MIMO detection problem. In particular, one can easily show that the channel (1) can be converted into one with an $n_t LT \times 1$ transmitted vector with entries from the input constellation, an $n_r LT \times n_t LT$ effective channel matrix obtained as a function of the channel matrices and the dispersion matrices, and an $n_r LT \times 1$ received vector. This allows them to be decoded using the same methods used for ML MIMO detection (see, e.g., [37]), most notably sphere decoding [10]–[12]. More generally, a wide class of sequential decoding algorithms become readily applicable [13]. The codes to be introduced in this paper are *not* linear dispersion code and their decoding will be the subject of Section VI.

Note that a linear dispersion code is not completely over the input constellation \mathcal{A}_{in} . The codeword entries are linear combinations of symbols from \mathcal{A}_{in} and thus belong to a larger constellation. This constellation is usually not of any concern in the literature dealing with such codes and is sometimes referred to as being *unconstrained*. However, such language is merely an artifact of the code construction method and nothing prevents us from analyzing these codes from a rate–diversity tradeoff perspective. Every space–time code is completely over some constellation. The smallest such constellation is the union of the entries of all the codewords

$$\mathcal{A} = \bigcup_{X \in \mathcal{X}} \{(X)_{ij} \mid i \in \{1, 2, \dots, n_t\}, j \in \{1, 2, \dots, LT\}\}.$$

and can accordingly be used to define the rate. Linear dispersion codes are usually constructed to be full diversity in which case the rate would satisfy

$$R = \frac{R_b}{\log_2 |\mathcal{A}|} \leq \frac{1}{L} \cdot \max \left\{ \frac{n_t}{T}, 1 \right\} \quad (13)$$

and the code would be rate–diversity optimal if and only if this held with equality.

Moreover, linear dispersion codes can be constructed to both be full diversity and to have $|\mathcal{A}_{in}|^{n_t LT}$ distinct codewords. Examples include certain codes constructed from CDAs [22] as well as all of the codes in [18]–[21] that will be used as empirical error performance baselines in this paper. Regardless of whether or not we have rate–diversity optimality, we will have a bpcu rate of

$$R_b = n_t \cdot \log_2 |\mathcal{A}_{in}|.$$

Furthermore, such codes can be constructed with the input constellation \mathcal{A}_{in} being arbitrarily large. Thus, they can provide full diversity with an arbitrarily large bpcu rate. Another

¹We have slightly modified the definition from that of [17].

notable example of codes allowing for this is the codes of [38].

Given that such codes exist, there is no tradeoff between bpcu rate and diversity if the constellation size is not constrained. Indeed, if our *only* interest is in maximizing bpcu rate and diversity, the rate–diversity tradeoff is irrelevant since we can always impose full diversity. In such a setting, it is typical to design for *diversity–multiplexing tradeoff* [39] optimality. This typically amounts to asking slightly more of a full diversity linear dispersion code. In particular, in the case of minimal delay linear dispersion codes constructed from CDAs, it suffices to impose that the code has a *non-vanishing determinant* property [40], [41]. This amounts to being able to bound the magnitude of the determinant of the codeword differences (or product of the determinants of sub-codeword differences in the multiblock case) away from zero independently of R_b .

The codes to be introduced in this paper are neither designed for diversity–multiplexing optimality nor naturally amenable to an analysis of this tradeoff. However, this is not to suggest that it is not possible or that we are dealing with a fundamentally different kind of a code. For example, in [42], bounds on the diversity–multiplexing tradeoff for similarly constructed codes are obtained. Nonetheless, the only relevance of the diversity–multiplexing tradeoff to this paper is that the codes to be used as performance baselines in this paper happen to be optimal with respect to this tradeoff. The baseline codes have been chosen based on the fact (to the best of the authors’ knowledge) that they are the only explicitly described *multiblock* codes admitting a feasible decoder. In any case, such codes are standard benchmarks in the single-block setting as well.

We will now consider two situations in which the rate–diversity tradeoff might be relevant. In particular, we will consider situations where we might be interested in codes that are not full diversity. These situations are:

- The size or nature of the constellation is of concern.
- The low-SNR error performance is of concern.

Importantly, we argue that when a space–time coded system is scaled in a natural way, both of these issues necessarily become of practical concern.

We begin with the first situation. It is well-known that large constellations are associated with implementation challenges. For example, [43], [44] consider transmitter-side quantization as well as peak-to-average power ratio issues arising from the constellations produced by certain linear dispersion codes. Receiver-side quantization issues which are exacerbated by large constellations are studied in [45], [46]. Moreover, in [47], techniques for reducing the signalling complexity, i.e., constellation size, for CDA-based linear dispersion codes are provided. However, as will be seen in the next section, such an issue is inherent to full diversity codes.

B. A Signalling-Complexity Perspective

Consider an L -block $n_t \times T$ space–time code completely over some constellation \mathcal{A} with rate R and transmit diversity gain of d satisfying $1 \leq d \leq L \cdot \min\{n_t, T\}$. Next, take the

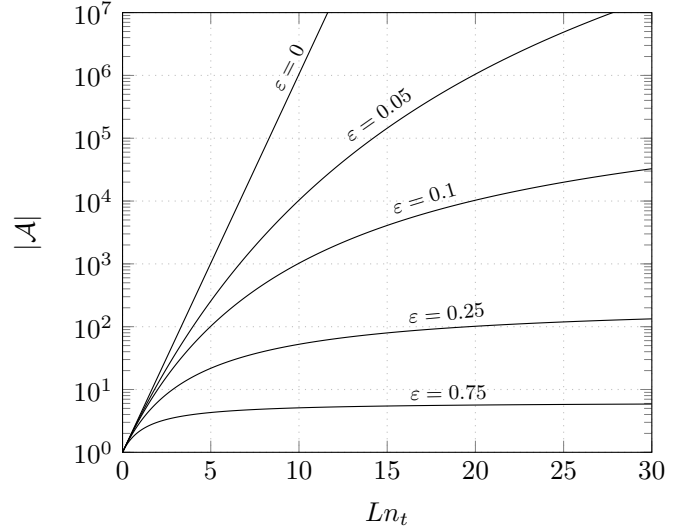


Fig. 1. Constellation size lower bounds for $T \geq n_t$, $R_b/n_t = 2$, and $d = \lceil (1 - \varepsilon) L n_t \rceil$

diversity gain to be a $(1 - \varepsilon)$ fraction of the total available diversity gain. In particular, fix some ε satisfying $0 \leq \varepsilon < 1$ and let $d = \lceil (1 - \varepsilon) \cdot L \cdot \min\{n_t, T\} \rceil$. Consider further fixing $R_{b/\text{tx}} = R_b/n_t$.

Multiplying both sides of the rate–diversity tradeoff (8) by $1/n_t$, we get

$$\begin{aligned} \frac{R_{b/\text{tx}}}{\log_2 |\mathcal{A}|} &\leq 1 - \frac{\lceil (1 - \varepsilon) \cdot L \cdot \min\{n_t, T\} \rceil}{L \cdot \min\{n_t, T\}} + \frac{1}{L \cdot \min\{n_t, T\}} \\ &\leq \varepsilon + \frac{1}{L \cdot \min\{n_t, T\}} \end{aligned}$$

hence

$$|\mathcal{A}| \geq \exp \left(\frac{R_{b/\text{tx}} \ln 2}{\varepsilon + \frac{1}{L \cdot \min\{n_t, T\}}} \right).$$

Thus, we have a lower bound on the constellation size which we will view as a function F_ε of $L \cdot \min\{n_t, T\}$, i.e., define

$$F_\varepsilon(L \cdot \min\{n_t, T\}) = \exp \left(\frac{R_{b/\text{tx}} \ln 2}{\varepsilon + \frac{1}{L \cdot \min\{n_t, T\}}} \right). \quad (14)$$

This gives the constellation size obtained by a rate–diversity optimal code (provided that $(1 - \varepsilon) \cdot L \cdot \min\{n_t, T\}$ is an integer) and is also the smallest constellation size possible.

Observe that for $\varepsilon = 0$, we have

$$F_0(L \cdot \min\{n_t, T\}) = \exp(L \cdot \min\{n_t, T\} \cdot R_{b/\text{tx}} \ln 2) \quad (15)$$

and for $\varepsilon > 0$, we have

$$F_\varepsilon(L \cdot \min\{n_t, T\}) < \exp \left(\frac{R_{b/\text{tx}} \ln 2}{\varepsilon} \right). \quad (16)$$

We now consider scaling the system in $L \cdot \min\{n_t, T\}$. This has two very natural interpretations:

The first is to take n_t and T to be fixed and L to be growing. In this case, a fixed $R_{b/\text{tx}}$ corresponds to a fixed R_b . Thus, we are scaling the system in the number of fading blocks L being coded across with a fixed bpcu rate R_b and improving reliability in $(1 - \varepsilon) \cdot L$. We then see that we have

exponential growth of the constellation size in L for $\varepsilon = 0$ and a constellation size that is bounded independently of L at best for $\varepsilon > 0$.

The second is to take L to be fixed and n_t to be growing with $T \geq n_t$. The $T \geq n_t$ requirement is needed to obtain the transmit diversity gain afforded by n_t transmit antennas and is standard in diversity–multiplexing literature. Moreover, the bpcu rate $R_b = R_{b/\text{tx}} \cdot n_t$ grows linearly with n_t so as to match the rate of uncoded independent signalling on each antenna. This is also as would be the case for families of diversity–multiplexing optimal linear dispersion codes. Again, we have exponential growth of the constellation size in n_t for $\varepsilon = 0$ and potentially bounded constellation size otherwise.

Fig. 1 plots constellation size lower bounds for $R_{b/\text{tx}} = 2$ and $T \geq n_t$. They can be interpreted from either of the points of view just discussed. From this, we see that full diversity codes necessitate exponential growth in the constellation size. On the other hand, by giving up only a fixed fraction of the total available diversity gain, a bounded constellation size is possible².

C. Low-SNR Error Performance

Recall that diversity gain is only a characterization of the error performance in the limit of large SNR. In [49], it is argued that a full diversity requirement becomes increasingly less important as the total available diversity gain increases. Analytical arguments and simulation evidence are provided with trellis codes and in a single-block setting. In particular, it may be the case that a code which is not full diversity code has relatively few codeword pairs for which the sum of ranks (6) is minimal. With that said, we will not attempt to analyze the distance distributions of the proposed codes nor connect them to rate–diversity optimality. Rather, we will simply demonstrate in simulation that the proposed codes can have good low-SNR performance.

Finally, we remark that what constitutes a low SNR is relative and one need not be nominally interested in low-SNR performance to back away from full diversity codes. We can replace the term *low* with *finite* in the previous discussion and it will hold. This will also be reflected by the simulation results.

IV. CODE CONSTRUCTION

This section will begin with the required background on sum-rank codes after which we define linearized Reed–Solomon codes in Section IV-B. Following this, we provide some background and results regarding rank-metric-preserving maps in Section IV-C which are applied in Section IV-D to yield the main code construction.

A. Background on Sum-Rank Codes

The sum-rank metric was introduced in the context of multishot network coding in [50]. We shall define it adopting

²In actuality, the code construction will require $|A| > L$ (see Definition 7 in Section IV-B). Whether this bound is fundamental is connected to some open problems. The reader is referred to the relevant discussions at the end of [48].

the more recent framework of [34], [48]. The space–time coding analogue of the sum-rank metric occurring in (6) appears earlier in [7], [9], [25]. We will use the terms *metric* and *distance* interchangeably.

The finite field with q elements (with q a prime power) will be denoted by \mathbb{F}_q . We adopt the convention that $\mathbb{F}_q^s = \mathbb{F}_q^{1 \times s}$.

The extension field \mathbb{F}_{q^m} forms an m -dimensional vector space over the base field \mathbb{F}_q . Therefore, there exists a vector space isomorphism between \mathbb{F}_{q^m} and \mathbb{F}_q^m . We will accordingly define a matrix representation of the elements of $\mathbb{F}_{q^m}^s$ with respect to some choice of basis. Let $\mathcal{B} = (\beta_1, \beta_2, \dots, \beta_m)$ be an ordered basis of \mathbb{F}_{q^m} over \mathbb{F}_q . Then, any $\mathbf{c} \in \mathbb{F}_{q^m}^s$ can be written as

$$\begin{aligned} \mathbf{c} &= [\sum_{i=1}^m \beta_i c_{i1} \quad \sum_{i=1}^m \beta_i c_{i2} \quad \cdots \quad \sum_{i=1}^m \beta_i c_{is}] \\ &= \sum_{i=1}^m \beta_i [c_{i1} \quad c_{i2} \quad \cdots \quad c_{is}] \\ &= \sum_{i=1}^m \beta_i \mathbf{c}_i \end{aligned}$$

where $\mathbf{c}_i = [c_{i1} \quad c_{i2} \quad \cdots \quad c_{is}] \in \mathbb{F}_q^s$ contains the i th coordinates of the representations of the s elements of \mathbb{F}_{q^m} in \mathbf{c} in terms of the basis \mathcal{B} for $i = 1, 2, \dots, m$.

Definition 3 (Matrix Representation Map [34]). Let $\mathcal{B} = (\beta_1, \beta_2, \dots, \beta_m)$ be an ordered basis of \mathbb{F}_{q^m} over \mathbb{F}_q . The matrix representation of any $\mathbf{c} \in \mathbb{F}_{q^m}^s$ with respect to \mathcal{B} is given by the *matrix representation map* $M_{\mathcal{B}}: \mathbb{F}_{q^m}^s \rightarrow \mathbb{F}_q^{m \times s}$ defined by

$$M_{\mathcal{B}}\left(\sum_{i=1}^m \beta_i \mathbf{c}_i\right) = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1s} \\ c_{21} & c_{22} & \cdots & c_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{ms} \end{bmatrix}$$

where $\mathbf{c} = \sum_{i=1}^m \beta_i \mathbf{c}_i$ and $\mathbf{c}_i = [c_{i1} \quad c_{i2} \quad \cdots \quad c_{is}] \in \mathbb{F}_q^s$ for $i = 1, 2, \dots, m$.

For some fixed positive integer N , we define a *sum-rank length partition* [34] as a choice of a positive integer L and ordered positive integers r_1, r_2, \dots, r_L such that $N = r_1 + r_2 + \cdots + r_L$. For a fixed sum-rank length partition, any $\mathbf{c} \in \mathbb{F}_{q^m}^N$ can be partitioned as

$$\mathbf{c} = [\mathbf{c}^{(1)} \quad \mathbf{c}^{(2)} \quad \cdots \quad \mathbf{c}^{(L)}]$$

where $\mathbf{c}^{(\ell)} \in \mathbb{F}_{q^m}^{r_\ell}$ for $\ell = 1, 2, \dots, L$. Moreover, it shall be understood that any $\mathbf{c} \in \mathbb{F}_{q^m}^N$ partitions this way once a sum-rank length partition has been specified.

Remark. The matrix representation map is \mathbb{F}_q -linear. In particular, for any $A, B \in \mathbb{F}_q^{s \times t}$ and $\mathbf{c}, \mathbf{d} \in \mathbb{F}_{q^m}^s$, we have

$$M_{\mathcal{B}}(\mathbf{c}A + \mathbf{d}B) = M_{\mathcal{B}}(\mathbf{c})A + M_{\mathcal{B}}(\mathbf{d})B.$$

Furthermore, for any $a, b \in \mathbb{F}_q$ and $\mathbf{c}, \mathbf{d} \in \mathbb{F}_{q^m}^s$, we have

$$M_{\mathcal{B}}(a\mathbf{c} + b\mathbf{d}) = aM_{\mathcal{B}}(\mathbf{c}) + bM_{\mathcal{B}}(\mathbf{d}).$$

Definition 4 (Sum-Rank Metric [34], [48], [50]). Let $\mathcal{B} = (\beta_1, \beta_2, \dots, \beta_m)$ be an ordered basis of \mathbb{F}_{q^m} over \mathbb{F}_q and fix a sum-rank length partition $N = r_1 + r_2 + \cdots + r_L$ so that

any $\mathbf{c} \in \mathbb{F}_{q^m}^N$ partitions as $\mathbf{c} = [\mathbf{c}^{(1)} \ \mathbf{c}^{(2)} \ \dots \ \mathbf{c}^{(L)}]$ with $\mathbf{c}^{(\ell)} \in \mathbb{F}_{q^m}^{r_\ell}$ for $\ell = 1, 2, \dots, L$. The *sum-rank weight* is the function $w_{\text{SR}}: \mathbb{F}_{q^m}^N \rightarrow \mathbb{N}$ defined by

$$w_{\text{SR}}(\mathbf{c}) = \sum_{\ell=1}^L \text{rank}(M_{\mathcal{B}}(\mathbf{c}^{(\ell)}))$$

for any $\mathbf{c} \in \mathbb{F}_{q^m}^N$. The *sum-rank metric* (or distance) is the function $d_{\text{SR}}: \mathbb{F}_{q^m}^N \times \mathbb{F}_{q^m}^N \rightarrow \mathbb{N}$ defined by

$$\begin{aligned} d_{\text{SR}}(\mathbf{c}, \mathbf{d}) &= w_{\text{SR}}(\mathbf{c} - \mathbf{d}) \\ &= \sum_{\ell=1}^L \text{rank}(M_{\mathcal{B}}((\mathbf{c} - \mathbf{d})^{(\ell)})) \\ &= \sum_{\ell=1}^L \text{rank}(M_{\mathcal{B}}(\mathbf{c}^{(\ell)}) - M_{\mathcal{B}}(\mathbf{d}^{(\ell)})). \end{aligned}$$

for any $\mathbf{c}, \mathbf{d} \in \mathbb{F}_{q^m}^N$.

