[15] E. Biglieri, “High level modulation and coding for nonlinear satellite channels,” *IEEE Trans. Commun.*, vol. COM-32, pp. 616–626, May 1984.

[16] G. Ungerboeck, “Channel coding with multilevel/phase signals,” *IEEE Trans. Inform. Theory*, vol. IT-28, pp. 55–67, Jan. 1982.

[17] G. D. Forney Jr, “Geometrically uniform codes,” *IEEE Trans. Inform. Theory*, vol. 37, pp. 1241–1270, Sept. 1991.

[18] E. Zehavi and J. K. Wolf, “On the performance evaluation of trellis codes,” *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 196–202, Mar. 1987.

[19] S. Benedetto, M. Mondin, and G. Montorsi, “Performance evaluation of trellis coded modulation schemes,” *Proc. IEEE*, vol. 82, pp. 833–855, June 1994.

[20] F. J. Hill and G. R. Peterson, *Introduction to Switching Theory and Logical Design*. New York: Wiley, 1981.

[21] J. L. Massey and M. K. Sain, “Inverses of linear sequential circuits,” *IEEE Trans. Comput.*, vol. C-17, pp. 330–337, Apr. 1968.

[22] D. Aktas, “Improved performance measures for space-time coding with applications to code design,” Ph.D. dissertation, The Ohio State Univ., Columbus, 2002.

[23] Z. Chen, J. Yuan, and B. Vucetic, “Improved space-time trellis coded modulation scheme on slow rayleigh fading channels,” *IEE Electron. Lett.*, vol. 37, pp. 440–441, Mar. 2001.

[24] E. Malkamäki and H. Leib, “Evaluating the performance of convolutional codes over block fading channels,” *IEEE Trans. Inform. Theory*, vol. 45, pp. 1643–1646, July 1999.

[25] W.-Y. Kuo and M. P. Fitz, “Design and analysis of transmitter diversity using intentional frequency offset,” *IEEE Trans. Veh. Technol.*, vol. 46, pp. 871–881, Nov. 1997.

[26] M. Chiani, A. Conti, and V. Tralli, “A pragmatic approach for space-time coding,” in *Proc. IEEE Int. Conf. Communications*, Helsinki, Finland, June 2001, pp. 2794–2799.

Systematic Construction of Full Diversity Algebraic Constellations

Mohamed Oussama Damen, *Member, IEEE*,
Hesham El Gamal, *Senior Member, IEEE*, and
Norman C. Beaulieu, *Fellow, IEEE*

***Abstract*—A simple and systematic approach for constructing full diversity m-dimensional constellations, carved from lattices over a number ring $\mathcal{R}$, is proposed for an arbitrary dimension m. When $\mathcal{R} = \mathbb{Z}[w_n]$, the nth cyclotomic number ring, all the possible dimensions that allow for achieving the optimal minimum product distances using the proposed approach are determined. It turns out that one can construct optimal unitary transformations using our construction if and only if m factors into a power of 2 and powers of the primes dividing n. For m not satisfying these conditions, a method based on Diophantine approximation theory is proposed to “optimize” the minimum product distance. A lower bound on the product distance is given in this case, thus ensuring full diversity with “*good*” minimum product distances. Furthermore, the proposed approach subsumes the optimal unitary transformations proposed by Giraud *et al.* over $\mathcal{R} = \mathbb{Z}[w_4]$ and $\mathcal{R} = \mathbb{Z}[w_3]$, while giving optimal unitary transformations for infinitely many new values of n and m.**

***Index Terms*—Constellations, Diophantine approximation, diversity methods, number fields, number rings.**

I. Introduction

The design of full diversity algebraic constellations for the Rayleigh-fading channel was pioneered by Boullé and Belfiore [1]. The main idea behind their work is to introduce redundancy in the signal space[1] (or signal space diversity) when the signal constellation is carved from some algebraic lattices. Signal space diversity can be obtained by applying *fully diverse* unitary transformations to inputs drawn from lattices or multidimensional digital modulation signals carved from a number ring, such as pulse amplitude modulation (PAM) or quadrature amplitude modulation (QAM) constellations. The resulting constellations have the property that each point is uniquely determined by any of its components which allows for the possibility of retrieving the whole point if some of the components are lost in a deep fade. Recent interest in full diversity unitary

