Generalizing Linear Real-Field Codes for Fading Channels

Yan Xin and Georgios B. Giannakis [1]
Department of ECE, University of Minnesota
200 Union Street SE, Minneapolis, MN 55455
e-mails: {yxin,georgios}@ece.umn.edu

Abstract — **We derive generalized analytical constructions of linear real-field (LRF) codes for transmissions over wireless fading channels. We show cases where LRF-coded QAM, PAM, or PSK constellations can achieve maximum diversity and large coding gains. We construct analytically LRF codes, which not only yield larger coding gains than existing designs in most cases, but also produce LRF-coded QAM or PAM with desirable constellation characteristics. We also disclose an inherent connection between the optimality of LRF code construction over QAM or PAM, and a long-held mathematical conjecture in the theory of geometry of numbers. In certain cases, these results allow us to conjecture the optimality of our LRF codes over these constellations. Simulations corroborate our theoretical findings.**

I. Introduction

Signal space diversity has been by now well-documented as a bandwidth- and power-efficient coding approach, considerably improving the reliability of transmissions over fading channels [2, 3, 4, 6, 11]; see also [9] for a tutorial treatment, recent results, and applications. Pertinent research has focused on developing high (or maximum) diversity constellations (such as rotating QAM) [2, 4, 6, 11]. These are constructed using linear code generator matrices, which multiply blocks of symbols drawn from standard constellations to generate blocks of symbols with large diversity gain (G_d), and coding gain (G_c). Depending on the field the entries of these matrices are drawn from, they can be classified into two categories: linear complex-field (LCF) codes [6, 11], and linear real-field (LRF) codes [6]. In general, LCF codes yield larger coding gain than LRF ones [11], whereas LRF codes can be decoded with lower complexity than LCF ones [3]. In this paper, we will focus on analytical constructions of *square* LRF code matrices of size N over QAM, PAM, or PSK constellations.

Two design paradigms have been developed for LRF codes [2, 4, 6, 11]. One is based on parameterization of real orthogonal matrices [4]. The complexity of this approach depends on N, and the underlying constellation size M, thus becoming infeasible for either large N, or, large M. The second approach is based on number-theoretic tools [2, 6], which can provide closed-form solutions, and only rely on the algebraic structure of constellations. Construction examples for LRF code matrices can be found in [2, 4, 6]. But these designs neither guarantee large G_c, nor they apply to PSK constellations. A hybrid approach based on parameterization and the algebraic constructions over 16-QAM, was reported in [2] to maximize G_c for certain values of N. This approach can guarantee large G_c only for small N, and its generalizations to other values of N seem infeasible. Furthermore, the following questions remain largely open: (**Q1**) what is the best achievable upper-bound on G_c of LRF codes? and (**Q2**) can algebraically constructed LRF codes achieve this bound?

The contribution of this paper is two-fold. From a design perspective, we construct generalized analytical LRF codes, which not only allow the underlying constellations to include PSK, but also yield LRF codes for many sizes N. From a performance evaluation perspective, we show that the novel LRF codes can always achieve maximum diversity gain. We also derive the coding gains of LRF codes for some specific constellations and sizes. We further disclose an inherent connection between the best achievable upper-bound on G_c, and the best achievable upper-bound on the minimum product of N real linear homogeneous forms in the theory of geometry of numbers. Based on the results in [5, 8] and the coding results derived in this paper, we show that one of the novel LRF codes is *optimal* over the square lattice $\mathbb{Z}[j]$ for $N = 2$ and $N = 3$, which means that it achieves the best achievable G_c over $\mathbb{Z}[j]$. In addition, we prove that for $N = 2$, the same LRF code achieves the largest G_c over any size QAM or PAM, among all LRF codes satisfying the power constraint. This result not only just answers questions (Q1) and (Q2) for $N = 2$ over QAM, or PAM, but also provides an approach to potential generalizations. We further conjecture that this LRF code construction achieves the largest G_c over QAM or PAM, when $2N + 1$ is prime.

Notation: Column vectors (matrices) are denoted by boldface lower (upper) case letters; ^{T} and ^{H} stand for transpose and conjugate transpose, respectively; $\mathrm{tr}(\cdot)$ denotes trace; $\boldsymbol{I}_N$ denotes an $N \times N$ identity matrix; $\mathrm{diag}(d_1, \ldots, d_N)$ denotes a diagonal matrix with diagonal entries $d_1, \ldots, d_N$; j denotes $\sqrt{-1}$; $\mathbb{N}$ and $\mathbb{Z}$ stand for the positive integer set and the integer ring, respectively.

II. System Model, Performance Analysis, and Design Criteria

In this section, we will present the system model, performance analysis, and pertinent design criteria.

A. System Model

Let us consider the wireless system depicted in Figure 1. A stream of information bits is first mapped into symbols drawn from a constellation (alphabet) $\mathcal{A}_s$ of size $|\mathcal{A}_s|$. These symbols are parsed into $N \times 1$ blocks, and each block is multiplied by an $N \times N$ matrix $\boldsymbol{G}$, having entries drawn from the real field. Consider $\boldsymbol{s} \triangleq [s_1, \cdots, s_N]^T$ as one such block with $\{s_n\}_{n=1}^N \in \mathcal{A}_s$. The corresponding LRF-coded block can be written as $\boldsymbol{x} \triangleq \boldsymbol{G}\boldsymbol{s} = [\boldsymbol{g}_1^T\boldsymbol{s}, \ldots, \boldsymbol{g}_N^T\boldsymbol{s}]^T$, where $\boldsymbol{g}_n^T$ denotes the nth row of $\boldsymbol{G}$, and $\boldsymbol{g}_n^T\boldsymbol{s}$ denotes the nth LRF-coded symbol.