In what follows, unless otherwise stated, we shall assume some fixed but arbitrary sum-rank length partition $N = r_1 + r_2 + \dots + r_L$ for some fixed positive integer N for the purposes of defining sum-rank distances and weights. The reader should keep in mind the dependency of these quantities on the sum-rank length partition which we suppress for brevity. On the other hand, we need not specify a basis since the rank of a matrix representation is independent of the choice of basis.

Remark. The subadditivity of rank, i.e., that for a pair of equal-sized matrices A and B over any field, we have $\text{rank}(A + B) \leq \text{rank}(A) + \text{rank}(B)$ can be used to verify that the sum-rank metric is indeed a metric.

Observe that when the sum-rank length partition is $r_1 = r_2 = \dots = r_N = 1$ (with $L = N$), the sum-rank distance recovers *Hamming distance* [51] since the zero column vector is the only column vector of rank zero. We denote Hamming distance by d_{H} . At the other extreme of sum-rank length partition $N = r_1$ (with $L = 1$), the sum-rank distance becomes the *rank distance* [2] which we denote by d_{R} . In this sense, the sum-rank metric generalizes the Hamming and rank metrics. Our particular notion of rank distance, i.e., as a metric on vector spaces over extension fields, was first studied by Gabidulin in [2]. A related notion of rank distance occurs earlier in [52].

We define the *minimum sum-rank distance* of a code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^N$, denoted $d_{\text{SR}}(\mathcal{C})$, as

$$\begin{aligned} d_{\text{SR}}(\mathcal{C}) &= \min_{\substack{\mathbf{c}, \mathbf{d} \in \mathcal{C} \\ \mathbf{c} \neq \mathbf{d}}} d_{\text{SR}}(\mathbf{c}, \mathbf{d}) \\ &= \min_{\substack{\mathbf{c}, \mathbf{d} \in \mathcal{C} \\ \mathbf{c} \neq \mathbf{d}}} \sum_{\ell=1}^L \text{rank}(M_{\mathcal{B}}(\mathbf{c}^{(\ell)}) - M_{\mathcal{B}}(\mathbf{d}^{(\ell)})). \end{aligned}$$

A code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^N$ is said to be *linear* if it is a k -dimensional subspace of the vector space $\mathbb{F}_{q^m}^N$ over the field \mathbb{F}_{q^m} . Adopting the standard concise notation, such a code will be said to be an $[N, k]_{q^m}$ code where the square brackets emphasize the linearity.

Theorem 6, which follows, is analogous to Theorem 2, the rate–diversity tradeoff, and may be proven in a similar manner.

Theorem 6 (A Generalized Singleton Bound [8], [34]). *For any code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^N$, we have*

$$|\mathcal{C}| \leq q^{m(N - d_{\text{SR}}(\mathcal{C}) + 1)}. \quad (17)$$

Moreover, if \mathcal{C} is an $[N, k]_{q^m}$ code, this is equivalent to

$$k \leq N - d_{\text{SR}}(\mathcal{C}) + 1. \quad (18)$$

Reiterating, it is implicit that all claims made about sum-rank distance are true for a fixed but arbitrary choice of sum-rank length partition. Codes which achieve (17) with equality are said to be *maximum sum-rank distance (MSRD)*. When the sum-rank length partition is chosen so that the sum-rank metric becomes the Hamming metric, (17) becomes the classical Singleton bound [31] achieved by classical Reed–Solomon codes [53]. MSRD thus becomes equivalent to *maximum distance separable (MDS)*. When the sum-rank length partition is chosen so that the sum-rank metric becomes the rank metric, being MSRD becomes equivalent to being *maximum rank distance (MRD)* which is achieved by Gabidulin codes [2].

By (9), it is easy to see that for any $\mathbf{c}, \mathbf{d} \in \mathbb{F}_{q^m}^N$, we have

$$d_{\text{R}}(\mathbf{c}, \mathbf{d}) \leq d_{\text{SR}}(\mathbf{c}, \mathbf{d}) \leq d_{\text{H}}(\mathbf{c}, \mathbf{d}). \quad (19)$$

One can further see that for any $\mathcal{C} \subseteq \mathbb{F}_{q^m}^N$, we have

$$d_{\text{R}}(\mathcal{C}) \leq d_{\text{SR}}(\mathcal{C}) \leq d_{\text{H}}(\mathcal{C}). \quad (20)$$

Straightforwardly generalizing this, we get the following result from [34]:

Proposition 7 (Refinement Preserves Sum-Rank [34]). *Denote by $d_{\text{SR}}^{\text{coarse}}$ the sum-rank metric for the sum-rank length partition $N = \sum_{\ell=1}^L r_\ell$. Let $r_\ell = \sum_{i=1}^{L_\ell} r_{\ell i}$ for $\ell = 1, 2, \dots, L$. Denote by $d_{\text{SR}}^{\text{fine}}$ the sum-rank metric for the sum-rank length partition $N = \sum_{\ell=1}^L \sum_{i=1}^{L_\ell} r_{\ell i}$. For any code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^N$, we have that*

$$d_{\text{SR}}^{\text{coarse}}(\mathcal{C}) \leq d_{\text{SR}}^{\text{fine}}(\mathcal{C}). \quad (21)$$

A crucial aspect of Theorem 6 is that we have the same bound regardless of the choice of sum-rank length partition—coarsening the metric does not lead to a codebook size penalty. Theorem 7 thus results in the following:

Corollary 7.1. *Let $d_{\text{SR}}^{\text{coarse}}$ and $d_{\text{SR}}^{\text{fine}}$ be as previously defined. If $\mathcal{C} \subseteq \mathbb{F}_{q^m}^N$ is MSRD with respect to $d_{\text{SR}}^{\text{coarse}}$, then it is also MSRD with respect to $d_{\text{SR}}^{\text{fine}}$.*

As special cases of this corollary, we have the following:

- If $\mathcal{C} \subseteq \mathbb{F}_{q^m}^N$ is MRD, then \mathcal{C} is MSRD for *any* sum-rank length partition.
- If $\mathcal{C} \subseteq \mathbb{F}_{q^m}^N$ is MSRD, then \mathcal{C} is MDS.

So, if $\mathcal{C} \subseteq \mathbb{F}_{q^m}^N$ is MRD, then $d_{\text{R}}(\mathcal{C}) = d_{\text{SR}}(\mathcal{C}) = d_{\text{H}}(\mathcal{C}) = N - \log_{q^m} |\mathcal{C}| + 1$ making it MSRD and MDS. In light of this, it is natural to ask why one might use an MSRD code over an MRD code. The answer lies in the following results from [34]:

Theorem 8 (Extension Degree Bound [34]). *Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^N$ be an MSRD code for the sum-rank length partition $r_1 = r_2 = \dots = r_L = N/L$ and let $d_{\text{SR}}(\mathcal{C}) > 1$, then*

$$m \geq \frac{N}{L}. \quad (22)$$

Corollary 8.1. *If $\mathcal{C} \subseteq \mathbb{F}_{q^m}^N$ is MRD and $d_R(\mathcal{C}) > 1$, then $m \geq N$.*

Thus, MRD codes impose a larger field extension degree. In particular, for the purposes of our space-time code construction, in the case of $T \geq n_t$, we will let $m = T$ and $N = Ln_t$. Corollary 8.1 then becomes the requirement that $T \geq Ln_t$ for constructions based on MRD codes such as those in [7], [25]. In the case of $T \leq n_t$, we will let $m = n_t$ and $N = LT$ in which case Corollary 8.1 becomes an $n_t \geq LT$ requirement for constructions based on MRD codes.

Linearized Reed–Solomon codes, to be introduced in the next subsection, are a recently introduced [8] family of linear MSRD codes which can achieve the field extension degree bound (22) with equality. This will enable multiblock space-time codes constructed from them to achieve $T = n_t$, or more generally, any relationship between T and n_t .

We conclude this section with some comments on generator matrices. A *generator matrix* of an $[N, k]_{q^m}$ code is a full rank matrix $G \in \mathbb{F}_{q^m}^{k \times N}$ whose row space is the code. A *systematic generator matrix* is one of the form $G = [I_k \ P]$ where $I_k \in \mathbb{F}_{q^m}^{k \times k}$ denotes the $k \times k$ identity matrix and $P \in \mathbb{F}_{q^m}^{k \times (N-k)}$. Clearly, any linear code has a generator matrix which is some column permutations away from a systematic one. While column permutations change the row space and hence the code, they are isometries of the Hamming and rank metrics making systematicity a non-issue when these are the metrics of interest. However, it is easy to see that column permutations are not in general isometries of the sum-rank metric.

With that said, this will be a non-issue because for any MSRD code, there exists a systematic generator matrix and, more generally, a generator matrix with the k columns of I_k occurring *anywhere* in it. This follows from the fact that MSRD codes are MDS and these are well-known properties of MDS codes (see, e.g., [54]).

B. Linearized Reed–Solomon Codes

Linearized Reed–Solomon codes were recently introduced by Martínez-Peñas in [8]. These codes are closely connected to skew polynomial evaluation codes [55]–[57]. Their significance to us should be clear at this point so we will limit our task in this section to providing the definition.

In particular, we will provide a specialization of the definition of linearized Reed–Solomon codes in [8] which is sufficient for the purposes of our space-time code construction.

We begin by specializing the sum-rank length partition to $r_1 = r_2 = \dots = r_L = N/L$ maintaining this henceforth. Define the field automorphism $\sigma: \mathbb{F}_{q^m} \rightarrow \mathbb{F}_{q^m}$ by $\sigma(a) = a^q$ for all $a \in \mathbb{F}_{q^m}$.

Definition 5 (Truncated norm [34]). Define $N_i: \mathbb{F}_{q^m} \rightarrow \mathbb{F}_{q^m}$ by

$$N_i(a) = \sigma^{i-1}(a)\sigma^{i-2}(a) \cdots \sigma(a)a.$$

for all $a \in \mathbb{F}_{q^m}$ and all $i \in \mathbb{N}$.

Definition 6 (Linear Operator (Composition) [8], [34]). For some fixed $a \in \mathbb{F}_{q^m}$, define the \mathbb{F}_q -linear operator $\mathcal{D}_a^i: \mathbb{F}_{q^m} \rightarrow \mathbb{F}_{q^m}$ by

$$\mathcal{D}_a^i(b) = \sigma^i(b)N_i(a)$$

for all $b \in \mathbb{F}_{q^m}$ and all $i \in \mathbb{N}$.

Remark. We have $\mathcal{D}_a^1(b) = \sigma(b)a$ and $\mathcal{D}_a^1 \circ \mathcal{D}_a^i = \mathcal{D}_a^{i+1}$ for all $i \in \mathbb{N}$.

For an $[N, k]_{q^m}$ code with generator matrix $G \in \mathbb{F}_{q^m}^{k \times N}$, it shall be understood that the generator matrix partitions according to the sum-rank length partition as

$$G = [G_1 \ G_2 \ \cdots \ G_L]$$

with $G_\ell \in \mathbb{F}_{q^m}^{k \times N/L}$ for $\ell = 1, 2, \dots, L$ referred to as *sub-codeword generators*.

Definition 7 (Linearized Reed–Solomon Code (Special Case) [8]). Let $q > L$, $m \geq N/L$, α be a primitive element of \mathbb{F}_{q^m} , and $\mathcal{B} = (\beta_1, \beta_2, \dots, \beta_m)$ be an ordered basis of \mathbb{F}_{q^m} over \mathbb{F}_q . A linearized Reed–Solomon code is an $[N, k]_{q^m}$ code with sub-codeword generators

$$G_\ell = \begin{bmatrix} \beta_1 & \beta_2 & \cdots & \beta_{N/L} \\ \mathcal{D}_{\alpha^{\ell-1}}^1(\beta_1) & \mathcal{D}_{\alpha^{\ell-1}}^1(\beta_2) & \cdots & \mathcal{D}_{\alpha^{\ell-1}}^1(\beta_{N/L}) \\ \mathcal{D}_{\alpha^{\ell-1}}^2(\beta_1) & \mathcal{D}_{\alpha^{\ell-1}}^2(\beta_2) & \cdots & \mathcal{D}_{\alpha^{\ell-1}}^2(\beta_{N/L}) \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{D}_{\alpha^{\ell-1}}^{k-1}(\beta_1) & \mathcal{D}_{\alpha^{\ell-1}}^{k-1}(\beta_2) & \cdots & \mathcal{D}_{\alpha^{\ell-1}}^{k-1}(\beta_{N/L}) \end{bmatrix}$$

for $\ell = 1, 2, \dots, L$.

Theorem 9 (MSRD Property [8]). An $[N, k]_{q^m}$ linearized Reed–Solomon code \mathcal{C} achieves $k = N - d_{SR}(\mathcal{C}) + 1$.

C. Background on Rank-Metric-Preserving Maps

A variety of methods [3], [5]–[7], [23], [32], [35], [36] exist for obtaining space-time codes from codes over finite fields. We set aside those focused on binary fields because linearized Reed–Solomon codes are only interesting when nonbinary due to the $q > L$ requirement. We further set aside those which do not lead to explicit constructions. This leaves over the methods in [3]–[7]. In [6], the authors propose a framework which encompasses as special cases mappings to the Gaussian [3], [4] and Eisenstein [5] integers and find that, with the exception of when a small PSK constellation is required, the method in [7] is outperformed. We accordingly define a notion of rank-metric-preserving map only general enough to subsume these important special cases.

Definition 8 (Rank-Metric-Preserving Map). Let q be a prime power, \mathcal{A} be a constellation of size q , and $\phi: \mathbb{F}_q \rightarrow \mathcal{A}$ be a bijection. Define $\tilde{\phi}: \mathbb{F}_q^{n_t \times T} \rightarrow \mathcal{A}^{n_t \times T}$ to be the corresponding entrywise map which is the bijection defined, for all $C \in \mathbb{F}_q^{n_t \times T}$, by $(\tilde{\phi}(C))_{ij} = \phi((C)_{ij})$ for $i = 1, 2, \dots, n_t$ and $j = 1, 2, \dots, T$. The map ϕ is said to be *rank-metric-preserving* if

$$\text{rank}(\tilde{\phi}(C) - \tilde{\phi}(D)) \geq \text{rank}(C - D)$$

for all $C, D \in \mathbb{F}_q^{n_t \times T}$, $C \neq D$.

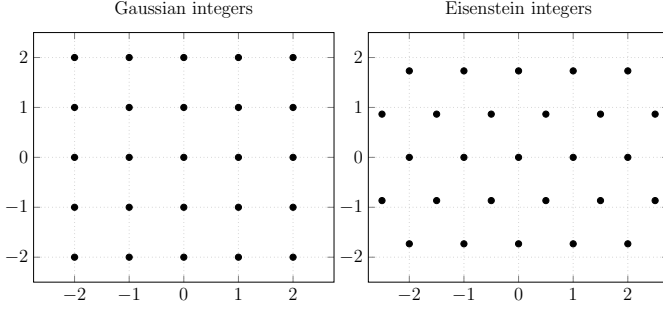


Fig. 2. Some Gaussian and Eisenstein integers in the complex plane

We will next introduce the Gaussian and Eisenstein integers and recall some useful properties. Some will be essential to the encoding and decoding procedures for the proposed codes and others will be relevant to answering existential questions.

In what follows, ι will denote the imaginary unit and ω will denote the primitive cube root of unity

$$\omega = \exp\left(\frac{2\pi\iota}{3}\right) = -\frac{1}{2} + \iota\frac{\sqrt{3}}{2}.$$

The *Gaussian integers* which we denote by \mathbb{G} are defined by [58]

$$\mathbb{G} = \mathbb{Z}[\iota] = \{a + b\iota \mid a, b \in \mathbb{Z}\}.$$

Noting that as a real vector space, \mathbb{C} is isomorphic to \mathbb{R}^2 , we see that, additively, \mathbb{G} is isomorphic to the square lattice $\mathbb{Z}^2 \subseteq \mathbb{R}^2$, i.e., the set of integral linear combinations of $[1 \ 0]^\top$ and $[0 \ 1]^\top$. The *Eisenstein integers* which we denote by \mathbb{E} are defined by [58]

$$\mathbb{E} = \mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}.$$

Additively, \mathbb{E} is isomorphic to the hexagonal lattice in \mathbb{R}^2 spanned by the integral linear combinations of $[1 \ 0]^\top$ and $[-1/2 \ \sqrt{3}/2]^\top$.

Additively and multiplicatively, the Gaussian and Eisenstein integers share many of the properties of the usual integers \mathbb{Z} . In particular, they are archetypal examples of rings other than \mathbb{Z} that are not fields and admit a Euclidean division [59], [60]. This allows finite fields to be easily constructed as their residue classes just as the prime field \mathbb{F}_p can be constructed as a set of residue classes of the usual integers $\mathbb{Z}/p\mathbb{Z}$.

In what follows, we will make claims and provide definitions involving both the Gaussian and Eisenstein integers. Some will apply to both and some will be specific to one or the other. We will use Λ to refer to any one of \mathbb{G} or \mathbb{E} when the definition or result applies to both.