Manuscript received September 6, 2002; revised July 24, 2003. The work of M. O. Damen and N. C. Beaulieu was supported in part by the Alberta Informatics Circle of Research Excellence (iCORE) and the Natural Science and Engineering Research Council of Canada (NSERC). The work of H. El Gamal was supported in part by the National Science Foundation under Grants CCR–0118859 and ITR-0219892. The material in this correspondence was presented at the Canadian Workshop on Information Theory, Waterloo, ON, Canada, May 2003.

M. O. Damen and N. C. Beaulieu are with the Department of Electrical and Computer Engineering, University of Alberta, ECERF, Edmonton, AB T6G 2V4, Canada (e-mail: damen@ee.ualberta.ca; beaulieu@ee.ualberta.ca).

H. El Gamal is with the Department of Electrical Engineering, The Ohio State University, Columbus, OH 43210 USA (e-mail: helgamal@ee.eng.ohio-state.edu).

Communicated by R. Koetter, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2003.820024

[1] Algebraic rotations do not expand the bandwidth of the transmitted signal, and the rotated vectors at the output of the rotation have the same dimension as the unrotated ones from the input constellation. However, rotations, in general, induce an expansion of the input constellation at the component level (i.e., the components of the rotated vectors have higher dynamic ranges than the input constellation). This, generally, results in an increased peak-to-average power ratio of the rotated constellation, e.g., in a similar way to orthogonal frequency-division multiplexing (OFDM) signals.

0018-9448/03$17.00 © 2003 IEEE

transformations includes applications to the construction of full diversity linear space–time block constellations with optimized coding gains [2]–[4].

Algebraic tools were used in [5]–[7] for constructing m-dimensional transformations over the ring of integers $\mathbb{Z}$ and the ring of Gaussian integers $\mathbb{Z}[i]$, with $i \triangleq \sqrt{-1}$, for $m = 2^r$, $r \geq 1$, and over the ring of Eisenstein integers $\mathbb{Z}[j]$, with $j \triangleq e^{2i\pi/3}$, for $m = 3 \times 2^r$, $r \geq 0$. For other values of m, one can construct these transformations as a product of Givens planar rotations [8, p. 215], as proposed in [9] for $m = 2, \dots, 5$. The transformations obtained in this way, however, are not necessarily optimal since one does not exploit all the degrees of freedom (m^2) of the unitary transformations' manifold. More importantly, these transformations are dependent on the constellation over which the planar Givens rotations were optimized: they are not necessarily fully diverse over high-order constellations carved from the same ring. For example, the 2×2 unitary transformation

$$\boldsymbol{U} \triangleq \begin{pmatrix} \cos\beta & i\sin\beta \\ i\sin\beta & \cos\beta \end{pmatrix}$$

with $\beta = \pi/4$, which is constructed as a product of complex Givens rotations in [10] is fully diverse over a binary phase-shift keying (BPSK) constellation (over which the complex Givens rotations were optimized) but is not fully diverse over any QAM constellations (e.g., consider $\boldsymbol{U}\boldsymbol{s}$, with $\boldsymbol{s} = (1, i)^T$). Also, the ability to control the entries of the unitary transformation $\boldsymbol{U}$ to be algebraic in a Galois *extension* of $\mathbb{Q}$ that has the smallest possible degree [11] has been shown to be crucial for constructing full rate and full diversity linear space–time constellations in [4]. Such control over the entries of $\boldsymbol{U}$ is not feasible when using computer-based search methods [9], [10], [12].