The coded symbols are assumed to be perfectly interleaved so that symbols in each coded block experience *independent*

[1] This work was supported by the ARL/CTA grant no. DAAD19-01-2-011.

Rayleigh fading. Denoting the fading coefficient of $\boldsymbol{g}_n^T\boldsymbol{s}$ by h_n, we can express the noisy received block as:

$$\boldsymbol{y} = \boldsymbol{H}\boldsymbol{x} + \boldsymbol{w}, \tag{1}$$

where $\boldsymbol{H} \triangleq \mathrm{diag}(h_1, \ldots, h_N)$, h_n's are assumed independent identically distributed complex Gaussian random variables with mean zero and variance $1/2$ per dimension, i.e., $h_n \sim \mathcal{CN}(0,1)$; and the noise block $\boldsymbol{w} \sim \mathcal{CN}(0, N_0\boldsymbol{I}_N)$, with $N_0/2$ denoting the power spectral density of the noise.

We further assume that: **as1)** perfect channel state information is available at the receiver but not at the transmitter; and **as2)** the receiver relies on maximum likelihood (ML) decoding to detect $\boldsymbol{s}$ from $\boldsymbol{y}$. Based on as1) and as2), the ML decoder yields:

$$\hat{\boldsymbol{s}} = \arg\min_{\boldsymbol{s}\in\mathcal{A}_s^N} \|\boldsymbol{y} - \boldsymbol{H}\boldsymbol{G}\boldsymbol{s}\|^2,$$

where $\|\cdot\|$ denotes the Euclidean norm.

B. Performance Analysis and Design Criteria

We start with computing the probability of the pairwise error event $\{\boldsymbol{s} \to \tilde{\boldsymbol{s}}\}$ that the ML receiver decodes $\tilde{\boldsymbol{s}}$ erroneously, when $\boldsymbol{s}$ was actually sent. It can be shown that at high SNR the average pairwise error probability (PEP) can be tightly upper-bounded by

$$\mathbb{P}\{\boldsymbol{s} \to \tilde{\boldsymbol{s}}\} \le \left[G_{e,c}\frac{1}{4N_0}\right]^{-G_{e,d}}, \tag{2}$$

where $G_{e,d} \triangleq |\mathcal{S}_{s,\tilde{s}}|$ denotes the cardinality of the set $\mathcal{S}_{s,\tilde{s}} \triangleq \{n : |\boldsymbol{g}_n^T(\boldsymbol{s}-\tilde{\boldsymbol{s}})|^2 \neq 0\}$, and $G_{e,c}$ is defined as $\left[\prod_{n\in\mathcal{S}_{s,\tilde{s}}} |\boldsymbol{g}_n^T(\boldsymbol{s}-\tilde{\boldsymbol{s}})|^2\right]^{1/G_{e,d}}$. Based on (2), we define the diversity and coding gains in terms of the LRF code matrix $\boldsymbol{G}$ as follows:

1. *Diversity gain*: For all possible error patterns $\boldsymbol{e} \triangleq \boldsymbol{s} - \tilde{\boldsymbol{s}}$, the diversity gain is defined as

$$G_d \triangleq \min_{\boldsymbol{s}\neq\tilde{\boldsymbol{s}}} G_{e,d} = \min_{\boldsymbol{s}\neq\tilde{\boldsymbol{s}}} |\mathcal{S}_{s,\tilde{s}}|. \tag{3}$$

2. *Coding gain*: For a given G_d, the coding gain is:

$$G_c \triangleq \min_{\boldsymbol{s}\neq\tilde{\boldsymbol{s}}} G_{e,c} = \min_{\boldsymbol{s}\neq\tilde{\boldsymbol{s}}} \prod_{n\in\mathcal{S}_{s,\tilde{s}}} |\boldsymbol{g}_n^T(\boldsymbol{s}-\tilde{\boldsymbol{s}})|^{2/G_d}.$$

When $G_d = N$, the coding gain becomes

$$G_c = \min_{\boldsymbol{s}\neq\tilde{\boldsymbol{s}}} \prod_{n=1}^{N} |\boldsymbol{g}_n^T(\boldsymbol{s}-\tilde{\boldsymbol{s}})|^{2/N} = \delta_c^{2/N}, \tag{4}$$

where $\delta_c \triangleq \min_{\boldsymbol{s}\neq\tilde{\boldsymbol{s}}} \prod_{n=1}^{N} |\boldsymbol{g}_n^T(\boldsymbol{s}-\tilde{\boldsymbol{s}})|$ stands for the *minimum product distance.* From (3), $\delta_c > 0$ implies that the maximum diversity gain N is achieved.

We have proved in [11] that there always exist LRF codes achieving maximum diversity gain. Motivated by this fact, we will look for LRF codes that maximize the coding gain G_c within the class of LRF codes achieving the maximum G_d. Therefore, the overall optimization problem in designing LRF codes for $G_d = N$ can be formulated as:

$$\hat{\boldsymbol{G}} = \underset{\boldsymbol{G}}{\mathrm{argmax}} \left[\min_{\boldsymbol{s}\neq\tilde{\boldsymbol{s}}} \prod_{n=1}^{N} |\boldsymbol{g}_n^T(\boldsymbol{s}-\tilde{\boldsymbol{s}})|^{2/N}\right], \tag{5}$$

subject to the power constraint $\mathrm{tr}(\boldsymbol{G}\boldsymbol{G}^H) = N$.

In other words, the problem of interest in this paper is to construct *optimal* LRF codes in the sense of achieving both maximum diversity, and maximum (or as large as possible) coding gains over M-QAM, M-PAM, or M-PSK constellations, which we term as *generalized constellations.* Algebraically, these generalized constellations are finite sets of the ring $\mathbb{Z}[\zeta_m]$ generated by $\mathbb{Z}$ and $\zeta_m \triangleq e^{j2\pi/m}$ for some m. For example, M-QAM, M-PAM, and 4-PSK are just finite subsets of the ring $\mathbb{Z}[j]$, where $m = 4$. M-PSK signaling points are subsets of the ring $\mathbb{Z}[\zeta_m]$ with $m = M$.