We define a *quantization function* $Q_\Lambda : \mathbb{C} \rightarrow \Lambda$ as in [61] by

$$Q_\Lambda(z) = \operatorname{argmin}_{\lambda \in \Lambda} |z - \lambda| \quad (23)$$

for all $z \in \mathbb{C}$. We will comment later on the well-definedness of this function. Importantly, the quantization can be performed efficiently for the sets under consideration. For $\Lambda = \mathbb{G}$, we have, for all $z \in \mathbb{C}$, [62]

$$Q_{\mathbb{G}}(z) = [\operatorname{Re}\{z\}] + \iota [\operatorname{Im}\{z\}]$$

where $[\cdot]$ denotes the usual operation of rounding to the nearest integer. For $\Lambda = \mathbb{E}$, we have the following algorithm from [61]: For any $z \in \mathbb{C}$, compute

$$\begin{aligned} \lambda_1 &= [\operatorname{Re}\{z\}] + \sqrt{-3} \left\lceil \frac{\operatorname{Im}\{z\}}{\sqrt{3}} \right\rceil \\ \lambda_2 &= [\operatorname{Re}\{z - \omega\}] + \sqrt{-3} \left\lceil \frac{\operatorname{Im}\{z - \omega\}}{\sqrt{3}} \right\rceil + \omega \end{aligned}$$

which are the nearest points to z in two sets which partition \mathbb{E} . We then have

$$Q_{\mathbb{E}}(z) = \operatorname{argmin}_{\lambda \in \{\lambda_1, \lambda_2\}} |z - \lambda|.$$

We will be interested in quantization to a sub-lattice $\Lambda' \subseteq \Lambda$ obtained as $\Lambda' = \Pi\Lambda$ where $\Pi \in \Lambda \setminus \{0\}$. In this case, we have

$$Q_{\Lambda'}(z) = Q_{\Pi\Lambda}(z) = \Pi \cdot Q_\Lambda\left(\frac{z}{\Pi}\right)$$

for all $z \in \mathbb{C}$. Finally, given Λ and $\Pi \in \Lambda \setminus \{0\}$, we define a *modulo function* $\operatorname{mod}_{\Pi\Lambda} : \Lambda \rightarrow \Lambda$ as in [5] by

$$\begin{aligned} \operatorname{mod}_{\Pi\Lambda}(z) &= z - Q_{\Pi\Lambda}(z) \\ &= z - \Pi \cdot Q_\Lambda\left(\frac{z}{\Pi}\right) \end{aligned}$$

for all $z \in \Lambda$. The modulo function provides a unique representative of the coset in the quotient ring $\Lambda/\Pi\Lambda$ to which any $z \in \Lambda$ belongs. Consider the constellation $\mathcal{A}_{\Pi\Lambda}$ obtained as

$$\mathcal{A}_{\Pi\Lambda} = \{\operatorname{mod}_{\Pi\Lambda}(z) \mid z \in \Lambda\}.$$

It can be shown (see, e.g., [5], [62]) that

$$|\mathcal{A}_{\Pi\Lambda}| = |\Lambda/\Pi\Lambda| = |\Pi|^2.$$

Moreover, by the fact that if $\Pi = rs$ for some $r, s \in \Lambda$, then $|\Pi|^2 = |r|^2 |s|^2$, we have the following:

Proposition. *If $|\Pi|^2$ is prime in \mathbb{Z} , then Π is prime in Λ .*

If we take Π to be a prime in Λ , then $\Lambda/\Pi\Lambda$ will be isomorphic to $\mathbb{F}_{|\Pi|^2}$ and the same will be true of the constellation $\mathcal{A}_{\Pi\Lambda}$ under the appropriate arithmetic. Note that the converse of the previous proposition is not true; primes in Λ corresponding to non-prime squared absolute value can exist and will allow for isomorphisms to finite fields of prime power sizes (refer to, e.g., [5], [6], [61]). However, we will limit ourselves to prime fields for simplicity. Importantly, constellations corresponding to prime Π give rise to rank-metric-preserving maps. We will proceed to give some useful properties of these constellations.

Proposition 10. *If $z \in \Lambda$, then $z \in \mathcal{A}_{\Pi\Lambda}$ if and only if $\operatorname{mod}_{\Pi\Lambda}(z) = z$. Equivalently, if $z \in \Lambda$, then $z \in \mathcal{A}_{\Pi\Lambda}$ if and only if $Q_\Lambda(z/\Pi) = 0$.*

We now briefly digress to address a technicality. In order for Proposition 10 to be true, we must either have there be no lattice points on the boundary of the Voronoi region of zero for the quantizer $Q_{\Pi\Lambda}$ or we should choose tie-breaking rules for (23) carefully as to guarantee that the modulo function yields unique coset representatives. In this paper, we will not be considering constellations where this is an issue. We refer

$ \Pi ^2$	Π	$ \Pi ^2$	Π
5	$2 + 1i$	97	$9 + 4i$
13	$3 + 2i$	101	$10 + 1i$
17	$4 + 1i$	109	$10 + 3i$
29	$5 + 2i$	113	$8 + 7i$
41	$5 + 4i$	157	$6 + 11i$
53	$7 + 2i$	241	$4 + 15i$
61	$6 + 5i$	257	$1 + 16i$
73	$8 + 3i$	373	$7 + 18i$
89	$8 + 5i$	389	$10 + 17i$

TABLE I
SOME GAUSSIAN PRIMES

$ \Pi ^2$	Π	$ \Pi ^2$	Π
7	$3 + 1\omega$	73	$9 + 1\omega$
13	$4 + 1\omega$	79	$10 + 3\omega$
19	$5 + 2\omega$	97	$11 + 3\omega$
29	$5 + 2\omega$	103	$11 + 2\omega$
31	$6 + 1\omega$	109	$12 + 5\omega$
37	$7 + 3\omega$	127	$13 + 6\omega$
43	$7 + 1\omega$	241	$15 + 16\omega$
61	$9 + 4\omega$	271	$9 + 19\omega$
67	$9 + 2\omega$	277	$12 + 19\omega$

TABLE II
SOME EISENSTEIN PRIMES

the reader to [63] for a treatment of this fine point since it is otherwise important.

Observe that for any $\Pi = a + bi \in \mathbb{G} \setminus \{0\}$, we have $|\Pi|^2 = |a + bi|^2 = a^2 + b^2$, and for any $\Pi = a + b\omega \in \mathbb{E} \setminus \{0\}$, we have $|\Pi|^2 = |a + b\omega|^2 = a^2 - ab + b^2$. In light of this, the following classical results of number theory will characterize the constellation sizes that we can obtain if we insist that $|\Pi|^2$ is prime in \mathbb{Z} . The first can be found in [59] and the second can be found in [64].

Theorem. *Let p be a prime in \mathbb{Z} greater than 2. Then, $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$ if and only if $p = 4n + 1$ for some $n \in \mathbb{Z}$.*

Theorem. *Let p be a prime in \mathbb{Z} greater than 3. Then, $p = a^2 - ab + b^2$ for some $a, b \in \mathbb{Z}$ if and only if $p = 3n + 1$ for some $n \in \mathbb{Z}$.*

Thus, we are restricted to constellations of prime size p where p is $4n + 1$ for Gaussian integer constellations or $3n + 1$ for Eisenstein integer constellations for some $n \in \mathbb{Z}$. When $p = 12n + 1$ for some $n \in \mathbb{Z}$, we can choose between a Gaussian and Eisenstein integer constellation. The Eisenstein integers are more densely packed making them preferable absent any other considerations.

It can be shown (see, [5], [6]) that $\{0, 1, \dots, |\Pi|^2 - 1\}$ are a complete set of coset representatives so that we have

$$\mathcal{A}_{\Pi\Lambda} = \{\text{mod}_{\Pi\Lambda}(z) \mid z \in \{0, 1, \dots, |\Pi|^2 - 1\}\}.$$

Finally, we have the following theorem:

Theorem 11 (Part of Robert Breusch's Extension of Bertrand's Postulate [65]). *There is at least one prime p of the form $p = 4n + 1$ for some $n \in \mathbb{Z}$ and at least one prime p' of the form $p' = 3n' + 1$ for some $n' \in \mathbb{Z}$ between m and $2m$ for any $m \geq 7$.*

This means that for any desired constellation size, we can always find a constellation which is at worst twice the size of what is required. Importantly, this will imply the existence of codes close to the constellation size lower bounds in Fig. 1 for arbitrary parameters.

The following theorem consolidates results from [3]–[6], [23].

Theorem 12 (Gaussian [3], [4], [6], [23] and Eisenstein [5], [6] Integer Maps Are Rank-Metric-Preserving). *Let Λ be \mathbb{G} or \mathbb{E} . Let Π be a prime in Λ with $|\Pi|^2$ a prime in \mathbb{Z} . Let $\mathbb{F}_{|\Pi|^2} = \mathbb{Z}_{|\Pi|^2} = \{0, 1, \dots, |\Pi|^2 - 1\}$. The map $\phi: \mathbb{F}_{|\Pi|^2} \rightarrow \mathcal{A}_{\Pi\Lambda}$*

defined by $\phi(z) = \text{mod}_{\Pi\Lambda}(z)$ for all $z \in \mathbb{F}_{|\Pi|^2}$ and evaluated in \mathbb{C} is rank-metric-preserving.

A detailed proof of this theorem would be essentially identical to the proof of a very similar theorem for $\Lambda = \mathbb{E}$ occurring in [5] so we will omit it.

Finally, we consider another kind of rank-metric preserving map which occurs as a special case of the code construction technique in [7]. The proof of the main result in [7] can be seen to encompass a proof of the following theorem:

Theorem 13 (p -PSK Map Is Rank-Metric-Preserving [7]).

Let $\mathbb{F}_p = \mathbb{Z}_p = \{0, 1, \dots, p - 1\}$ with p a prime. The map $\phi: z \mapsto \exp\left(\frac{i2\pi z}{p}\right)$ evaluated in \mathbb{C} is rank-metric-preserving.

D. Rate-Diversity Optimal Multiblock Space-Time Codes

We now provide explicit constructions of rate-diversity optimal multiblock space-time codes which arise as a straightforward consequence of what has been discussed thus far. For the cases of $T \geq n_t$ and $T \leq n_t$, we name the constructions *Sum-Rank A (SRA)* and *Sum-Rank B (SRB)* respectively. In the case of $T = n_t$, the constructions differ by a transposition of the sub-codewords and SRB will be preferable for convenience in the decoding procedure.

Proposition 14 (SRA Construction). *Fix positive integers n_t , T , L , d , and q with $T \geq n_t$, $d \leq Ln_t$, and q a prime power satisfying $q > L$. Let \mathcal{A} be a constellation of size q and let $\phi: \mathbb{F}_q \rightarrow \mathcal{A}$ be a rank-metric-preserving map with $\tilde{\phi}: \mathbb{F}_q^{n_t \times T} \rightarrow \mathcal{A}^{n_t \times T}$ the corresponding entrywise map. Let $\mathcal{B} = (\beta_1, \dots, \beta_T)$ be an ordered basis of \mathbb{F}_{q^T} over \mathbb{F}_q and $M_{\mathcal{B}}: \mathbb{F}_q^{n_t} \rightarrow \mathbb{F}_q^{T \times n_t}$ be a matrix representation map. Let $G_1, \dots, G_L \in \mathbb{F}_{q^T}^{(Ln_t - d + 1) \times n_t}$ be the sub-codeword generators of an $[Ln_t, Ln_t - d + 1]_{q^T}$ linearized Reed-Solomon code. Then, the L -block $n_t \times T$ space-time code \mathcal{X}_{SRA} completely over \mathcal{A} defined by*

$$\mathcal{X}_{\text{SRA}} = \left\{ \begin{bmatrix} \tilde{\phi}(M_{\mathcal{B}}(\mathbf{u}G_1)^T) & \cdots & \tilde{\phi}(M_{\mathcal{B}}(\mathbf{u}G_L)^T) \end{bmatrix} \mid \mathbf{u} \in \mathbb{F}_{q^T}^{Ln_t - d + 1} \right\}$$

has transmit diversity gain d and is rate-diversity optimal.

Proof. We have $|\mathcal{X}_{\text{SRA}}| = q^{T(Ln_t - d + 1)}$ yielding rate $R = n_t - (d - 1) \cdot L^{-1}$ so that (R, d) is an optimal rate-diversity pair. We then have

$$\begin{aligned} d &= Ln_t - LR + 1 \\ &\geq \min_{\substack{\mathbf{u}, \mathbf{v} \in \mathbb{F}_{q^T}^{Ln_t - d + 1} \\ \mathbf{u} \neq \mathbf{v}}} \sum_{\ell=1}^L \text{rank}(\tilde{\phi}(M_{\mathcal{B}}(\mathbf{u}G_{\ell})^T) - \tilde{\phi}(M_{\mathcal{B}}(\mathbf{v}G_{\ell})^T)) \\ &\geq \min_{\substack{\mathbf{u}, \mathbf{v} \in \mathbb{F}_{q^T}^{Ln_t - d + 1} \\ \mathbf{u} \neq \mathbf{v}}} \sum_{\ell=1}^L \text{rank}(M_{\mathcal{B}}(\mathbf{u}G_{\ell})^T - M_{\mathcal{B}}(\mathbf{v}G_{\ell})^T) \\ &= \min_{\substack{\mathbf{u}, \mathbf{v} \in \mathbb{F}_{q^T}^{Ln_t - d + 1} \\ \mathbf{u} \neq \mathbf{v}}} \sum_{\ell=1}^L \text{rank}(M_{\mathcal{B}}(\mathbf{u}G_{\ell}) - M_{\mathcal{B}}(\mathbf{v}G_{\ell})) = d \end{aligned}$$

where the first inequality is by the rate–diversity tradeoff (Theorem 2) and the last equality is by the MSRD property of linearized Reed–Solomon codes (Theorem 9). Therefore, \mathcal{X}_{SRA} achieves the rate–diversity pair (R, d) . \square

We can similarly show the following:

Proposition 15 (SRB Construction). *Fix positive integers n_t , T , L , d , and q with $T \leq n_t$, $d \leq LT$, and q a prime power satisfying $q > L$. Let \mathcal{A} be a constellation of size q and let $\phi: \mathbb{F}_q \rightarrow \mathcal{A}$ be a rank-metric-preserving map with $\tilde{\phi}: \mathbb{F}_q^{n_t \times T} \rightarrow \mathcal{A}^{n_t \times T}$ the corresponding entrywise map. Let $\mathcal{B} = (\beta_1, \dots, \beta_{n_t})$ be an ordered basis of $\mathbb{F}_{q^{n_t}}$ over \mathbb{F}_q and $M_{\mathcal{B}}: \mathbb{F}_{q^{n_t}}^T \rightarrow \mathbb{F}_q^{n_t \times T}$ be a matrix representation map. Let $G_1, \dots, G_L \in \mathbb{F}_{q^{n_t}}^{(LT-d+1) \times T}$ be the sub-codeword generators of an $[LT, LT-d+1]_{q^{n_t}}$ linearized Reed–Solomon code. Then, the L -block $n_t \times T$ space–time code \mathcal{X}_{SRB} completely over \mathcal{A} defined by*

$$\mathcal{X}_{\text{SRB}} = \left\{ \begin{bmatrix} \tilde{\phi}(M_{\mathcal{B}}(\mathbf{u}G_1)) & \dots & \tilde{\phi}(M_{\mathcal{B}}(\mathbf{u}G_L)) \end{bmatrix} \mid \mathbf{u} \in \mathbb{F}_{q^{n_t}}^{LT-d+1} \right\}$$

has transmit diversity gain d and is rate–diversity optimal.

A consequence of the underlying codes in the SRA and SRB constructions being MDS is the following:

Corollary. *Let \mathcal{X} be an L -block $n_t \times T$ SRA or SRB code completely over \mathcal{A} with X sampled uniformly at random from \mathcal{X} . Then, $(X)_{ij}$ is uniformly distributed over \mathcal{A} for $i = 1, \dots, n_t$, $j = 1, \dots, LT$ and we have*

$$\mathbb{E}[\|X\|_F^2] = \frac{n_t LT}{|\mathcal{A}|} \sum_{a \in \mathcal{A}} |a|^2.$$

We can also interpret these constructions in terms of the signalling complexity perspective provided in Section III-B. In particular, we have the following:

Corollary. *Fix positive integers n_t , T , and L . Fix some $R_{b/\text{tx}}$ and some ε satisfying $0 \leq \varepsilon < 1$. Let*

$$B = \max\{7, L+1, \lceil F_\varepsilon(L \cdot \min\{n_t, T\}) \rceil\} \quad (24)$$

where F_ε is as defined in (14). Then, there exists a constellation $\mathcal{A} \subset \mathbb{G}$ (or $\mathcal{A} \subset \mathbb{E}$) such that $B \leq |\mathcal{A}| < 2B$ and an L -block $n_t \times T$ space–time code completely over \mathcal{A} achieving a transmit diversity gain of $d = \lfloor (1-\varepsilon) \cdot L \cdot \min\{n_t, T\} \rfloor$ and a bpcu/tx rate of at least $R_{b/\text{tx}}$.

As will be seen later in Fig. 9, it will usually be the case for the parameters of interest that the $L+1$ in (24) does not come into play. Consequently, we will be able to construct codes near the constellation size lower bounds in Fig. 1.

We conclude this section by commenting briefly on connections to other constructions. In the case of $T \geq Ln_t$, we can replace linearized Reed–Solomon codes with Gabidulin codes and, by Corollary 7.1, we will have a rate–diversity optimal code which coincides with a special case of the multiblock construction in [7] when a p -PSK map (Theorem 13) is used. Moreover, in the case of $L = 1$, linearized Reed–Solomon codes become Gabidulin codes and these codes will become identical to those in [3], [4] when a Gaussian integer

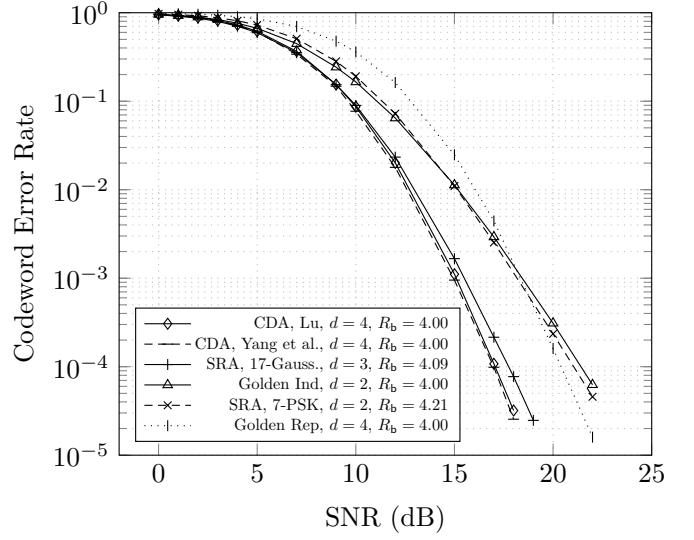


Fig. 3. Performance of coding across $L = 2$ fading blocks of a 2×2 MIMO channel

constellation is used and identical to those in [5] when an Eisenstein integer constellation is used.

V. SIMULATIONS

In this section, we study the performance of the proposed codes under ML decoding in comparison to competing codes. We defer the description of the decoders which were used to obtain the simulation results to Section VI.

For the entirety of this section, we will have $n_r = n_t = T$. We will refer to Gaussian and Eisenstein integer constellations of size p as p -Gauss. and p -Eis. constellations respectively.

A. The Case of $L = 2$

We begin with the case of coding across two fading blocks with $n_t = 2$ and consider a bpcu/tx rate of 2. Since the proposed codes require certain prime constellation sizes, they will not exactly achieve this bpcu/tx rate. We will typically choose constellations so that the bpcu rate is at least what is required. Moreover, the total available transmit diversity gain in this case is $Ln_t = 4$.

A variety of codes are considered and the codeword error rate (CER) versus SNR curves are provided in Fig. 3. We also provide all of the corresponding constellations in Figures 4 and 5. We will proceed to describe these codes.

We provide two $d = 4$ CDA-based 2-block linear dispersion codes as a reference both using 4-QAM input constellations to achieve a bpcu rate of 4. One is due to Lu [18] and the other is due to Yang and Belfiore [19]. We then provide our SRA construction with $d = 3$ and a 17-Gauss. constellation to achieve a bpcu rate of 4.09. It can be seen that the SRA code performs worse but the gap is less than 1 dB at a CER of 10^{-4} . In exchange, the constellation size is significantly smaller as can be seen in Figures 4 and 5. Moreover, we see from (13) that the code due to Yang and Belfiore [19] is also rate–diversity optimal hence the smaller constellation than that of Lu [18].

We further provide as a reference the performance of a *single-block* full diversity linear dispersion code, namely the Golden Code [41]. It is used in our two-block channel in two ways. The first is with sending independent codewords in each fading block with a 4-QAM input constellation to achieve a bpcu rate of 4 and $d = 2$. We refer to this code, which is the Cartesian product of two Golden Codes, as *Golden Ind*. This yields the performance of coding across a single fading block as the code was designed for. We further provide the result of repeating a Golden Code codeword in each fading block. This is referred to as *Golden Rep*. This represents a trivial way of obtaining a full diversity, i.e., $d = 4$ code. To compensate for the rate loss, we use a 16-QAM input constellation to obtain a bpcu rate of 4. As can be seen in Fig. 3, this code performs quite poorly which verifies, in some sense, the nontriviality of the other $d = 4$ and $d = 3$ codes intended for multiblock channels.

Note that the Golden Ind and Golden Rep codes are *multi-block* codes constructed from the *single-block* Golden Code and can be analyzed as such. In particular, one can verify that the Golden Rep code is rate–diversity optimal. On the other hand, the Golden Ind code is not rate–diversity optimal. It has a rate of 1 while the maximum possible for $d = 2$ is 1.5. Again, this is in an $L = 2$ setting and would not be true if we were analyzing the Golden Code itself as a single-block code.

In light of this, we consider a rate–diversity optimal $d = 2$ code, particularly our SRA code with a 7-PSK constellation achieving a bpcu rate of 4.21. This performs comparably to the Golden Ind code. The higher bpcu rate achieved with a 7-PSK constellation is due to its rate–diversity optimality. Alternatively, we can interpret it as a result of exploiting the possibilities admitted by the sum-rank metric. For example, rather than always needing rank-distance-2 sub-codewords in at least one fading block which is the case for the Golden Ind code, rank-distance-1 sub-codewords may be transmitted in the first fading block provided that rank-distance-1 *or* rank-distance-2 sub-codewords occur in the next fading block. Indeed, such combinations do occur in the codebook.

Next, we consider increasing the bpcu/tx rate to 4 which corresponds to a bpcu rate of 8. This is achieved by using 16-QAM input constellations for the CDA-based codes of Lu [18] and Yang and Belfiore [19]. We compare these to our SRB codes with $d = 3$ and a few different constellations. The results and constellations for our codes are provided in Figures 6 and 7. The constellations for the competing codes cannot be easily plotted or found in this case, but the constellation size lower bound says that they should have a size of at least $2^{Ln_t R_{b/tx}} = 2^{16} = 65536$ points. In this case, the performance gap between our codes and the competing codes becomes worse, but our constellation sizes are again significantly smaller. Besides this, the results are self-explanatory and the better point density of the Eisenstein integers is evident.

B. The Case of $L = 4$

We now consider increasing L to 4 with $n_t = 2$ and a bpcu/tx rate of 2. In this case, the total available transmit diversity gain is $Ln_t = 8$.

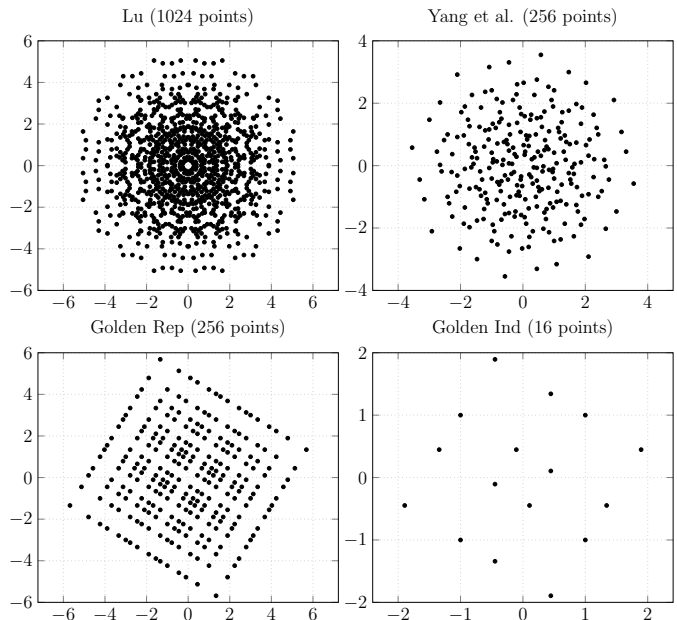


Fig. 4. Constellations for CDA-based codes

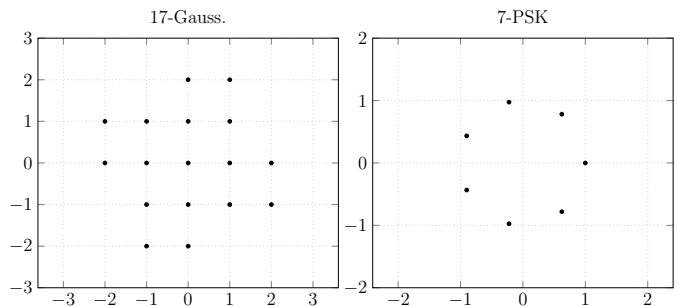


Fig. 5. Constellations for proposed codes

We provide the performance of a 4-block $d = 8$ CDA-based linear dispersion code due to Yang and Belfiore [19]. From our construction, we provide $d = 5$ and $d = 4$ SRB codes. Notably, our $d = 5$ code outperforms the $d = 8$ code with no sign of a closing performance gap over the range of simulated SNRs. Moreover, the $d = 8$ code has a constellation with at least 65536 points compared to 17 for our $d = 5$ code.

In Fig. 9, we provide constellation size lower bounds for $n_t = 2$ and $R_{b/tx} = 2$ as a function of L and some of the constellation sizes achieved by the codes discussed thus far. This also shows when the $|\mathcal{A}| \geq L + 1$ requirement of our construction might come into play.

C. The Case of $L = 1$

We now consider the case of $L = 1$. In this case, our SRA and SRB constructions recover the known space–time code constructions in [3]–[6] based on Gabidulin codes. However, in these works, no ML decoding techniques apart from exhaustive search are provided and there is consequently no ability to compare the performance of the codes to high-rate linear dispersion codes. Facilitated by the decoding techniques which will be introduced in Section VI, we are able to decode these

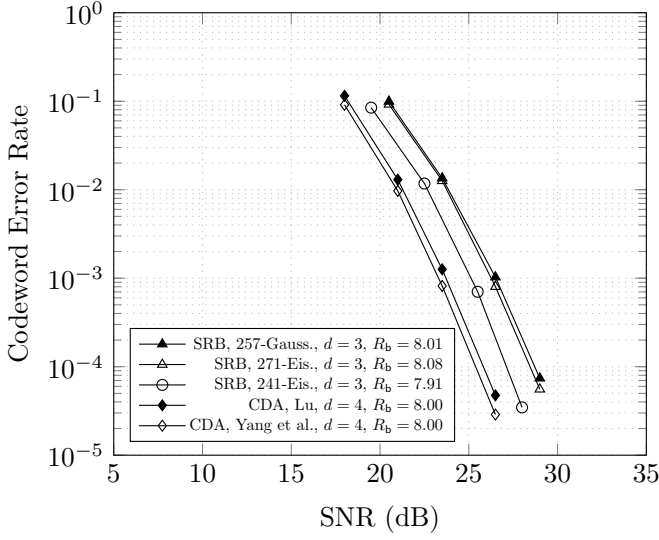


Fig. 6. Performance of coding across $L = 2$ fading blocks of a 2×2 MIMO channel

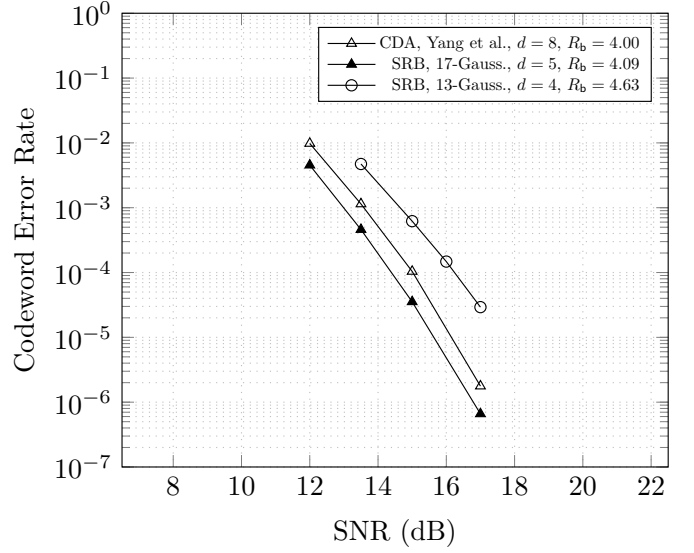


Fig. 8. Performance of coding across $L = 4$ fading blocks of a 2×2 MIMO channel

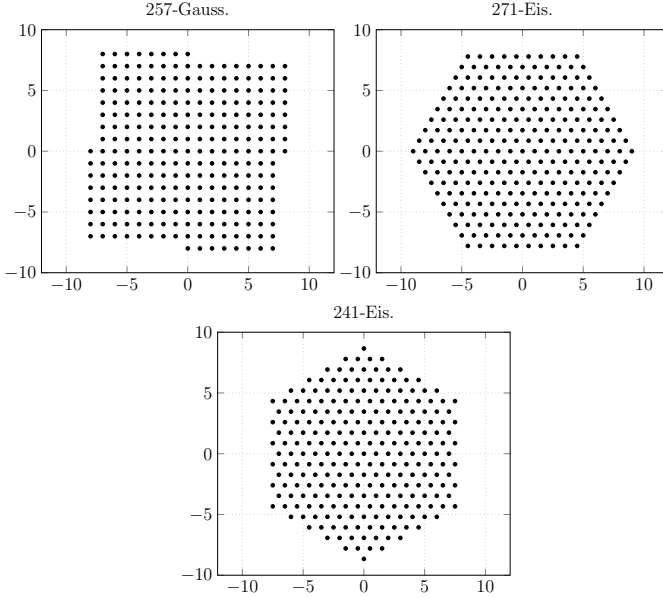


Fig. 7. Constellations for proposed codes

codes for the first time at sufficiently high bpcu rates to enable such a comparison.

In the case of $n_t = 2$, our codes have little to offer since the only options for the diversity gain are 2 which is full diversity and 1 which is achieved by uncoded signalling. Therefore, we skip to $n_t = 3$ in which case we have a total available diversity gain of $n_t = 3$. We consider target bpcu/tx rates of 2 and 3 and compare to the Perfect 3×3 codes from [20] using 4-HEX and 8-HEX input constellations which are also defined in [20]. The results are provided in Fig. 10. In this case, there are no admissible constellation sizes for our construction that get us close enough to the desired rate so the comparisons are not very fair. Nonetheless, one can see that the performances are close and our codes, as usual, have a constellation size advantage.

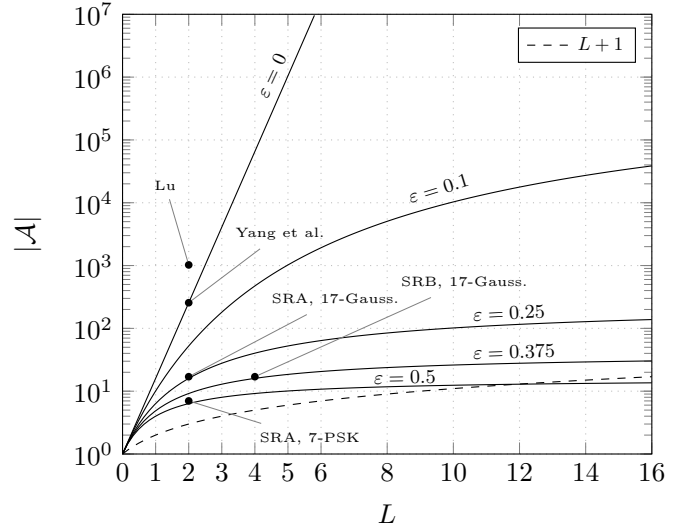


Fig. 9. Constellation size lower bounds for $R_b = 4$, $n_t = 2$, and $d = \lfloor (1 - \epsilon)Ln_t \rfloor$

We proceed to the case of $n_t = 4$ where we compare to the Perfect 4×4 code from [20]. We further compare to a code which improves upon this one which we refer to as *Improved* 4×4 . This code is from [21] which also credits [66]. We consider a target bpcu/tx rate of 2 which corresponds to a bpcu rate of 8 and 4-QAM input constellations for the competing codes. In this case, our $d = 3$ code with a 17-Gauss. constellation outperforms both codes all the way up to a CER of 10^{-6} and with a bpcu rate and constellation size advantage. On the other hand, a closing performance gap can be seen due to the diversity gain difference. Furthermore, the fact that the CERs for our code are only provided for high SNRs foreshadows another issue: this is that they can have a higher decoding complexity.

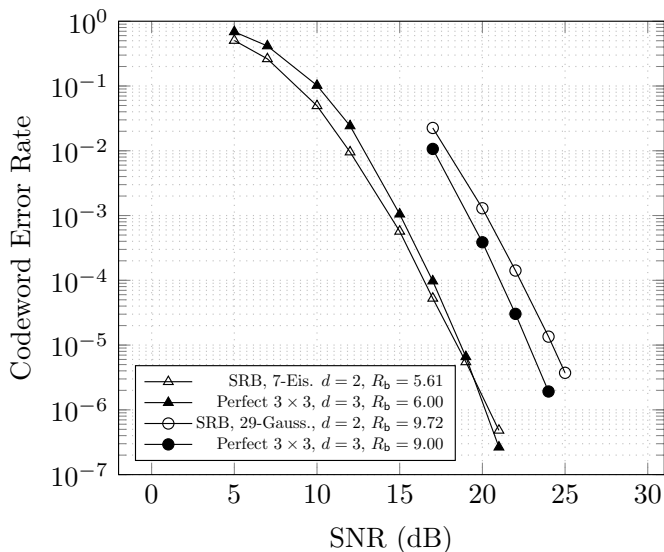


Fig. 10. Performance of single-block coding on a 3×3 MIMO channel

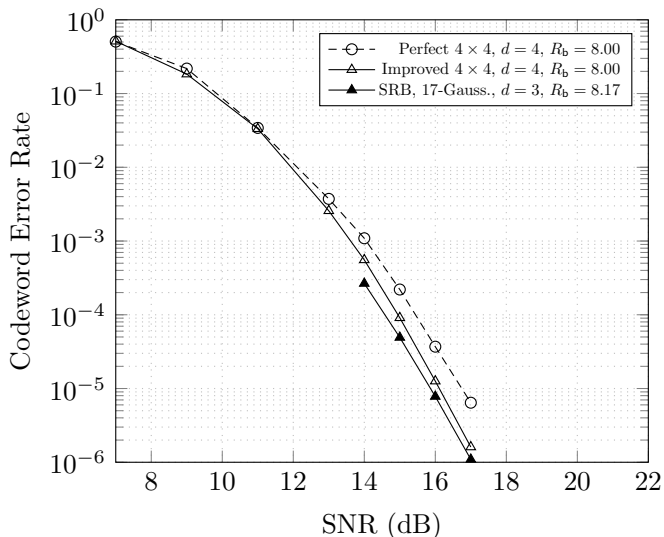


Fig. 11. Performance of single-block coding on a 4×4 MIMO channel

VI. DECODING

In this section, we provide an ML decoder for the proposed codes which combines ideas from the sequential decoding of linear block codes, optimal MIMO detection, and sphere decoding of linear dispersion codes. For concreteness of exposition, we describe a single family of decoders. However, in the process, we provide methods for more generally adapting some of the known techniques for the decoding of linear dispersion codes to both our codes and identically or similarly constructed space-time codes such as those of [3]–[5], [7]. The decoders to be considered are based on tree search algorithms which have good average-case complexity at high SNRs and exponential worst-case complexity in the codeword dimensions, as is typical.