III. LRF Codes For Generalized Constellations

Even though LCF codes can yield larger coding gains than LRF codes [11], they generally require higher decoding complexity than real ones [3], especially as N increases. In light of complexity-performance tradeoffs, it is desirable to construct LRF codes with large G_c, especially when N is large. We pursue such LRF codes here for various values of N and m. To classify our constructions, we define the following three sets;

$$\mathcal{S}_\alpha^{(m)} \triangleq \{N \in \mathbb{N} : P \triangleq 2N+1 \text{ is a prime and } \gcd(m,P) = 1\};$$
$$\mathcal{S}_\beta^{(m)} \triangleq \{N \in \mathbb{N} : P \triangleq 2N = 2^{Q+1} \text{ and } \gcd(m,P) = 1, 2, \text{or}, 4\};$$
$$\mathcal{S}_\gamma^{(m)} \triangleq \{N \in \mathbb{N} : N = \phi(P)/2 \text{ for a } P \ \in \mathbb{N} \ \& \ \gcd(m,P) = 1\}.$$

Note that the superscript in $\mathcal{S}_\alpha^{(m)}, \mathcal{S}_\beta^{(m)}$, or, $\mathcal{S}_\gamma^{(m)}$ indicates that the values of N in these sets may vary according to m. For any QAM or PAM, m is treated as 4. Thus, the values in these sets are independent of the size M of QAM or PAM.

A. Generalized LRF Codes

In this subsection, we provide three classes of LRF code constructions.

A.1) Design LRF-A: $N \in \mathcal{S}_\alpha^{(m)}$

In this case, we consider the class of matrices that we express in closed-form as follows:

$$\boldsymbol{G} = \frac{-j}{\sqrt{P}}\begin{bmatrix} \alpha_1 - \alpha_1^{-1} & \alpha_1^3 - \alpha_1^{-3} & \cdots & \alpha_1^{2N-1} - \alpha_1^{-(2N-1)} \\ \alpha_2 - \alpha_2^{-1} & \alpha_2^3 - \alpha_2^{-3} & \cdots & \alpha_2^{2N-1} - \alpha_2^{-(2N-1)} \\ \vdots & \vdots & & \vdots \\ \alpha_N - \alpha_N^{-1} & \alpha_N^3 - \alpha_N^{-3} & \cdots & \alpha_N^{2N-1} - \alpha_N^{-(2N-1)} \end{bmatrix} \tag{6}$$

where $N = (P-1)/2$, $\{\alpha_n = e^{j2\pi n/P}\}_{n=1}^N$, and $1/\sqrt{P}$ is a constant ensuring the power constraint $\mathrm{tr}(\boldsymbol{G}\boldsymbol{G}^H) = N$. Note that $\alpha_n^p - \alpha_n^{-p} = 2j\sin(2\pi np/P)$ with $p = 1, 3, \ldots, 2N-1$, and the code matrix $\boldsymbol{G}$ in (6) has indeed real valued entries. In addition, the set $\mathcal{S}_\alpha^{(m)}$ includes many values of N for each fixed m in $\mathcal{S}_\alpha^{(m)}$. For instance, $\{2, 3, 5, 6, 8, 9, 11, 14, 15, 18, 20\ldots\} \subset \mathcal{S}_\alpha^{(4)}$. Next, we present construction examples for specific constellations with $\gcd(m,P) = 1$. Also note that the LRF code matrices in (6) apply to $m = 2, 4, 8, \ldots, 2^Q$, which include QAM, PAM, and 2^Q-PSK constellations.

Example 1 If $N = 2$, then $P = 5$, and (6) reduces to

$$\boldsymbol{G} = \frac{1}{2\sqrt{5}}\begin{bmatrix} \sqrt{10+2\sqrt{5}} & -\sqrt{10-2\sqrt{5}} \\ \sqrt{10-2\sqrt{5}} & \sqrt{10+2\sqrt{5}} \end{bmatrix}.$$

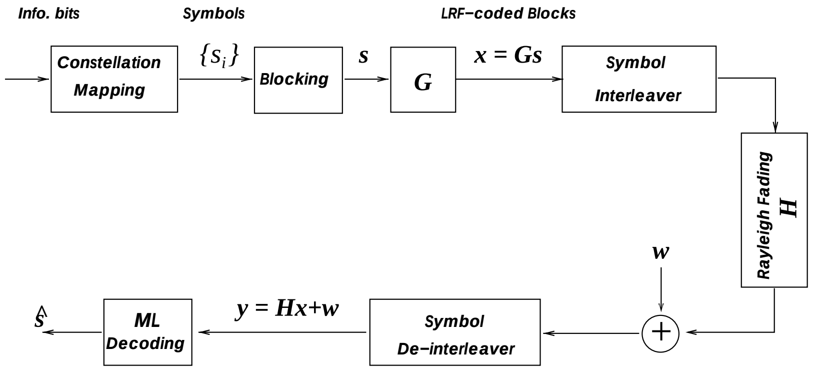

Figure 1: System Model

Example 2 If $N = 3$, then $P = 7$, and (6) reduces to:

$$G = \frac{2}{\sqrt{7}} \begin{bmatrix} \sin(\frac{2\pi}{7}) & \sin(\frac{6\pi}{7}) & -\sin(\frac{4\pi}{7}) \\ \sin(\frac{4\pi}{7}) & -\sin(\frac{2\pi}{7}) & \sin(\frac{6\pi}{7}) \\ \sin(\frac{6\pi}{7}) & \sin(\frac{4\pi}{7}) & \sin(\frac{2\pi}{7}) \end{bmatrix}. \quad (7)$$

Table 1 lists LRF-A code examples for $N < 21$, and $N \in \mathcal{S}_\alpha^{(m)}$ for $m \not\equiv 0 \pmod{P}$.

A.2) Design LRF-B: $N \in \mathcal{S}_\beta^{(m)} \cap \overline{\mathcal{S}}_\alpha^{(m)}$

With overbar denoting the complement of a set in $\overline{\mathcal{S}}_\alpha^{(m)}$, this LRF-B design is given by

$$G = \frac{-j}{\sqrt{P}} \begin{bmatrix} \beta_1 - \beta_1^{-1} & \beta_1^3 - \beta_1^{-3} & \cdots & \beta_1^{2N-1} - \beta_1^{-(2N-1)} \\ \beta_2 - \beta_2^{-1} & \beta_2^3 - \beta_2^{-3} & \cdots & \beta_2^{2N-1} - \beta_2^{-(2N-1)} \\ \vdots & \vdots & & \vdots \\ \beta_N - \beta_N^{-1} & \beta_N^3 - \beta_N^{-3} & \cdots & \beta_N^{2N-1} - \beta_N^{-(2N-1)} \end{bmatrix} \quad (8)$$

where $P = 2N = 2^{Q+1}$ with $Q \in \mathbb{N}$, $\{\beta_n = e^{j\pi(4n-3)/2^{Q+2}}\}_{n=1}^N$, and $1/\sqrt{P}$ is a normalizing factor ensuring the power constraint $\mathrm{tr}(GG^H) = N$. A construction similar to LRF-B was first given in [1] for QAM or PAM. We show here that it can be generalized to PSK constellations when $\gcd(m, P) = 1, 2, \text{or } 4$, and the coding gains of the construction can be obtained in closed-form for certain constellations, which will be detailed in Section III.C.

Example 3 When $N = 4$, LRF-B is constructed as in [1]

$$G = \frac{1}{\sqrt{8}} \begin{bmatrix} \sin(\frac{\pi}{16}) & \sin(\frac{3\pi}{16}) & \sin(\frac{5\pi}{16}) & \sin(\frac{7\pi}{16}) \\ \sin(\frac{5\pi}{16}) & \sin(\frac{\pi}{16}) & \sin(\frac{7\pi}{16}) & \sin(\frac{3\pi}{16}) \\ \sin(\frac{7\pi}{16}) & \sin(\frac{5\pi}{16}) & \sin(\frac{3\pi}{16}) & \sin(\frac{\pi}{16}) \\ \sin(\frac{3\pi}{16}) & \sin(\frac{7\pi}{16}) & \sin(\frac{\pi}{16}) & \sin(\frac{5\pi}{16}) \end{bmatrix}.$$

A.3) Design LRF-C: $N \in \mathcal{S}_\gamma^{(m)} \cap \overline{\mathcal{S}}_\alpha^{(m)} \cap \overline{\mathcal{S}}_\beta^{(m)}$

Let $\Phi_P(x)$ be the Pth cyclotomic polynomial of $\gamma_1 = e^{j2\pi/P}$, and $\{\gamma_n\}_{n=1}^N$ be the roots of $\Phi_P(x)$. LRF-C constructs

$$G = \frac{1}{\lambda} \begin{bmatrix} 1 & \gamma_1 + \gamma_1^{-1} & \cdots & \gamma_1^{N-1} + \gamma_1^{-(N-1)} \\ 1 & \gamma_2 + \gamma_2^{-1} & \cdots & \gamma_2^{N-1} + \gamma_2^{-(N-1)} \\ \vdots & \vdots & & \vdots \\ 1 & \gamma_N + \gamma_N^{-1} & \cdots & \gamma_N^{N-1} + \gamma_N^{-(N-1)} \end{bmatrix}, \quad (9)$$

where P is chosen so that $N \triangleq \phi(P)/2$, and $1/\lambda$ is a normalizing factor ensuring the power constraint $\mathrm{tr}(GG^H) = N$.

Table 1: LRF-A for $N = 2, 3, 5, 6, 8, 9, 11, 14, 15, 18, 20$

N	Generators $\{\alpha_n\}_{n=1}^N$ of G
$N = 2$	$\alpha_n = e^{j2\pi n/5},\ n = 1, 2$
$N = 3$	$\alpha_n = e^{j2\pi n/7},\ n \in [1, 3]$
$N = 5$	$\alpha_n = e^{j2\pi n/11},\ n \in [1, 5]$
$N = 6$	$\alpha_n = e^{j2\pi n/13},\ n \in [1, 6]$
$N = 8$	$\alpha_n = e^{j2\pi n/17},\ n \in [1, 8]$
$N = 9$	$\alpha_n = e^{j2\pi n/19},\ n \in [1, 9]$
$N = 11$	$\alpha_n = e^{j2\pi n/23},\ n \in [1, 11]$
$N = 14$	$\alpha_n = e^{j2\pi n/29},\ n \in [1, 14]$
$N = 15$	$\alpha_n = e^{j2\pi n/31},\ n \in [1, 15]$
$N = 18$	$\alpha_n = e^{j2\pi n/37},\ n \in [1, 18]$
$N = 20$	$\alpha_n = e^{j2\pi n/41},\ n \in [1, 20]$

B. Properties

In this subsection, we will present some properties of LRF-A, LRF-B, and LRF-C. Their proofs can be found in [12].

Property 1 *Matrices G under LRF-A and LRF-B are orthogonal.*

This property is interesting because it ensures that the performance remains invariant for additive white Gaussian noise (AWGN) or near AWGN channels after LRF coding by LRF-A or LRF-B.