While we will comment extensively on how the decoding problem for the proposed codes compares to the decoding

problem for the competing linear dispersion codes, we will not attempt to quantify the difference in computational complexity. Rather, we will have the less ambitious goal of providing a starting point for decoding and giving a sense of the challenges involved in comparison to linear dispersion codes. The central point to be made regarding this matter is as follows: There is one fundamental advantage and one fundamental disadvantage in the decoding problem for an SRA/SRB code in comparison to the decoding problem for a comparable linear dispersion code. The fundamental advantage is that the effective channel matrix when decoding the SRA/SRB code is block diagonal and there are many ways to exploit this. The fundamental disadvantage is that the tree structure for the SRA/SRB code is inherently worse. In particular, we must perform the decoding over a larger alphabet and over a search space with unfavorable boundaries. We also note that this point as well as the entire content of this section applies in the single-block, i.e., $L = 1$ setting as well.

The extent to which the advantage can compensate for the disadvantage is an open question and depends on the code parameters. Nonetheless, the advantage can certainly be exploited enough to make the decoding feasible. Moreover, this question neglects the potential benefits of smaller constellations to the implementation complexity so is not necessarily the pertinent question from an engineering perspective.

A. Summary of Existing Decoders

We begin by commenting on existing methods for decoding the proposed codes. In [5], the authors consider a suboptimal algebraic decoding technique for Gabidulin-based space-time codes which is, in principle, adaptable to SRA/SRB codes via the associated algebraic decoding methods for linearized Reed–Solomon codes [48], [67], but the performance is quite far from ML. To the best of the authors’ knowledge, there has been no other attempt at decoding space-time codes similar to the proposed codes aside from that in [5] and exhaustive search. With that said, the decoding methods to be proposed generalize existing methods in fairly straightforward ways. The methods to be built upon will be referred to as they occur in the upcoming development of a decoder.

B. The Vanilla Stack Decoder

In this subsection, we will describe a generic decoding technique and apply it to the decoding of the SRB code in the special case of $n_r = n_t$ with a focus on Gaussian or Eisenstein integer constellations. We will stick to this special case to simplify notation and exposition but we will comment on how deviations from this special case can be handled later.

We will begin by considering a general formulation of a minimum cost path finding problem on a tree. Our decoding problem will turn out to be a special case of this problem. The initial algorithm to be described which we refer to as a *vanilla stack decoder* is essentially a MIMO analogue of the Zigangirov–Jelinek stack decoding algorithm [68], [69]. Later on, it will evolve into an analogue of a stack decoder with variable bias-term (VBT) metric [70] which itself constitutes an instance of the A* algorithm [71]. The fundamental ideas

here are well-known and are constantly rediscovered in the literature. While the aforementioned literature was the starting point for the development of the proposed decoder, the closest pre-existing decoders to what we will describe are likely to be found in the sections in [37] relating to ML MIMO detection and the approaches described in [12], [13].

Following the introduction of the vanilla stack decoder, we will build upon it with improvements that exploit structure that is more specific to the decoding problem and to the code. These improvements will be quantified in simulations in Section VI-F.

We will now consider the problem of generically decoding a tree code. In this subsection and the others that will follow, we will make use of the language and notation of strings rather than vectors. Adjacent symbols (or characters) will represent concatenated strings rather than multiplication in \mathbb{C} unless otherwise indicated or suggested by context.

Consider a code \mathcal{S} of length n over a q -ary alphabet $\mathcal{A} = \{a_1, a_2, \dots, a_q\}$. That is, some $\mathcal{S} \subseteq \mathcal{A}^n$ with $|\mathcal{S}| > 1$. Any codeword $s \in \mathcal{S}$ is a string of length n so that $s = s_1 s_2 \dots s_n$ where $s_1, s_2, \dots, s_n \in \mathcal{A}$. Denote by \mathcal{A}^* the *Kleene closure* of \mathcal{A} . This is the set of all strings of any length over \mathcal{A} . That is,

$$\mathcal{A}^* = \{\epsilon, a_1, \dots, a_q, a_1 a_1, \dots, a_1 a_q, a_2 a_1, a_2 a_2, a_2 a_3, \dots\}$$

where ϵ here denotes the *empty string* which is the identity element of concatenation. That is, $\epsilon a = a \epsilon = a$. The length of a string will be denoted by $|\cdot|$ and the empty string has length zero, i.e., $|\epsilon| = 0$.

Denote by \mathcal{S}^* the set of all prefixes of codewords in \mathcal{S} . That is,

$$\mathcal{S}^* = \{p \in \mathcal{A}^* \mid pt \in \mathcal{S} \text{ for some } t \in \mathcal{A}^*\}.$$

Note that \mathcal{A}^* is an infinite set while \mathcal{S}^* is finite. Observe that if $p \in \mathcal{S}^*$ and $|p| = n$, then $p \in \mathcal{S}$.

Denote by $\wp(\mathcal{A})$ the power set of \mathcal{A} . This is the set of all subsets of \mathcal{A} . Define the function $E: \mathcal{S}^* \rightarrow \wp(\mathcal{A})$ by

$$E(p) = \{a \in \mathcal{A} \mid pa \in \mathcal{S}^*\}. \quad (25)$$

Thus, given a prefix of a codeword, this function gives us the set of all possible candidates for the next character. Observe that if $p \in \mathcal{S}^*$ and $pb \in \mathcal{S}$ for some $b \in \mathcal{A}$, then $b \in E(p)$. Moreover, if $p \in \mathcal{S}$, then $E(p) = \emptyset$.

Assuming that we can easily compute this function for our code, i.e., that we can easily enumerate the elements of this set, we can easily construct a representation of our code as a q -ary tree of depth n . Each node represents a prefix of a codeword and the leaf nodes correspond to the codewords. In particular, we can label the root node by ϵ . Its children at depth 1 are then labelled by the elements of $E(\epsilon) = \{a \in \mathcal{A} \mid a \in \mathcal{S}^*\}$. Given a child c at depth 1, we can find its children at depth 2 as $E(c) = \{a \in \mathcal{A} \mid ca \in \mathcal{S}^*\}$, and so on.

Consider n functions $f_i: \mathcal{A}^i \rightarrow \mathbb{R}_{\geq 0}$ for $i = 1, 2, \dots, n$. Define the cost function $C: \mathcal{S} \rightarrow \mathbb{R}_{\geq 0}$ by

$$\begin{aligned} C(a_1 a_2 \dots a_n) &= f_1(a_1) + f_2(a_1 a_2) + \dots + f_n(a_1 a_2 \dots a_n) \\ &= \sum_{j=1}^n f_j(a_1 a_2 \dots a_j) \end{aligned} \quad (26)$$

for all $a_1 a_2 \dots a_n \in \mathcal{S}$ (with $a_1, a_2, \dots, a_n \in \mathcal{A}$). We refer to such a function as a *causal cost function*. Given such a function, we can replace it by one which is extended to arbitrary length prefixes. Define the *extended causal cost function* $C: \mathcal{S}^* \rightarrow \mathbb{R}_{\geq 0}$ for arguments of length i by

$$\begin{aligned} C(a_1 a_2 \dots a_i) &= f_1(a_1) + f_2(a_1 a_2) + \dots + f_i(a_1 a_2 \dots a_i) \\ &= \sum_{j=1}^i f_j(a_1 a_2 \dots a_j) \end{aligned} \quad (27)$$

for all $a_1 a_2 \dots a_i \in \mathcal{S}^*$ (with $a_1, a_2, \dots, a_i \in \mathcal{A}$) for $i = 1, 2, \dots, n$. Observe that the function can now be defined recursively for each argument by

$$C(a_1 a_2 \dots a_i) = C(a_1 a_2 \dots a_{i-1}) + f_i(a_1 a_2 \dots a_i)$$

and

$$C(a_1) = f_1(a_1)$$

for $i = 2, 3, \dots, n$.

Suppose that we are interested in solving

$$\min_{s \in \mathcal{S}} C(s).$$

A problem of this form can be solved by a best-first tree search algorithm like the Zigangirov–Jelinek stack decoding algorithm [68], [69]. Traditionally, these algorithms are used in the context of binary codes ($|\mathcal{A}| = 2$) and where the cost function is simple. In particular, we usually have no dependence on previous symbols in the additive decomposition of the cost function. That is, $f_i(a_1 a_2 \dots a_i) = g_i(a_i)$ for some $g_i: \mathcal{A} \rightarrow \mathbb{R}_{\geq 0}$. Fortunately, the generalization to allow for arbitrary causal cost functions is effortless.

We will now describe this algorithm. The algorithm will make use of a priority queue data structure. This is a stack with *push* and *pop* operations. However, rather than having a last-in first-out (LIFO) order, the elements are paired with priority measures and sorted accordingly so that the element with the highest priority comes out first. Each entry in our priority queue will be a codeword prefix $p \in \mathcal{S}^*$ and a priority measure which will be its cost $C(p)$. The highest priority element will be the one with the smallest cost. The algorithm can now be described very simply:

- Start by pushing every $a \in E(\epsilon)$ onto the priority queue with its respective cost $C(a) = f_1(a)$.
- Pop an element from the priority queue which will consist of a prefix p and its priority measure $C(p)$.
- For every $t \in E(p)$, push pt onto the priority queue with its priority measure $C(pt) = C(p) + f_{|p|+1}(pt)$.
- Repeat the previous two steps until a prefix s with $|s| = n$ is popped.

For a proof that this algorithm works, i.e., terminates and yields the minimum cost codeword, the reader is referred to [29]. Alternatively, the reader may simply recognize this as an instance of a standard best-first search algorithm like A* [71].

Application to the Decoding of the Proposed Codes: We now proceed to the application of this to the decoding of our space-time codes. We can associate an $n_t \times LT$ codeword matrix with a length- LTn_t string via the bijection defined by:

$$\begin{bmatrix} x_1 & x_{n_t+1} & \cdots & x_{(LT-1)n_t+1} \\ x_2 & x_{n_t+2} & \cdots & x_{(LT-1)n_t+2} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n_t} & x_{2n_t} & \cdots & x_{LTn_t} \end{bmatrix} \mapsto x_1 x_2 \cdots x_{LTn_t}.$$

Our code \mathcal{X} is thus in bijection with a code \mathcal{S} as defined in the previous section. We will also use a similar representation for our receive matrix which will also be $n_t \times LT$ since we are assuming that $n_r = n_t$.

The first order of business is to find the function E . Since the underlying code is MDS, this is easy. Let k be the dimension of the linearized Reed-Solomon code ($k = LT - d + 1$ for the SRB construction) and assume that we are using a systematic generator matrix. Then, for all $p \in \mathcal{S}^*$ such that $|p| < kn_t$, we have $E(p) = \mathcal{A}$. On the other hand, for any $p \in \mathcal{S}^*$ with $|p| \geq kn_t$, the entire remaining symbols are parity symbols which can be computed from the first kn_t symbols so we have $|E(p)| = 1$, i.e., there is only one possible continuation of the prefix. Fig. 12 illustrates the structure of the resulting code tree.

It remains to verify that the cost function has the appropriate form. This is merely a matter of performing QL decompositions. Recall our convention that $X = [X_1 \ X_2 \ \cdots \ X_L]$. For $\ell = 1, 2, \dots, L$, we have

$$\|Y_\ell - \rho H_\ell X_\ell\|_F^2 = \|\tilde{Y}_\ell - \mathbf{L}_\ell X_\ell\|_F^2$$

where $\rho H_\ell = Q_\ell \mathbf{L}_\ell$ and $\tilde{Y}_\ell = Q_\ell^\dagger Y_\ell$ where Q_ℓ is a unitary matrix and \mathbf{L}_ℓ is a lower-triangular matrix. Moving forward, we will drop the tilde from the \tilde{Y}_ℓ . Denote by $\ell(j)$ the index of the fading block corresponding the j th column of X , i.e.,

$$\ell(j) = \left\lfloor \frac{j-1}{T} \right\rfloor + 1$$

for $j = 1, 2, \dots, LT$. For $m = 1, 2, \dots, n_t LT$, define the functions $g_m: \mathcal{A}^{m - \lfloor \frac{m-1}{n_t} \rfloor n_t} \rightarrow \mathbb{R}_{\geq 0}$ by

$$g_m(x_{\lfloor \frac{m-1}{n_t} \rfloor n_t + 1} x_{\lfloor \frac{m-1}{n_t} \rfloor n_t + 2} \cdots x_m) = \left| y_m - \sum_{k=\lfloor \frac{m-1}{n_t} \rfloor n_t + 1}^m \left(\mathbf{L}_{\ell(\lfloor \frac{m-1}{n_t} \rfloor + 1)} \right)_{m - \lfloor \frac{m-1}{n_t} \rfloor n_t, k - \lfloor \frac{m-1}{n_t} \rfloor n_t} x_k \right|^2$$

We then have (see [29] for details)

$$\begin{aligned} C(x_1 x_2 \cdots x_{LTn_t}) &= \sum_{\ell=1}^L \|Y_\ell - \mathbf{L}_\ell X_\ell\|_F^2 \\ &= \sum_{m=1}^{LTn_t} g_m(x_{\lfloor \frac{m-1}{n_t} \rfloor n_t + 1} x_{\lfloor \frac{m-1}{n_t} \rfloor n_t + 2} \cdots x_m) \\ &= \sum_{m=1}^{LTn_t} f_m(x_1 x_2 \cdots x_m) \end{aligned}$$

where

$$f_m(x_1 x_2 \cdots x_m) = g_m(x_{\lfloor \frac{m-1}{n_t} \rfloor n_t + 1} x_{\lfloor \frac{m-1}{n_t} \rfloor n_t + 2} \cdots x_m)$$

for $m = 1, 2, \dots, LTn_t$. Thus, we have a causal cost function as required and the vanilla stack decoder is fully specified. In fact, we have something better than what we needed. Each function in the additive decomposition of the cost function depends on at most n_t previous terms rather than at most LTn_t previous terms.

Alternatively, we can interpret this as the *effective channel matrix* being block diagonal with lower-triangular blocks. In particular, we can express the cost function as

$$C(x_1 x_2 \cdots x_{LTn_t}) = \|\mathbf{y} - \mathbf{H}\mathbf{x}\|_2^2 \quad (28)$$

where (recalling that $n_r = n_t$) $\mathbf{x}, \mathbf{y} \in \mathbb{C}^{n_t LT}$ are given by

$$\begin{aligned} \mathbf{x} &= [x_1 \ x_2 \ \cdots \ x_{n_t LT}]^\top \\ \mathbf{y} &= [y_1 \ y_2 \ \cdots \ y_{n_t LT}]^\top \end{aligned}$$

and $\mathbf{H} \in \mathbb{C}^{n_t LT \times n_t LT}$ is given by

$$\mathbf{H} = \begin{bmatrix} \mathbf{L}_1 & & & & \\ & \ddots & & & \\ & & \mathbf{L}_1 & & \\ & & & \mathbf{L}_2 & \\ & & & & \ddots \\ & & & & & \mathbf{L}_2 \\ & & & & & & \ddots \\ & & & & & & & \mathbf{L}_L \end{bmatrix} \quad (29)$$

where each $\mathbf{L}_\ell \in \mathbb{C}^{n_t \times n_t}$ for $\ell = 1, 2, \dots, L$ occurs T times on the diagonal of the matrix. On the other hand, the general case of a causal cost function depending on all LTn_t past terms corresponds to the matrix \mathbf{H} simply being lower-triangular.