Our next property deals with the geometry of LRF-coded constellations for LRF-A and LRF-B, and the corresponding peak-to-average power ratio (PAR) values, which are useful in assessing performance in the presence of nonlinear power amplification effects.

Property 2 *For $s \in \mathcal{A}_s^N$ with $\mathcal{A}_s$ being QAM or PAM and $x = Gs$ with G from (6) or (8), the LRF-coded constellation of x_n is geometrically identical $\forall$ n; i.e., $\mathcal{A}_{x_1} = \mathcal{A}_{x_2} = \cdots = \mathcal{A}_{x_N}$. Moreover, their PAR values are:*

$$PAR_x^{LRF\text{-}A} \triangleq \frac{\max|x_n|^2}{\mathbb{E}\{|x_n|^2\}} = \frac{1}{2N+1} \cot^2\left(\frac{\pi}{4N+2}\right) PAR_s,$$

$$PAR_x^{LRF\text{-}B} \triangleq \frac{\max|x_n|^2}{\mathbb{E}\{|x_n|^2\}} = \frac{1}{2N} \csc^2\left(\frac{\pi}{4N}\right) PAR_s$$

where $PAR_x^{LRF\text{-}A}$ and $PAR_x^{LRF\text{-}B}$ denote PAR values of the corresponding LRF-coded constellations $\{\mathcal{A}_{x_n}\}_{n=1}^N$, and PAR_s denotes the PAR value of the original alphabet $\mathcal{A}_s$.

Table 2: PAR Values of LRF-Coded 4-QAM

N	2	3	4	5	6	8
$\text{PAR}_x^{\text{LRF-A}}$ (dB)	2.8	4.4	–	6.4	7.2	8.4
$\text{PAR}_x^{\text{LRF-B}}$ (dB)	–	–	5.2	–	–	8.1

Example 4 Table 2 lists the PAR values of $\{\mathcal{A}_{x_n}\}_{n=1}^N$ for LRF-A and -B designs when $N = 2, 3, 4, 5, 6, 8$. Notice that for $N = 2$, LRF-A increases the PAR by about 2.77 dB, which is comparable to the PAR value 2.55 dB of the standard 16-QAM.

C. Diversity and Coding Gains

In this subsection, we will evaluate the diversity and coding gains of the LRF codes we designed in Section III.A. These codes always guarantee the maximum diversity gain for QAM, PAM, and PSK, whenever N belongs to the $\mathcal{S}_\alpha^{(m)}$, $\mathcal{S}_\beta^{(m)}$, and $\mathcal{S}_\gamma^{(m)}$. Thanks to the special structure of LRF-A, -B, and -C matrices, the coding gain can be obtained in closed-form for $m = 2, 3, 4, 6$.

Proposition 1 *Given QAM, PAM, or, PSK constellations, LRF-A, LRF-B, and LRF-C achieve maximum diversity gains; i.e., $G_d = N$, for $N \in \mathcal{S}_\alpha^{(m)}$, $\mathcal{S}_\beta^{(m)}$, $\mathcal{S}_\gamma^{(m)}$, respectively. Furthermore, if we only consider M-QAM ($\forall\ M$), M-PAM ($\forall\ M$), 3-PSK, or, 6-PSK constellations $\mathcal{A}_s$, with minimum Euclidean distance $d_{\min}$, the coding gain is:*

1. *For LRF-A:*

$$G_c^{\textit{LRF-A}} = \frac{d_{\min}^2 \sqrt[N]{2N+1}}{2N+1}, \quad N \in \mathcal{S}_\alpha^{(m)}; \quad (10)$$

2. *For LRF-B:*

$$G_c^{\textit{LRF-B}} = \frac{d_{\min}^2 \sqrt[N]{2}}{2N}, \quad N \in \mathcal{S}_\beta^{(m)}; \quad (11)$$

3. *For LRF-C:*

$$G_c^{\textit{LRF-C}} = \frac{d_{\min}^2}{\lambda^2}, \quad N \in \mathcal{S}_\gamma^{(m)}. \quad (12)$$

Remark: The coding gain in (11) was also conjectured but not proved in [3]. Our proof in [12] establishes (11) along with (10) and (12).

D. Optimality

In this subsection, we address the optimality of LRF-A, -B, and -C within the class of LRF code matrices. In our designs, we do not impose a particular structure except for the power constraint $\text{tr}(\boldsymbol{G}\boldsymbol{G}^H) = N$. Thus, our considerations and claims for the optimality of LRF constructions are more general than those in [2], where LRF code matrices are constrained to be orthogonal. To benchmark our designs, it is useful to find the best upper-bound on G_c achieved by LRF codes. To address this question, we will link this problem with the best achievable upper-bound on the minimum product of N real linear homogeneous forms — a well-known problem in the theory of geometry of numbers [7].

D.1) Product of N Real Linear Homogeneous Forms

Definition 1 *(Product of N real linear homogeneous forms) Consider N real linear homogeneous forms*

$$\begin{aligned}
\hat{u}_1 &= \hat{g}_{11}\hat{e}_1 + \hat{g}_{12}\hat{e}_2 + \cdots + \hat{g}_{1N}\hat{e}_N, \\
\hat{u}_2 &= \hat{g}_{21}\hat{e}_1 + \hat{g}_{22}\hat{e}_2 + \cdots + \hat{g}_{2N}\hat{e}_N, \\
&\vdots \\
\hat{u}_N &= \hat{g}_{N1}\hat{e}_1 + \hat{g}_{N2}\hat{e}_2 + \cdots + \hat{g}_{NN}\hat{e}_N,
\end{aligned} \quad (13)$$

where $\{\hat{e}_n\}_{n=1}^N \in \mathbb{Z}$, and $\hat{g}_{pq}$ for $p = 1, \ldots, N$ and $q = 1, \ldots, N$ are real numbers. We can express (13) *in a compact matrix form as follows*

$$\hat{\boldsymbol{u}} = \hat{\boldsymbol{G}}\hat{\boldsymbol{e}}, \quad (14)$$

where $\hat{\boldsymbol{u}} \triangleq [\hat{u}_1, \hat{u}_2, \cdots \hat{u}_N]^T$, $[\hat{\boldsymbol{G}}]_{pq} \triangleq g_{pq}$, and $\hat{\boldsymbol{e}} \triangleq [\hat{e}_1, \hat{e}_2, \ldots, \hat{e}_N]^T \in \mathbb{Z}^N$.

An interesting question about the product of N real linear homogeneous forms is [7] : *What is the best achievable upper-bound on the minimum $|\hat{u}_1\hat{u}_2\cdots\hat{u}_N|$ when $\hat{\boldsymbol{e}} \neq \boldsymbol{0}$?*

Comparing $\prod_{n=1}^N |\boldsymbol{g}_n^T(\boldsymbol{s} - \tilde{\boldsymbol{s}})|$ from Equation (4) with $|\hat{u}_1\hat{u}_2\cdots\hat{u}_N|$, one can readily notice that this question is ultimately related to the question on the best achievable upper-bound on G_c. However, we also find the following differences: 1) vector $\hat{\boldsymbol{e}} \in \mathbb{Z}^N$ whereas $\boldsymbol{s} - \tilde{\boldsymbol{s}} \in \mathcal{A}_s^N$ with $\mathcal{A}_s$ denoting a finite constellation; 2) matrix $\hat{\boldsymbol{G}}$ is not confined by the power constraint. We will first present existing results on the product of N real linear homogeneous forms, and then elaborate on the connection with the optimality of LRF-A, B, C.

When $N = 2$, the best achievable bound was obtained by Hurwitz in studying Diophantine approximations of real positive irrational numbers [8]. For $N = 3$, Davenport found the best achievable upper-bound in [5]. However, the problem on the best achievable upper-bound of the product of N real linear homogeneous forms remains unsolved for more than a century when $N \geq 4$ [7]. Upper-bounds which may not be the tightest have been reported for $N = 4, 5$ in [7].

Result 1 *(Hurwitz and Davenport's results for $N = 2$ and $N = 3$ in [8, 5]) For the linear form in* (13)*, there is an $\hat{\boldsymbol{s}} \neq \boldsymbol{0}$:*

$$|\hat{u}_1\hat{u}_2| \leq \frac{D}{\sqrt{5}}, \quad \textit{and} \quad |\hat{u}_1\hat{u}_2\hat{u}_3| \leq \frac{D}{7}. \quad (15)$$

where $D \triangleq |\det\hat{\boldsymbol{G}}|$. The upper-bounds in (15) *are achievable. Later on, we will present the matrices $\hat{\boldsymbol{G}}$ achieving the upper-bound of* (15)*.*

Result 2 *(Žilinskas and Godwin's results for $N = 4$ and $N = 5$ in [7]) For the linear form in* (13)*, there is an $\hat{\boldsymbol{s}} \neq \boldsymbol{0}$:*

$$|\hat{u}_1\hat{u}_2\hat{u}_3\hat{u}_4| \leq \frac{D}{14.9}, \quad \textit{and} \quad |\hat{u}_1\hat{u}_2\hat{u}_3\hat{u}_4\hat{u}_5| \leq \frac{D}{57.02}. \quad (16)$$

D.2) Optimality over $\mathbb{Z}[j]$

Motivated by Result 1, we define the *optimality* for LRF codes over $\mathbb{Z}[j]$ as follows:

Definition 2 *(Optimality over $\mathbb{Z}[j]$) If an LRF code matrix achieves maximum coding gain over $\mathbb{Z}[j]$, the LRF code matrix is defined as being optimal over $\mathbb{Z}[j]$.*

To delineate the optimality of LRF-A,B,C over $\mathbb{Z}[j]$, we first establish the following proposition.

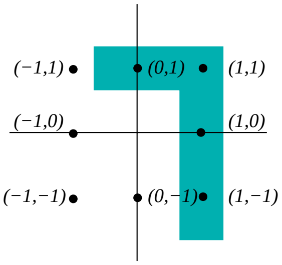

Figure 2: Lattice points in the shaped region

Proposition 2 *All LRF code matrices $\boldsymbol{G}$ satisfying $tr(\boldsymbol{G}\boldsymbol{G}^H) = N$, have $|\det \boldsymbol{G}| \leq 1$.*

Based on Result 1 and Proposition 2, we further establish

Proposition 3 *For $N = 2$ and $N = 3$, LRF-A in (6) is optimal over $\mathbb{Z}[j]$.*

The optimality of LRF-A over $\mathbb{Z}[j]$ is meaningful only when the size M of QAM or PAM is large. Thus, it is natural to ask whether LRF-A is still optimal over QAM or PAM carved from $\mathbb{Z}[j]$. Because QAM or PAM are just finite subsets (constellation points) of $\mathbb{Z}[j]$, it is plausible that the achievable upper-bounds over some QAM or PAM are larger than those over $\mathbb{Z}[j]$, and thus LRF-A may not be optimal over these constellations. Interestingly, as we show next, LRF-A is still optimal for any QAM, or PAM, when $N = 2$.

D.3) Optimality over QAM or PAM

The following proposition establishes the best achievable upper-bound of LRF-A over any QAM, or, PAM for $N = 2$.