Comparison to the Decoding of Linear Dispersion Codes: As previously mentioned, the decoding problem for a linear dispersion code can be converted into a standard MIMO detection problem for an $n_t LT \times 1$ vector over the input constellation with an $n_t LT \times n_t LT$ channel (assuming $n_r = n_t$). In particular, suppose that we have an L -block $n_t \times T$ linear dispersion code as defined in (12) with dispersion matrices $A_1, A_2, \dots, A_{n_t LT} \in \mathbb{C}^{n_t \times LT}$. Denote by $\mathbf{a}_i^{(j)}$ the j th column of the i th dispersion matrix so that

$$A_i = [\mathbf{a}_i^{(1)} \ \mathbf{a}_i^{(2)} \ \cdots \ \mathbf{a}_i^{(LT)}]$$

for $i = 1, 2, \dots, n_t LT$. One can then verify that the cost function can be placed into the form of (28) by taking

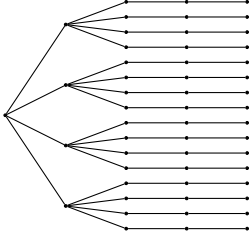


Fig. 12. Structure of the code tree resulting from a systematic generator matrix

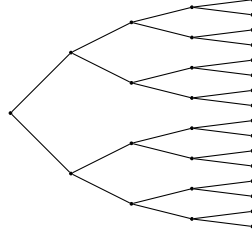


Fig. 13. Structure of the code tree resulting from a linear dispersion code or uncoded signalling

$\mathcal{S} = \mathcal{A}_{\text{in}}^{n_t LT}$ (which is in bijection with the code) and taking $\mathbf{H} \in \mathbb{C}^{n_t LT \times n_t LT}$ to be

$$\mathbf{H} = \rho \begin{bmatrix} H_1 \mathbf{a}_1^{(1)} & H_1 \mathbf{a}_2^{(1)} & \cdots & H_1 \mathbf{a}_{n_t LT}^{(1)} \\ H_1 \mathbf{a}_1^{(2)} & H_1 \mathbf{a}_2^{(2)} & \cdots & H_1 \mathbf{a}_{n_t LT}^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ H_1 \mathbf{a}_1^{(T)} & H_1 \mathbf{a}_2^{(T)} & \cdots & H_1 \mathbf{a}_{n_t LT}^{(T)} \\ H_2 \mathbf{a}_1^{(T+1)} & H_2 \mathbf{a}_2^{(T+1)} & \cdots & H_2 \mathbf{a}_{n_t LT}^{(T+1)} \\ H_2 \mathbf{a}_1^{(T+2)} & H_2 \mathbf{a}_2^{(T+2)} & \cdots & H_2 \mathbf{a}_{n_t LT}^{(T+2)} \\ \vdots & \vdots & \ddots & \vdots \\ H_L \mathbf{a}_1^{(LT)} & H_L \mathbf{a}_2^{(LT)} & \cdots & H_L \mathbf{a}_{n_t LT}^{(LT)} \end{bmatrix}. \quad (30)$$

Observe now that the problem of minimizing (28) is itself a special case of our decoding problem so that the algorithm just developed is readily applicable. In particular, we substitute 1 for L and T and substitute $n_t LT$ for n_t . We can then lower-triangularize the channel as before to get a causal cost function or equivalently, a new effective channel

$$\mathbf{H} = \mathbf{L}_1 \quad (31)$$

where $\mathbf{L}_1 \in \mathbb{C}^{n_t LT \times n_t LT}$ is lower-triangular. Thus, one key difference between the decoding problems for the proposed codes and linear dispersion codes is in the effective channels (29) for the proposed codes and (31) for linear dispersion codes. Apart from the obvious ways in which the block diagonal structure of (29) is better such as reduced cost of QL decompositions, we will see that there are many more significant advantages. We also emphasize that this structural benefit still holds in the case of single-block coding (i.e., $L = 1$).

On the other hand, since $\mathcal{S} = \mathcal{A}_{\text{in}}^{n_t LT}$ for a linear dispersion code, we will have a tree structure as in Fig. 13. The major advantage in the decoding of linear dispersion codes is that the decoding can be performed over the input constellation which will generally be smaller than the constellation for an equal bpcu rate SRB code. Observe that Figures 12 and 13 represent codes of equal size and hence equal bpcu rate but the latter has a smaller outdegree.

The key principle behind sequential decoding is that of pruning the tree of unpromising paths via the priority measure to avoid an exhaustive search. This is easier to do in the case of a tree like that in Fig. 13 rather than Fig. 12. In fact, for Fig. 12, the length of the long legs relative to the depth up to which we have a full tree is proportional to the diversity

gain. In the case of full diversity, the tree constitutes only long legs stemming from the root node and no meaningful pruning is possible; the vanilla stack decoder becomes an exhaustive search.

The proposed codes are thus inherently disadvantaged from a tree structure perspective and the closer they operate to full diversity, the closer the decoding complexity becomes to exhaustive search. Moreover, the tree structure is always worse for any diversity gain greater than 1 hence for any nontrivial code. With that said, we have seen that they do not need to be close to full diversity to perform well and we have the block diagonal effective channel advantage which can compensate to some extent for the tree structure disadvantage.

In the coming subsections, we will proceed to provide improvements upon the vanilla stack decoder. These improvements will typically involve some extra computations or pre-computations that offer diminishing returns as the SNR increases.

C. Future Costing

We now consider an improvement upon the vanilla stack decoder via the A* algorithm [71]. We adopt some of the terminology associated with A*. The idea is to add to the cost associated with a prefix a lower bound on the cost of any possible continuation of that prefix—the future cost. The hope is that this will cause more paths to be pruned early on in the decoding procedure.

Consider n heuristic functions $h_i: \mathcal{A}^i \rightarrow \mathbb{R}_{\geq 0}$ for $i = 1, 2, \dots, n$. Define the *modified extended causal cost function* $C': \mathcal{S}^* \rightarrow \mathbb{R}_{\geq 0}$ by

$$C'(a_1 a_2 \cdots a_i) = C(a_1 a_2 \cdots a_i) + h_i(a_1 a_2 \cdots a_i)$$

for all $a_1 a_2 \cdots a_i \in \mathcal{S}^*$ (with $a_1, a_2, \dots, a_i \in \mathcal{A}$) for $i = 1, 2, \dots, n$. The heuristic functions are said to be *admissible* if

$$h_i(a_1 \cdots a_i) \leq \min_{\substack{b_1 \cdots b_n \in \mathcal{S} \\ b_1 \cdots b_i = a_1 \cdots a_i}} f_{i+1}(b_1 \cdots b_{i+1}) + \cdots + f_n(b_1 \cdots b_n) \quad (32)$$

for all $a_1 a_2 \cdots a_i \in \mathcal{S}^*$ (with $a_1, a_2, \dots, a_i \in \mathcal{A}$) for $i = 1, 2, \dots, n-1$ and

$$h_n(a_1 \cdots a_n) = 0$$

for all $a_1 \cdots a_n \in \mathcal{S}$.

We claim that if the cost function in the vanilla stack decoder is replaced with a modified extended causal cost function with admissible heuristics, the algorithm still terminates and yields the minimum cost codeword. For a proof of this, again, the reader may simply recognize this as an instance of A* [71] or refer to [29].

Application to the Decoding of the Proposed Codes: The utility of a heuristic relies critically on the complexity of its evaluation. Solving the minimization in (32) for every $a_1 a_2 \cdots a_i \in \mathcal{S}^*$ for $i = 1, 2, \dots, n$ is just as hard as the decoding problem that we are trying to solve to start with. We instead hope to find lower bounds on that minimization that are sufficiently easy to compute. The particular topic of obtaining such bounds in the context of sphere decoding is

studied extensively in [15]. The same topic is studied in [16] in the context of MIMO detection with an A* algorithm and the authors arrive at a bound equivalent to one appearing in [15]. The techniques from these works are more or less readily applicable to our decoder. In particular, one might need to relax the constellation constraints to $\Lambda = \mathbb{G}$ or $\Lambda = \mathbb{E}$ in which case the appropriate quantization functions can be applied to get constant-time solutions to 1-dimensional detection problems. This has the effect of slightly loosening the resultant bounds.

However, there is one way in which our problem differs from those considered in [15], [16] that we can exploit. This is in that we have a block diagonal lower-triangular effective channel matrix (29) rather than a dense lower-triangular effective channel matrix (31). This gives the proposed codes a decoding advantage in the particular area of A* heuristics. We interject to elaborate.

Comparison to the Decoding of Linear Dispersion Codes: Earlier, we showed that our cost function additively decomposes into functions which depend on at most the past n_t terms

$$f_m(x_1 x_2 \cdots x_m) = g_m(x_{\lfloor \frac{m-1}{n_t} \rfloor n_t + 1} x_{\lfloor \frac{m-1}{n_t} \rfloor n_t + 2} \cdots x_m)$$

for $m = 1, 2, \dots, LTn_t$.

On the other hand, in the decoding of linear dispersion codes, it is neither feasible nor intended that the codeword be considered directly in the decoding process due to the enormous constellation size. Rather, they are intended to be decoded over their *input* constellation. For this to be done, the channel matrices must be combined with the generator matrices leading to an $n_t LT \times n_t LT$ effective channel (30) acting on a single $n_t LT \times 1$ vector with symbols from the input constellation. After lower-triangularizing the channel, the cost function thus ends up taking the most general form (26) with dependence on the past $n_t LT$ symbols.

The implication this has for heuristics is that they need to be constantly re-computed on the fly as nodes are explored since the minimization depends on the previous symbols. This strongly restricts the complexity allowed for these heuristics. Naïve choices lead to complexity equivalent to that of simply visiting the nodes that we are trying to prune. In contrast, if the cost function breaks up as it does for the proposed codes, we get heuristics that can be pre-computed and are identical for any prefix. For example, we can solve the column-by-column MIMO detection problem or find a lower bound on its cost and this only has to be done once. The fact that it only has to be done once means that heuristics that would otherwise be useless, like solving a lower-dimensional version of the same decoding problem under consideration, are now potentially useful.

Application to the Decoding of the Proposed Codes Continued: We require that our heuristic satisfies

$$h_i(x_1 \cdots x_i) \leq \min_{\substack{z_1 \cdots z_n \in \mathcal{S} \\ z_1 \cdots z_i = x_1 \cdots x_i}} \sum_{j=i+1}^{LTn_t} f_j(z_1 \cdots z_j) \quad (33)$$

for $i = 1, 2, \dots, LTn_t - 1$ and $h_{LTn_t}(x_1 \cdots x_{LTn_t}) = 0$. As previously mentioned, such heuristics can be found in [15], [16]. However, we will shift our interest to heuristics that

do not depend on $x_1 \cdots x_i$ in which case we can use more complex heuristics (in the sense of computational complexity), that are conceptually trivial. In particular, simply solving smaller versions of the decoding problem under consideration.

Firstly, we can remove the codeword constraint for the purposes of the lower-bounding (33). That is,

$$\begin{aligned} & \min_{\substack{z_1 \cdots z_n \in \mathcal{S} \\ z_1 \cdots z_i = x_1 \cdots x_i}} \sum_{j=i+1}^{LTn_t} f_j(z_1 \cdots z_j) \\ & \geq \min_{\substack{z_1 \cdots z_n \in \mathcal{A}^{LTn_t} \\ z_1 \cdots z_i = x_1 \cdots x_i}} \sum_{j=i+1}^{LTn_t} f_j(z_1 \cdots z_j). \end{aligned}$$

We further would like that our heuristic does not depend on $x_1 \cdots x_i$. We can remove the appropriate number of terms from the beginning of the sum:

$$\begin{aligned} \sum_{j=i+1}^{LTn_t} f_j(z_1 \cdots z_j) & \geq \sum_{j=\lfloor \frac{i-1}{n_t} \rfloor n_t + n_t + 1}^{LTn_t} f_j(z_1 \cdots z_j) \\ & = \sum_{j=\lfloor \frac{i-1}{n_t} \rfloor n_t + n_t + 1}^{LTn_t} g_j(z_{\lfloor \frac{j-1}{n_t} \rfloor n_t + 1} \cdots z_j) \end{aligned} \quad (34)$$

where we have $\lfloor \frac{i-1}{n_t} \rfloor n_t + n_t + 1 \geq i + 1$ and (34) depends on $z_{\lfloor \frac{i-1}{n_t} \rfloor n_t + n_t + 1} \cdots z_{LTn_t}$.

There are three points that must be noted now. The first is that we can break up the sum (34) in any way we like and lower-bound its minimization by the term-by-term minimization of the broken up sum. The second is that we can lower-bound any terms trivially by 0. This allows us to obtain lower-bounds which consist of MIMO detection problems of any size, i.e, with 1×1 to $n_t \times n_t$ channels. The third is that these do not need to be computed for every $i = 1, 2, \dots, LTn_t - 1$ (this a separate matter from independence of $x_1 \cdots x_i$). The same heuristic will be shared by ranges of i and the heuristics for larger i just involve fewer terms of (34) so are obtained by subtracting components of the heuristic for smaller i .

For example, for $i = 1$, we can break down (34) into $LT - 1$ terms corresponding to the last $LT - 1$ columns of the codeword X :

$$\begin{aligned} & \sum_{j=n_t+1}^{2n_t} g_j(z_{\lfloor \frac{j-1}{n_t} \rfloor n_t + 1} \cdots z_j) + \sum_{j=2n_t+1}^{3n_t} g_j(z_{\lfloor \frac{j-1}{n_t} \rfloor n_t + 1} \cdots z_j) \\ & + \cdots + \sum_{j=(LT-1)n_t+1}^{LTn_t} g_j(z_{\lfloor \frac{j-1}{n_t} \rfloor n_t + 1} \cdots z_j). \end{aligned} \quad (35)$$

Minimizing each of these constitutes a standard MIMO detection problem with an $n_t \times n_t$ channel. These can be solved by another instance of the decoder we are describing—perhaps a more vanilla one to give us $LT - 1$ minima. The heuristic for $i = 1, 2, \dots, n_t$ would be the sum of these $LT - 1$ minima. For $i = n_t + 1, \dots, 2n_t$, it would be the sum of the last $LT - 2$ of these minima, and so on. This is in direct analogy to obtaining the cost of symbol-by-symbol hard decisions in the VBT metric decoder described in [70]. In fact, with $n_t = 1$ it would be precisely that but with a fading channel.

As previously mentioned, we need not solve an $n_t \times n_t$ problem, we can solve a 1×1 problem which would correspond to replacing (35) by the first term in each sum and costs almost nothing. The SNR and the codebook size will determine whether the computational effort put into computing the heuristic is made up for by a reduction of the complexity of the main tree search. For example, in obtaining the $n_t = 4$, $L = 1$ simulation result in the previous section, it was found that solving the $n_t \times n_t$ problem was worthwhile and significantly reduced the overall complexity.

Finally, note that we can mix and match heuristics such as those described here and those intended for dependence on $x_1 \cdots x_i$. Generally, if our codeword X is short and wide, we can get sufficiently tight heuristics which do not depend on the previous symbols, but if the codeword is tall and narrow, it might only be worthwhile to consider heuristics which depend on $x_1 \cdots x_i$ and simply apply the approaches in [15], [16].

Moreover, completely separately from this point, we can use the computationally less expensive heuristics in [15], [16] to lower-bound the terms of (35) rather than outright solve the minimizations. For example, we can consider the bound in [15] termed the *eigenbound* which is also independently arrived at in [16]. Take some $M \in \mathbb{C}^{n_t \times n_t}$ and $\mathbf{u}, \mathbf{v} \in \mathbb{C}^{n_t}$ with M invertible and let λ_{\min} be the smallest eigenvalue of the positive definite matrix $M^\dagger M$. Then, one can easily show that [15]

$$\|M\mathbf{u} - \mathbf{v}\|_2^2 \geq \lambda_{\min} \|\mathbf{u} - M^{-1}\mathbf{v}\|_2^2.$$

We can then perform the minimization over $\mathbf{u} \in \mathcal{A}^{n_t}$ component-wise. We can simplify this further by relaxing the minimization to over $\mathbf{u} \in \Lambda^{n_t}$ with $\Lambda = \mathbb{G}$ or \mathbb{E} and use the appropriate quantization function.

D. Spherical Bounding

We consider using a spherical bound stack decoder first proposed in [14]. This decoder is essentially a best-first variation on the depth-first sphere decoder [10], [11] which is a commonly used decoder for linear dispersion codes. The spherical bounding idea is to pick a threshold \mathcal{T} and restrict the search to the $s \in \mathcal{S}$ satisfying $C(s) \leq \mathcal{T}$. If there are no codewords satisfying $C(s) \leq \mathcal{T}$, increase \mathcal{T} and start over. Clearly, if we find the minimum cost codeword among the codewords whose cost is less than or equal to \mathcal{T} , then it must be the minimum cost codeword among all codewords so the resulting decoder is still ML.

The modification to the basic algorithm is simply as follows: Rather than pushing pt onto the stack for every $t \in E(p)$, we push pb onto the stack for every

$$b \in \{t \in E(p) \mid f_{|p|+1}(pt) \leq \mathcal{T} - C(p)\}. \quad (36)$$

There is now a possibility that the priority queue size will decrease because something popped might not be replaced. Nonetheless, one can simply increase \mathcal{T} and start over should the priority queue become empty. It can again be verified that the resulting algorithm works. Moreover, combining this with future costing is also straightforward.

The challenge now is in enumerating the elements of the set in (36). In the case of $|p| < kn_t$, we have $E(p) = \mathcal{A}$ so we must find the constellation points $t \in \mathcal{A}$ for which $f_{|p|+1}(pt) \leq \mathcal{T} - C(p)$. The naive way would be to go through all of the constellation points and compare to the threshold. However, this would give us only a space complexity reduction. In order to obtain a time complexity reduction, this must be done without going through all of the constellation points every time. We will start by showing that this problem amounts to finding the constellation points that lie in a circle in the complex plane.