Proposition 4 *Given any 2×2 LRF code matrix $\boldsymbol{G}$*

$$\boldsymbol{G} = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

with $tr(\boldsymbol{G}\boldsymbol{G}^H) = a^2 + b^2 + c^2 + d^2 = 2$, where a, b, c, d are real numbers, it holds that

$$\min(|ac|, |bd|, |(a+b)(c+d)|, |(a-b)(c-d)|) \leq \frac{1}{\sqrt{5}}. \quad (17)$$

Let us now turn to the optimality of LRF-A for QAM and PAM when $N = 2$.

Proposition 5 *For QAM, and PAM, LRF-A enjoys the best achievable G_c for $N = 2$.*

When $N = 2$, Proposition 4 shows that one of lattice points in the shaped region of Figure 2 must have a product distance bounded by $1/\sqrt{5}$. Together with the coding gain result in (10), we are able to prove that our LRF-A indeed is optimal because LRF-A achieves the upper-bound (17) independent of the QAM or PAM size. For $N > 2$, we are unable to prove the optimality of LRF-A,B,C for QAM or PAM. However, we conjecture that our LRF-A is still optimal over QAM, or, PAM when $2N + 1$ is a prime number. We formulate the following mathematical conjecture:

Conjecture 1 *Consider any LRF code matrix $\boldsymbol{G}$ under the power constraint $tr(\boldsymbol{G}\boldsymbol{G}^H) = N$. If $\boldsymbol{x} = \boldsymbol{G}\boldsymbol{s}$, then*

$$\min_{\boldsymbol{s} \in \mathcal{T}_N} |x_1 x_2 \cdots x_N| \leq \frac{\sqrt[N]{2N+1}}{2N+1}, \quad (18)$$

where x_n and s_n denote the nth entries of $\boldsymbol{x}$ and $\boldsymbol{s}$, respectively, and $\mathcal{T}_N$ is defined recursively as follows:

$$\mathcal{T}_1 = \{\boldsymbol{s} \in \mathcal{B} : s_1 = 1\};$$

$$\mathcal{T}_2 = \{\boldsymbol{s} \in \mathcal{B}^{2\times 1} : s_1 = 1\} \cup \{\boldsymbol{s} \in \mathcal{B}^{2\times 1} : [0, s_2]^T,\ s_2 \in \mathcal{T}_1\};$$

$$\vdots$$

$$\mathcal{T}_N = \{\boldsymbol{s} \in \mathcal{B}^{N\times 1} : s_1 = 1\} \cup \{\boldsymbol{s} \in \mathcal{B}^{N\times 1} : [0, \tilde{\boldsymbol{s}}]^T,\ \tilde{\boldsymbol{s}} \in \mathcal{T}_{N-1}\},$$

with $\mathcal{B} \triangleq \{-1, 0, 1\}$, and $\mathcal{T}_N$ being a subset of N-dimensional vectors, corresponding to lattice points in a unit N-dimensional cube.

Table 3: Coding Gains for *Normalized* Constellations

N	2	4
$G_c^{\text{LRF-}}$ (4-PSK)	0.8944 [A]	0.2973 [B]
$G_c^{\text{LRF-}}$ (8-PSK)	0.2620 [A]	0.0144 [C]
$G_c^{\text{LRF-}}$ (16-QAM)	0.1798 [A]	0.0595 [B]
$G_c^{\text{LRF-}}$ (16-PSK)	0.0681 [A]	0.0033 [C]
G_c^{UB} (4-PSK)	1	0.5
G_c^{UB} (8-PSK)	0.2929	0.1464
G_c^{UB} (16-QAM)	0.2	0.1
G_c^{UB} (16-PSK)	0.0761	0.0381

Clearly, the implication of this conjecture is that LRF-A will be optimal for any QAM or PAM, when $2N+1$ is a prime number.

IV. Simulation Examples

In this section, we provide corroborating simulations for LCF, LRF-A, -B, and -C codes for different constellations, and compare these constructions with existing designs. The average bit error rate (BER) is obtained by Monte-Carlo simulations, and the SNR is defined as E_s/N_0. All simulations use the sphere decoding algorithms [10] (see also [11, Section IV] for detailed exposition).

Test Example 1 Table 3 lists the coding gains achieved by LRF-A, -B, and -C for $N = 2, 4$ over normalized[1] 4-PSK, 8-PSK, 16-PSK, and 16-QAM, where the letters in square brackets indicate which LRF code has been used. The upper-bound on coding gains, G_c^{UB}, is obtained from [11, Eq.(8)].

Test Example 2 Table 4 lists G_c for $N = 2, 3, 4, 5, 6, 8$ with 4-QAM, and LRF-A, -B, and the LCF codes of [11].

Test Example 3 Figure 3 depicts performance comparisons among LRF-A, the LRF codes of [2], and the LCF codes of [11] when $N = 6$. Figure 4 compares LRF-A, the LRF codes of [2], the LRF codes of [3], and the LCF codes of [11], when $N = 8$. In both figures, 4-QAM constellations are used. Figure 3 confirms that LRF-A outperforms the LRF codes of [2] more than 1 dB at the same decoding complexity, and performs similar to the LCF codes of [11] with lower decoding complexity. Figure 4 shows that LRF-A outperforms the LRF codes of [2] by about 1 dB at BER $= 10^{-3}$ and slightly outperforms the LRF codes of [3] at the same decoding complexity; while LRF-A performs close to the LCF codes with lower complexity.

[1] Average symbol energy E_s of $\mathcal{A}_s$ is normalized to unity.

Table 4: Coding Gains over *Normalized* 4-QAM for $N = 2, 3, 4, 5, 6, 8$

N	2	3	4	5	6	8
$G_c^{\text{LRF-}}$	0.8944 [A]	0.5466 [A]	0.2973 [B]	0.2937 [A]	0.2359 [A]	0.1676 [A]
G_c^{LCF}	1	0.62	0.5	0.2947	0.3333	0.25
G_c^{UB}	1	0.6667	0.5	0.4	0.3333	0.25

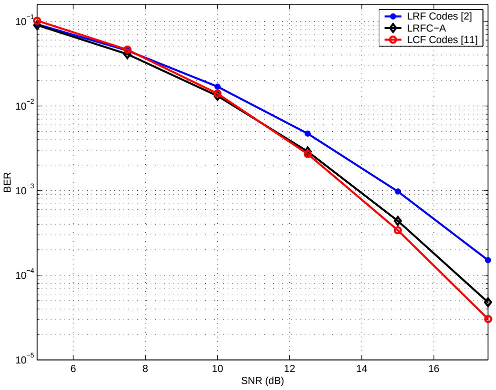

Figure 3: $N = 6$ and 4-QAM

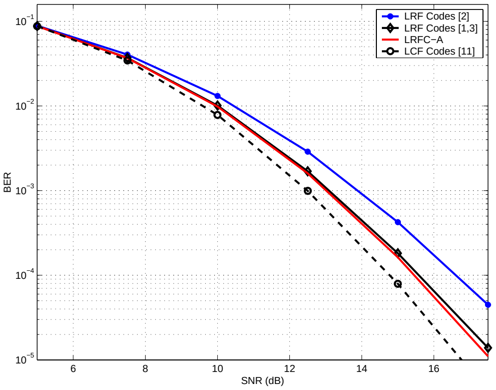

Figure 4: $N = 8$ and 4-QAM

Test Example 4 Figure 5 depicts LRF-A in (6) for $N = 2$, LRF-C in (9) for $N = 4$, and the uncoded system corresponding to $N = 1$ when 8-PSK constellation is used. It verifies that in both cases, LRF-A and LRF-C considerably outperform the uncoded system.

V. Conclusions

Generalized analytical constructions of LRF codes have been derived. The novel LRF codes were shown to achieve maximum diversity and large coding gains for QAM, PAM, or, PSK constellations in many cases. We proved the optimality of our LRF code designs over $\mathbb{Z}[j]$ when $N = 2, 3$, and the optimality of this design over any QAM or PAM when $N = 2$. Based on this result, we further conjectured that this LRF code design is optimal, when $2N + 1$ is a prime. Simulations confirmed that our LRF codes have similar performance with some existing designs, and outperform others depending on the code size and the underlying constellation size. In the full version of this work [12], we provide the detailed proofs of propositions and properties in this paper.

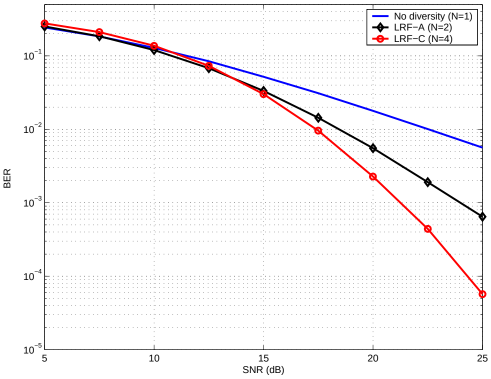

Figure 5: $N = 2, 4$ and 8-PSK Constellation

References

[1] J.-C. Belfiore, X. Giraud, and J. Rodriguez-Guisantes, "Optimal linear labelling for the minimisation of both source and channel distortion," *Proc. of ISIT*, Sorrento, Italy, June 25-30, 2000, pp. 404.

[2] J. Boutros and E. Viterbo, "Signal space diversity: A power and bandwidth efficient diversity technique for the Rayleigh fading channel," *IEEE Trans. on Information Theory*, vol. 44, pp. 1453-1467, July 1998.

[3] M. O. Damen, K. Abed-Meraim, and J.-C. Belfiore, "Diagonal algebraic space-time block codes," *IEEE Trans. on Information Theory*, vol. 48, pp. 628-636, March 2002.

[4] V. M. DaSilva and E. S. Sousa, "Fading-resistant modulation using several transmitter antennas," *IEEE Trans. on Communications*, vol. 45, pp. 1236-1244, October 1997.

[5] H. Davenport, "On the product of three homogeneous linear forms (II)," *Proc. London Math. Soc.*, vol. 44, pp. 412-431, 1938.

[6] X. Giraud, E. Boutillon, and J.-C. Belfiore, "Algebraic tools to build modulation schemes for fading channels," *IEEE Trans. on Information Theory*, vol. 43, pp. 938-952, May 1997.

[7] P. M. Gruber and C. G. Lekkerkerker, *Geometry of Numbers*, North-Holland Mathematical Library, 1987.

[8] A. Hurwitz, "Über die angenäherte Darstellung der Irrationalzaheln durch rationale Brüche." *Mathematische Annalen* 39, pp. 279-284, 1891.

[9] X. Ma, and G. B. Giannakis, "Complex field coded MIMO systems: performance, rate, and tradeoffs," *Wireless Communications and Mobile Computing*, pp. 693-717, November 2002.

[10] E. Viterbo and J. Boutros, "A universal lattice code decoder for fading channels," *IEEE Trans. on Information Theory*, vol. 45, pp. 1639-1642, July 1999.

[11] Y. Xin, Z. Wang, and G. B. Giannakis, "Space-time diversity systems based on linear constellation precoding," *IEEE Trans. on Wireless Communications*, March 2003 (to appear); see also *Proc. of 34th Asilomar Conf. on Signals, Systems, and Computers*, pp. 1553-1557, Pacific Grove, CA, Oct. 29-Nov. 1, 2000.

[12] Y. Xin and G. B. Giannakis, "Generalizing linear real- and complex-field codes for fading channels," *IEEE Transactions on Information Theory*, February 2003 (submitted).