Let $p = x_1 \dots x_{|p|}$, define h by

$$h = \left(\mathbf{L}_{\ell(\lfloor \frac{|p|}{n_t} \rfloor + 1)} \right)_{|p|+1 - \lfloor \frac{|p|}{n_t} \rfloor n_t, |p|+1 - \lfloor \frac{|p|}{n_t} \rfloor n_t}, \quad (37)$$

and define u by

$$u = y_{|p|+1} - \sum_{k=\lfloor \frac{|p|}{n_t} \rfloor n_t + 1}^{|p|} \left(\mathbf{L}_{\ell(\lfloor \frac{|p|}{n_t} \rfloor + 1)} \right)_{|p|+1 - \lfloor \frac{|p|}{n_t} \rfloor n_t, k - \lfloor \frac{|p|}{n_t} \rfloor n_t} x_k.$$

One can then verify that

$$f_{|p|+1}(pt) = |u - ht|^2$$

which leads to

$$|u - ht|^2 \leq \mathcal{T} - C(p).$$

This is equivalent to

$$|t - c| \leq r \quad (38)$$

where

$$r = \frac{\sqrt{\mathcal{T} - C(p)}}{|h|} \quad (39)$$

and

$$c = \frac{u}{h}.$$

We seek to enumerate the constellation points $t \in \mathcal{A}$ satisfying (38). At this point, we interject to comment on what happens in the case of linear dispersion codes.

Comparison to the Decoding of Linear Dispersion Codes: When a linear dispersion code is used with a QAM input constellation which is a Cartesian product of PAM constellations, the channel model is usually converted into an equivalent real-valued model. Finding the constellation points which satisfy (38) reduces to the trivial problem of enumerating the integers on an interval. For this reason, most of the literature concerned with the decoding of linear dispersion codes works with real-valued models. In contrast, we do not have that option and cannot readily apply the existing spherical bounding procedures.

Spherical Bounding Continued: We will now provide procedures for finding Gaussian and Eisenstein integer constellation points in a circle without necessarily exhaustively going through all $|\mathcal{A}|$ points. The procedures will be simple and applicable to arbitrary Gaussian or Eisenstein integer constellations. They might not necessarily be the most efficient possible procedures, but they will be efficient enough to realize

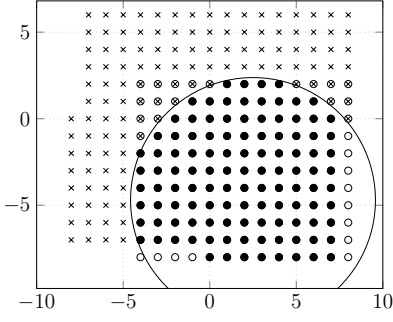


Fig. 14. Finding Gaussian integer constellation points in a circle; the hollow circles are the Gaussian integers that are visited

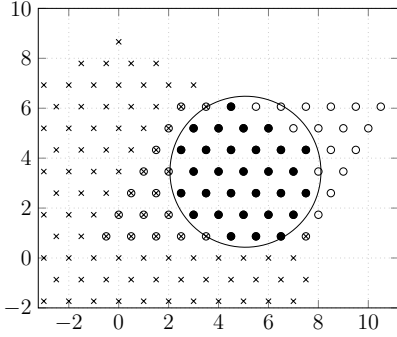


Fig. 15. Finding Eisenstein integer constellation points in a circle; the hollow circles are the Eisenstein integers that are visited

the task at hand which is obtaining the constellation points satisfying (38) in a small fraction of $|\mathcal{A}|$ steps (averaging over high SNRs). Figures 14 and 15 provide visualizations of these procedures.

We start by considering the problem of finding the points in Λ which are inside the circle where $\Lambda = \mathbb{G}$ or $\Lambda = \mathbb{E}$. Denote by $R_{\Lambda}^{\text{circle}}(c, r)$ the set of lattice points inside the circle defined by (38), i.e.,

$$R_{\Lambda}^{\text{circle}}(c, r) = \{z \in \Lambda \mid |z - c| \leq r\}.$$

We start with the case of $\Lambda = \mathbb{G}$. Rectangular subsets of \mathbb{G} can be naturally enumerated. We can start by finding the smallest square which contains the circle and then *shrinking* it so that the edges are aligned with \mathbb{G} . Let

$$\begin{aligned} i_{\min} &= \lceil \text{Re}\{c\} - r \rceil \\ i_{\max} &= \lfloor \text{Re}\{c\} + r \rfloor \\ j_{\min} &= \lceil \text{Im}\{c\} - r \rceil \\ j_{\max} &= \lfloor \text{Im}\{c\} + r \rfloor \end{aligned}$$

and denote by $R_{\mathbb{G}}^{\text{rectangle}}(c, r)$ the set

$$R_{\mathbb{G}}^{\text{rectangle}}(c, r) = \{i + \imath j \mid i, j \in \mathbb{Z}, i_{\min} \leq i \leq i_{\max}, j_{\min} \leq j \leq j_{\max}\}.$$

One can verify that $R_{\mathbb{G}}^{\text{circle}}(c, r) \subseteq R_{\mathbb{G}}^{\text{rectangle}}(c, r)$. We can then enumerate the elements of $R_{\mathbb{G}}^{\text{circle}}(c, r)$ by enumerating the elements of $R_{\mathbb{G}}^{\text{rectangle}}(c, r)$ and rejecting the $z \in \mathbb{G}$ for which $|z - c| > r$.

In the case of $\Lambda = \mathbb{E}$, parallelogram regions are naturally enumerated. We can similarly find a parallelogram which contains the circle and align it with \mathbb{E} in a manner that guarantees that no points inside the circle are missed. Denote by $R_{\mathbb{E}}^{\text{parallelogram}}(c, r)$ the set

$$R_{\mathbb{E}}^{\text{parallelogram}}(c, r) = \left\{ i_0 + j_0 \frac{\imath\sqrt{3}}{2} + i + j(\omega + 1) \mid \begin{array}{l} i, j \in \mathbb{Z} \\ 0 \leq i \leq i_{\max} \\ 0 \leq j \leq j_{\max} \end{array} \right\}$$

where i_0, j_0, i_{\max} , and j_{\max} are as follows:

$$\begin{aligned} j_0 &= \left\lfloor \frac{\text{Im}\{c\} - r}{\frac{\sqrt{3}}{2}} \right\rfloor \\ i_0 &= \begin{cases} \lfloor \text{Re}\{c\} - r\sqrt{3} \rfloor & \text{if } j_0 \text{ is even} \\ \lfloor \text{Re}\{c\} - r\sqrt{3} - 0.5 \rfloor + 0.5 & \text{if } j_0 \text{ is odd} \end{cases} \\ j_{\max} &= \left\lfloor \frac{\text{Im}\{c\} + r}{\frac{\sqrt{3}}{2}} \right\rfloor - j_0 \\ i_{\max} &= \begin{cases} \lfloor \text{Re}\{c\} + r\sqrt{3} \rfloor - \text{Re}\{\xi\} & \text{if } \frac{\text{Im}\{\xi\}}{\frac{\sqrt{3}}{2}} \text{ is even} \\ \lfloor \text{Re}\{c\} + r\sqrt{3} - 0.5 \rfloor + 0.5 - \text{Re}\{\xi\} & \text{if } \frac{\text{Im}\{\xi\}}{\frac{\sqrt{3}}{2}} \text{ is odd} \end{cases} \end{aligned}$$

$$\text{where } \xi = i_0 + j_0 \frac{\imath\sqrt{3}}{2} + j_{\max}(\omega + 1).$$

It can be verified that $R_{\mathbb{E}}^{\text{circle}}(c, r) \subseteq R_{\mathbb{E}}^{\text{parallelogram}}(c, r)$. As before, we can enumerate the elements of $R_{\mathbb{G}}^{\text{circle}}(c, r)$ by enumerating the elements of $R_{\mathbb{E}}^{\text{parallelogram}}(c, r)$ and rejecting the $z \in \mathbb{E}$ for which $|z - c| > r$.

The next task is to restrict the points in $R_{\Lambda}^{\text{circle}}(c, r)$ to the points that belong to our constellation $\mathcal{A} = \mathcal{A}_{\Pi\Lambda}$. Obviously, it would defeat the purpose of the algorithm if we were to have to compare them to each point in \mathcal{A} . Fortunately, Proposition 10 gives us a constant-time deterministic set membership test for checking whether some $z \in \Lambda$ belongs to $\mathcal{A}_{\Pi\Lambda}$. We can find $\mathcal{A}_{\Pi\Lambda} \cap R_{\Lambda}^{\text{circle}}(c, r)$ by simply rejecting the $z \in \Lambda$ for which $Q_{\Lambda}(z/\Pi) \neq 0$ during the enumeration.

One issue remains. When the SNR is low, the radius r is frequently large enough for the circle to cover an area larger than the area covered by the constellation aside from the possibility of the circle being entirely outside of the constellation. Consequently, at low SNRs, this algorithm would lead to a higher average complexity than that of exhaustively going through all of the points in \mathcal{A} . Therefore, we must add a further step which is the enforcement of the boundaries of the constellation so that the worst-case complexity is comparable to enumeration by exhaustive search. We propose that this be done in simplest possible way which is by enforcing a rectangular boundary around the constellation. This is achieved by modifying the parameters of the rectangle and parallelogram regions to prevent them from extending further outside this rectangular boundary enclosing the constellation than is necessary. In the case of rectangle regions, this is trivial. In the case of parallelogram regions, it is a matter of elementary geometry which we will omit to detail. Further

refinement of the procedure offers diminishing returns because if the SNR is low enough for the circles to consistently stretch far beyond the constellation, there would not be any benefit to spherical bounding to begin with.

For completeness, we specify an initial choice of threshold. We start with

$$\mathcal{T} = \alpha \cdot \sum_{\ell=1}^L \mathbb{E}[\|W_\ell\|_F^2]$$

where the initial value of α is a manually tuned parameter. Whenever the search fails, we add δ to α where δ is also a manually tuned parameter. Justification for such a form of threshold can be found in [72].

E. Permutations

Spatial Permutations: We have some freedom in permuting the rows of the sub-codewords of X and hence the order in which the symbols within a column are detected. In particular, let P_1, P_2, \dots, P_L be some $n_t \times n_t$ permutation matrices. We then have $\rho H_\ell X_\ell = (\rho H_\ell P_\ell)(P_\ell^{-1} X_\ell)$. We can take $\rho H_\ell P_\ell$ as our channel matrix and perform the QL decomposition $\rho H_\ell P_\ell = Q_\ell \mathbf{L}_\ell$ for $\ell = 1, 2, \dots, L$. We refer to such permutations as *spatial permutations*. For the purposes of decoding our codes, the modification to the algorithm is straightforward: We can perform the decoding as usual but must undo the permutation when computing the parity symbols as well as at the end of the decoding procedure.

The topic of spatial permutations is studied extensively in [12], [13]. The goal is usually to choose a permutation which leads to the matrices $\mathbf{L}_1, \mathbf{L}_2, \dots, \mathbf{L}_L$ having properties which result in a more efficient tree search. For example, from (37) and (39), we see that having large magnitude coefficients on the diagonals of these matrices leads to smaller radii in the spherical bounding procedure. We will consider the use of a simple heuristic proposed in [12] which is to sort the columns of the channel matrices in descending order of 2-norm.

Temporal Permutations: We have the freedom to permute the columns of X arbitrarily and hence detect the columns of the codeword in any order. This is enabled by the fact that the underlying code is MDS. Once a permutation has been chosen, the modification to the algorithm is straightforward:

- Permute the columns of Y accordingly as well as their associations with the different channel matrices (via $\ell(j)$).
- Permute the columns of the generator matrix used for generating the code tree accordingly and systematize it.
- Decode as usual and apply the inverse permutation to the columns of the resulting codeword.

It remains to determine how to choose a temporal permutation. We propose that we use the permutation which puts the columns of Y into descending order of 2-norm as is consistent with the principle of detecting the most reliable parts of the codeword first.

Comparison to the Decoding of Linear Dispersion Codes: In the case of linear dispersion codes, the effective codeword is an $n_t L T \times 1$ vector and there is no option for temporal permutations, we can only do spatial permutations. Moreover, since we have one large $n_t L T \times n_t L T$ effective channel matrix

rather than several $n_t \times n_t$ matrices, the number of possible spatial permutations is larger and the choice among them is important as is illustrated in [12], [13], [73].

It is worth noting that [73] argues that *spatial* permutations should be chosen as a function of both the channel matrix and the received signal vector and provides a relatively complex method for doing so. On the other hand, for the proposed codes, the block diagonal structure allows us to use the received signal to influence the detection order trivially via the proposed temporal permutation.

The General Case

We have developed an algorithm and a variety of improvements that are readily applicable to the decoding of SRB codes in the case of $n_r = n_t$. The case of $n_r > n_t$ is handled in the same way with the QL decomposition for rectangular matrices applied. This results in an immaterially different cost function. The reader is referred to [12], [13] for details.

On the other hand, the case of $n_r < n_t$ involves some challenges. A sphere decoder for the case of $n_r < n_t$ is proposed in [74] and the reader is also referred to [12] for some comments on this matter. In this case, the first term in the causal cost function depends on $n_r - n_t$ symbols rather than one. To use a stack decoder, we must begin by pushing all prefixes of length $n_r - n_t$ onto the priority queue incurring exponential complexity in $n_r - n_t$. Depth-first decoders might be more natural in this case. Nonetheless, the challenge of $n_r > n_t$ is not unique to the proposed codes and the techniques we provided for spherical bounding can be used to develop depth-first strategies.

Finally, we have the topic of SRA codes. In the case where there is no sub-codeword which contains both parity and information rows, all of the same decoding techniques apply readily. When this is not the case, it is not immediately apparent how to appropriately enumerate the codewords, (i.e., compute the E function (25)). A standard but not necessarily very efficient way of dealing with this is by removing the codeword constraints and checking at the end of the decoding procedure if the answer is a valid codeword. If the answer is not a valid codeword, the search is continued. Checking whether the codeword is valid can be done efficiently by representing the code as the null space of a *parity-check matrix* rather than the row space of a generator matrix.

F. Decoding Complexity Simulations

In this subsection, we examine the relative complexities of the proposed decoding strategies as a function of SNR in simulation. We consider the case of $n_r = n_t = T = L = 2$ and a $d = 3$ SRB code with a 271-Eis. constellation achieving a bpcu rate of 8.08. The CER versus SNR curve for this code was provided in Section V-A in Fig. 6.

The spherical bounding parameters are $\alpha = 1.75$ and $\delta = 0.25$. Moreover, the future costing is done by using the eigenbound to lower-bound the cost of the column-by-column MIMO detection problem where the component-wise minimization is performed with constellation constraints.

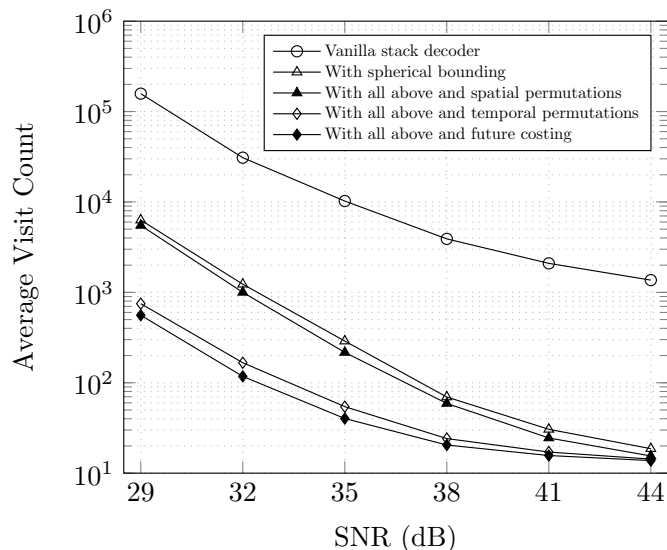


Fig. 16. Average number of code tree nodes visited versus SNR

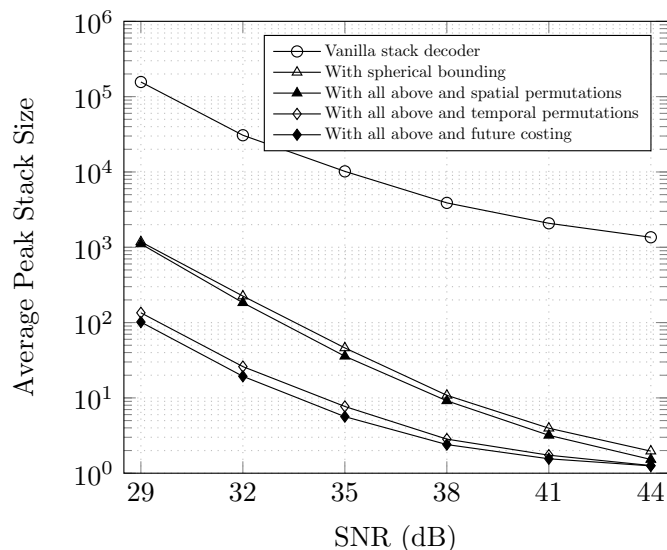


Fig. 17. Average peak stack size versus SNR

Fig. 16 plots the average number of code tree nodes visited as a function of SNR which is a proxy for the time complexity. In counting the number of nodes visited, we count all of the Eisenstein integers in the parallelogram occurring in the spherical bounding procedure as visited nodes even though some of them are not constellation points and are, strictly speaking, not part of the code tree. Nonetheless, they effectively act like virtual code tree nodes that are visited and rejected. Thus, the inefficiency of relaxing the circle constraint to a parallelogram constraint is accounted for. Moreover, the visit count is not reset if the tree search starts over due to the bounding threshold being too small.

Fig. 17 plots the average peak stack (or priority queue) size as a function of SNR which is a proxy for the space complexity. The *peak* is referring to the fact that the tree search might be repeated several times due to too small a bounding

threshold.

The results are self-explanatory so our comments will be brief. Firstly, note that the simulations start at an SNR which is already quite high—corresponding to a CER of less than 10^{-4} . The reason is that the vanilla stack decoder is infeasible at lower SNRs. One can expect larger gaps between the successive improvements at lower SNRs. Moreover, this is only one example and the relative significance of the various decoder improvements depends on the channel, code, and decoder parameters. For example, complex future costing heuristics were crucial to the decoding of the $n_t = 4, L = 1$ code simulated in Section V-C whereas here, they appear to be insignificant because a simple loose bound is used.

VII. CONCLUDING REMARKS

In this paper, we studied space-time codes based on rank and sum-rank metric codes from both the perspectives of coding-theoretic optimality properties and empirical error performance. We demonstrated that such codes can have competitive performance relative to codes designed for other criteria aside from utilizing significantly smaller constellations. Moreover, we demonstrated that such codes can be feasibly decoded with new challenges and opportunities arising from the decoding problem. Apart from the obvious ways in which these investigations can be extended, we suggest the following broad questions for future work:

- 1) Suboptimal decoding was not considered in this paper and the decoding complexity remains relatively high. It could be interesting to consider whether the lattice reduction approach of Puchinger et al. in [5] could be usefully combined with the proposed sequential decoding strategies.
- 2) We have demonstrated that the proposed codes can sometimes outperform full diversity codes even at higher SNRs. Yet, the rate-diversity optimality criterion for which the codes were constructed is not necessarily of any relevance to this error performance. In light of this, it could be interesting to consider other ways of designing good codes that are not full diversity.

REFERENCES

- [1] M. Shehadeh and F. R. Kschischang, "Rate-diversity optimal multiblock space-time codes via sum-rank codes," in *Proc. Int. Symp. Inf. Theory*, Los Angeles, CA, USA, Jun. 2020, pp. 3055–3060.
- [2] È. M. Gabidulin, "Theory of codes with maximum rank distance," *Problems Inf. Transmiss.*, vol. 21, no. 1, pp. 1–12, 1985.
- [3] M. Bossert, È. M. Gabidulin, and P. Lusina, "Space-time codes based on Gaussian integers," in *Proc. Int. Symp. Inf. Theory*, Lausanne, Switzerland, Jun. 2002, p. 273.
- [4] P. Lusina, È. M. Gabidulin, and M. Bossert, "Maximum rank distance codes as space-time codes," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2757–2760, Oct. 2003.
- [5] S. Puchinger, S. Stern, M. Bossert, and R. F. H. Fischer, "Space-time codes based on rank-metric codes and their decoding," in *Proc. Int. Symp. Wireless Commun. Syst.*, Poznań, Poland, Sep. 2016, pp. 125–130.
- [6] T. S. Kiran and B. S. Rajan, "Optimal rate-diversity tradeoff STBCs from codes over arbitrary finite fields," in *Proc. IEEE Int. Conf. Commun.*, Seoul, South Korea, May 2005, pp. 453–457.
- [7] H.-F. Lu and P. V. Kumar, "A unified construction of space-time codes with optimal rate-diversity tradeoff," *IEEE Trans. Inf. Theory*, vol. 51, no. 5, pp. 1709–1730, May 2005.

- [8] U. Martínez-Peñas, “Skew and linearized Reed–Solomon codes and maximum sum rank distance codes over any division ring,” *J. Algebra*, vol. 504, pp. 587–612, 2018.
- [9] H. El Gamal and A. R. Hammons, “On the design of algebraic space–time codes for MIMO block-fading channels,” *IEEE Trans. Inf. Theory*, vol. 49, no. 1, pp. 151–163, Jan. 2003.
- [10] O. Damen, A. Chkeif, and J.-C. Belfiore, “Lattice code decoder for space–time codes,” *IEEE Commun. Lett.*, vol. 4, no. 5, pp. 161–163, May 2000.
- [11] E. Viterbo and J. Boutros, “A universal lattice code decoder for fading channels,” *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1639–1642, Jul. 1999.
- [12] M. O. Damen, H. El Gamal, and G. Caire, “On maximum-likelihood detection and the search for the closest lattice point,” *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2389–2402, Oct. 2003.
- [13] A. D. Murugan, H. El Gamal, M. O. Damen, and G. Caire, “A unified framework for tree search decoding: Rediscovering the sequential decoder,” *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 933–953, Mar. 2006.
- [14] G. R. Ben-Othman, R. Ouertani, and A. Salah, “The spherical bound stack decoder,” in *Proc. IEEE Int. Conf. Wireless and Mobile Comput., Netw. and Commun.*, Avignon, France, Oct. 2008, pp. 322–327.
- [15] M. Stojnic, H. Vikalo, and B. Hassibi, “Speeding up the sphere decoder with H^∞ and SDP inspired lower bounds,” *IEEE Trans. Signal Process.*, vol. 56, no. 2, pp. 712–726, Feb. 2008.
- [16] R. Y. Chang, W.-H. Chung, and S.-J. Lin, “A* algorithm inspired memory-efficient detection for MIMO systems,” *IEEE Wireless Commun. Lett.*, vol. 1, no. 5, pp. 508–511, Oct. 2012.
- [17] B. Hassibi and B. M. Hochwald, “High-rate codes that are linear in space and time,” *IEEE Trans. Inf. Theory*, vol. 48, no. 7, pp. 1804–1824, Jul. 2002.
- [18] H.-F. Lu, “Constructions of multiblock space–time coding schemes that achieve the diversity–multiplexing tradeoff,” *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3790–3796, Aug. 2008.
- [19] S. Yang and J.-C. Belfiore, “Optimal space–time codes for the MIMO amplify-and-forward cooperative channel,” *IEEE Trans. Inf. Theory*, vol. 53, no. 2, pp. 647–663, Feb. 2007.
- [20] F. Oggier, G. Rekaya, J.-C. Belfiore, and E. Viterbo, “Perfect space–time block codes,” *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3885–3902, Sep. 2006.
- [21] K. P. Srinath and B. S. Rajan, “Improved perfect space–time block codes,” *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 7927–7935, Dec. 2013.
- [22] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, “Full-diversity, high-rate space–time block codes from division algebras,” *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2596–2616, Oct. 2003.
- [23] T. S. Kiran and B. S. Rajan, “Optimal STBCs from codes over Galois rings,” in *Proc. IEEE Int. Conf. Pers. Wireless Commun.*, New Delhi, India, Jan. 2005, pp. 120–124.
- [24] J.-C. Guey, M. P. Fitz, M. R. Bell, and W.-Y. Kuo, “Signal design for transmitter diversity wireless communication systems over Rayleigh fading channels,” in *Proc. Veh. Technol. Conf.*, Atlanta, GA, USA, Apr. 1996, pp. 136–140.
- [25] H.-F. Lu and P. V. Kumar, “Optimal constructions of space–time codes over multiple fading blocks,” in *Proc. Int. Symp. Inf. Theory*, Chicago, IL, USA, Jun. 2004, p. 409.
- [26] V. Tarokh, N. Seshadri, and A. R. Calderbank, “Space–time codes for high data rate wireless communication: Performance criterion and code construction,” *IEEE Trans. Inf. Theory*, vol. 44, no. 2, pp. 744–765, Mar. 1998.
- [27] H.-F. Lu, Y. Wang, P. V. Kumar, and K. M. Chugg, “Remarks on space–time codes including a new lower bound and an improved code,” *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2752–2757, Oct. 2003.
- [28] —, “On the performance of space–time codes,” in *Proc. IEEE Inf. Theory Workshop*, Bangalore, India, Oct. 2002, pp. 49–52.
- [29] M. Shehadeh, “Space–time codes from sum-rank codes,” Master’s thesis, Edward S. Rogers Sr. Dept. Elect. & Comput. Eng., Univ. Toronto, Toronto, ON, Canada, 2020.
- [30] H.-F. Lu and P. V. Kumar, “Rate–diversity tradeoff of space–time codes with fixed alphabet and optimal constructions for PSK modulation,” *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2747–2751, Oct. 2003.
- [31] R. C. Singleton, “Maximum distance q-nary codes,” *IEEE Trans. Inf. Theory*, vol. 10, no. 2, pp. 116–118, Apr. 1964.
- [32] H.-F. Lu, “On constructions of algebraic space–time codes with AM-PSK constellations satisfying rate–diversity tradeoff,” *IEEE Trans. Inf. Theory*, vol. 52, no. 7, pp. 3198–3209, Jul. 2006.
- [33] A. R. Hammons, “On space–time codes and constellation labelling,” in *Proc. IEEE Inf. Theory Workshop*, San Antonio, TX, USA, Oct. 2004, pp. 393–395.
- [34] U. Martínez-Peñas and F. R. Kschischang, “Universal and dynamic locally repairable codes with maximal recoverability via sum-rank codes,” *IEEE Trans. Inf. Theory*, vol. 65, no. 12, pp. 7790–7805, Dec. 2019.
- [35] A. R. Hammons and H. El Gamal, “On the theory of space–time codes for PSK modulation,” *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 524–542, Mar. 2000.
- [36] Y. Liu, M. P. Fitz, and O. Y. Takeshita, “A rank criterion for QAM space–time codes,” *IEEE Trans. Inf. Theory*, vol. 48, no. 12, pp. 3062–3079, Dec. 2002.
- [37] S. Yang and L. Hanzo, “Fifty years of MIMO detection: The road to large-scale MIMO,” *IEEE Commun. Surv. Tut.*, vol. 17, no. 4, pp. 1941–1988, 4th Quart. 2015.
- [38] H. El Gamal and M. O. Damen, “Universal space–time coding,” *IEEE Trans. Inf. Theory*, vol. 49, no. 5, pp. 1097–1119, May 2003.
- [39] L. Zheng and D. N. C. Tse, “Diversity and multiplexing: A fundamental tradeoff in multiple-antenna channels,” *IEEE Trans. Inf. Theory*, vol. 49, no. 5, pp. 1073–1096, May 2003.
- [40] P. Elia, K. R. Kumar, S. A. Pawar, P. V. Kumar, and H.-F. Lu, “Explicit space–time codes achieving the diversity–multiplexing gain tradeoff,” *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3869–3884, Sep. 2006.
- [41] J.-C. Belfiore, G. Rekaya, and E. Viterbo, “The Golden Code: A 2×2 full-rate space–time code with nonvanishing determinants,” *IEEE Trans. Inf. Theory*, vol. 51, no. 4, pp. 1432–1436, Apr. 2005.
- [42] P. Elia, P. V. Kumar, S. A. Pawar, K. R. Kumar, B. S. Rajan, and H.-F. Lu, “Diversity–multiplexing tradeoff analysis of a few algebraic space–time constructions,” in *Proc. Allerton Conf. Commun., Control, and Comput.*, Monticello, IL, USA, 2004.
- [43] J. Harshan and E. Viterbo, “On the robustness of algebraic STBCs to coefficient quantization,” in *Proc. Aust. Commun. Theory Workshop*, Wellington, New Zealand, 2012.
- [44] —, “Integer space–time block codes for practical MIMO systems,” *IEEE Wireless Commun. Lett.*, vol. 2, no. 4, pp. 455–458, Aug. 2013.
- [45] Y. Wu, L. M. Davis, and A. R. Calderbank, “Finite precision analysis for space–time decoding,” *IEEE Trans. Signal Process.*, vol. 57, no. 12, pp. 4861–4870, Dec. 2009.
- [46] J. A. Nossek and M. T. Ivrlač, “Capacity and coding for quantized MIMO systems,” in *Proc. Int. Conf. Wireless Commun. and Mobile Comput.*, Vancouver, BC, Canada, Jul. 2006.
- [47] H.-F. Lu, P. Elia, K. R. Kumar, S. A. Pawar, and P. V. Kumar, “Space–time codes meeting the diversity–multiplexing gain tradeoff with low signalling complexity,” in *Proc. Conf. Inf. Sci. and Syst.*, Baltimore, MD, USA, Mar. 2005.
- [48] U. Martínez-Peñas and F. R. Kschischang, “Reliable and secure multishot network coding using linearized Reed–Solomon codes,” *IEEE Trans. Inf. Theory*, vol. 65, no. 8, pp. 4785–4803, Aug. 2019.
- [49] B. Vucetic and J. Yuan, “Space–time coding performance analysis and code design,” in *Space–Time Coding*. Chichester, England: John Wiley & Sons, Ltd, 2003, ch. 2, pp. 49–89.
- [50] R. W. Nóbrega and B. F. Uchôa-Filho, “Multishot codes for network coding using rank-metric codes,” in *Proc. 3rd IEEE Int. Workshop Wireless Netw. Coding*, Boston, MA, USA, Jun. 2010.
- [51] R. W. Hamming, “Error detecting and error correcting codes,” *Bell Syst. Tech. J.*, vol. 29, no. 2, pp. 147–160, Apr. 1950.
- [52] P. Delsarte, “Bilinear forms over a finite field, with applications to coding theory,” *J. Combinatorial Theory A*, vol. 25, no. 3, pp. 226–241, 1978.
- [53] I. S. Reed and G. Solomon, “Polynomial codes over certain finite fields,” *J. Soc. Ind. Appl. Math.*, vol. 8, no. 2, pp. 300–304, Jun. 1960.
- [54] R. M. Roth, “MDS codes,” in *Introduction to Coding Theory*. New York, NY, USA: Cambridge University Press, 2006, ch. 11, pp. 333–364.
- [55] S. Liu, “Generalized skew Reed–Solomon codes and other applications of skew polynomial evaluation,” Ph.D. dissertation, Edward S. Rogers Sr. Dept. Elect. & Comput. Eng., Univ. Toronto, Toronto, ON, Canada, 2016.
- [56] S. Liu, F. Manganiello, and F. R. Kschischang, “Construction and decoding of generalized skew-evaluation codes,” in *Proc. Can. Workshop Inf. Theory*, St. John’s, NL, Canada, Jul. 2015, pp. 9–13.
- [57] D. Boucher and F. Ulmer, “Linear codes using skew polynomials with automorphisms and derivations,” *Des., Codes Cryptography*, vol. 70, pp. 405–431, 2014.
- [58] J. H. Conway and N. J. A. Sloane, “Coverings, lattices and quantizers,” in *Sphere Packings, Lattices and Groups*. New York, NY, USA: Springer-Verlag, 1999, ch. 2, pp. 31–62.

- [59] J. B. Fraleigh, "Gaussian integers and multiplicative norms," in *A First Course In Abstract Algebra*. Addison-Wesley, 2003, ch. 47, pp. 407–413.
- [60] W. A. Coppel, "More on divisibility," in *Number Theory: An Introduction to Mathematics; Part A*. New York, NY, USA: Springer Science+Business Media, 2006, ch. 3, pp. 151–207.
- [61] Q. T. Sun, J. Yuan, T. Huang, and K. W. Shum, "Lattice network codes based on Eisenstein integers," *IEEE Trans. Commun.*, vol. 61, no. 7, pp. 2713–2725, Jul. 2013.
- [62] S. Stern and R. F. H. Fischer, "Lattice-reduction-aided preequalization over algebraic signal constellations," in *Proc. Int. Conf. Signal Process. and Commun. Syst.*, Cairns, QLD, Australia, Dec. 2015.
- [63] K. Jarvis, "NTRU over the Eisenstein integers," Master's thesis, Dept. Math. Statist., Univ. Ottawa, Ottawa, ON, Canada, 2011.
- [64] T. Ernack, "A prime can be written as $a^2 - ab + b^2$ if $p \equiv 1 \pmod{3}$," Mathematics Stack Exchange. [Online]. Available: <https://math.stackexchange.com/q/3611243>
- [65] R. Breusch, "Zur Verallgemeinerung des Bertrandschen Postulates, daß zwischen x und $2x$ stets Primzahlen liegen," *Mathematische Zeitschrift*, vol. 34, no. 1, pp. 505–526, Dec. 1932.
- [66] F. Oggier, C. Hollanti, and R. Vehkalahti, "An algebraic MISO-MISO code construction," in *Proc. Int. Conf. Signal Process. and Commun.*, Bangalore, India, Jul. 2010.
- [67] U. Martínez-Peñas and F. R. Kschischang, "Evaluation and interpolation over multivariate skew polynomial rings," *J. Algebra*, vol. 525, pp. 111–139, 2019.
- [68] K. Sh. Zigangirov, "Some sequential decoding procedures," *Problems Inf. Transmiss.*, vol. 2, no. 4, pp. 1–10, 1966.
- [69] F. Jelinek, "Fast sequential decoding algorithm using a stack," *IBM J. Res. Develop.*, vol. 13, no. 6, pp. 675–685, Nov. 1969.
- [70] V. Sorokine and F. R. Kschischang, "A sequential decoder for linear block codes with a variable bias-term metric," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 410–416, Jan. 1998.
- [71] P. E. Hart, N. J. Nilsson, and B. Raphael, "A formal basis for the heuristic determination of minimum cost paths," *IEEE Trans. Syst. Sci. Cybern.*, vol. 4, no. 2, pp. 100–107, Jul. 1968.
- [72] T. Kailath, H. Vikalo, and B. Hassibi, "MIMO receive algorithms," in *Space-Time Wireless Systems: From Array Processing to MIMO Communications*, H. Bölcskei, D. Gesbert, C. B. Papadias, and A.-J. van der Veen, Eds. Cambridge, England: Cambridge University Press, 2006, ch. 15, pp. 302–321.
- [73] K. Su and I. J. Wassell, "A new ordering for efficient sphere decoding," in *Proc. IEEE Int. Conf. Commun.*, Seoul, South Korea, May 2005, pp. 1906–1910.
- [74] M. O. Damen, K. Abed-Meraim, and J.-C. Belfiore, "Generalised sphere decoder for asymmetrical space-time communication architecture," *Electron. Lett.*, vol. 36, no. 2, pp. 166–167, Jan. 2000.