In this correspondence, we propose a simple and systematic construction of fully diverse unitary transformations, with an arbitrary dimension m, over number rings. We show that one can choose the entries of the unitary transformation to be either algebraic in a Galois *extension*, or transcendental. We derive necessary and sufficient conditions on the number ring $\mathcal{R}$ and the dimension m, under which our constructions achieve the optimal values of the minimum product distances over $\mathcal{R}$. As special cases of the proposed construction, we rederive the optimal transformations in [5] when $\mathcal{R} = \mathbb{Z}[i]$, for $m = 2^r$, $r \geq 1$ and over $\mathbb{Z}[j]$ for $m = 3 \times 2^r$, $r \geq 0$. In these cases, the proposed constructions offer a new insight on the specificity of these values of m and $\mathcal{R}$. We also construct optimal transformations over $\mathcal{R}$ for infinitely many new values for m and infinitely many new rings $\mathcal{R}$, which have not been previously reported in the literature. Furthermore, we present algebraic tools for optimizing the transformations in the dimensions and rings where the optimal transformations cannot be found. In these scenarios, we give a lower bound on the minimum product distance for finite constellations carved from these rings. Finally, we note that the proposed construction is directly related to the computation of the determinant of a threaded space–time matrix [4, Lemmas 1–3].

II. Notation

The following notations are used throughout this correspondence. The letter $\mathcal{R}$ denotes a ring, $\mathbb{Z}$ the ring of integers, $\mathbb{Z}[i]$ the ring of complex integers (or Gaussian integers with $i \triangleq \sqrt{-1}$), $\mathbb{Z}[j]$ the ring of Eisenstein integers (with $j \triangleq e^{2i\pi/3}$). The letter $\mathbb{F}$ denotes a field, $\mathbb{Q}$ the field of rational numbers, $\mathbb{R}$ the field of real numbers, and $\mathbb{C}$ the field of complex numbers. For n integer, $w_n \triangleq e^{2i\pi/n}$ denotes the nth root of unity, and $\mathbb{Z}[w_n]$ is the ring of algebraic integers in the nth cyclotomic number field $\mathbb{Q}(w_n)$ [11]. For m and n integers, $(n|m)$ denotes their greatest common divisor (if m and n are coprime, then $(n|m) = 1$). The number of integers less than n and coprime with it is given by the Euler Φ-function $\Phi(n)$. The letter $\mathcal{S}$ denotes a multidimensional constellation carved from $\mathcal{R}^m$ where the ring $\mathcal{R}$ and the dimension m are determined from the context. Further, upper case boldface letters denote matrices and lower case boldface letters denote vectors, with the symbols $\boldsymbol{I}$ and $\boldsymbol{0}$ denoting, respectively, the identity matrix and the all-zero column vector of a size determined by the context. Finally, the superscripts ^{T}, ^{H}, and *, denote the transpose, Hermitian, and conjugate operators, respectively.

The following definitions [11] are also necessary for the development of our results.

Definition 1: A number ring $\mathcal{R} \subset \mathbb{C}$ is the set of algebraic integers in a number field (i.e., a finite degree extension of the rational numbers field $\mathbb{Q}$) equipped with the field binary operations $+$ and $\times$. We denote the information of the nonzero elements in $\mathcal{R}$ by $\Omega_{\mathcal{R}}$, i.e., $\Omega_{\mathcal{R}} \triangleq \inf\{|s|, s \neq 0 \in \mathcal{R}\}$ (note that $\Omega_{\mathcal{R}}$ is not necessarily attained by a nonzero element from $\mathcal{R}$). Finally, we denote by $\mathbb{F}$ the field of fractions of $\mathcal{R}$, i.e., $\mathbb{F} \triangleq \{\alpha/\beta : \alpha, \beta \in \mathcal{R}, \beta \neq 0\}$ (e.g., $\mathcal{R} = \mathbb{Z}, \mathbb{F} = \mathbb{Q}$). In the sequal, we restrict our attention to multidimensional constellations carved from number rings $\mathcal{S} \subset \mathcal{R}^m$, where a special attention is devoted to cyclotomic number rings.

Definition 2: A unitary transformation $\boldsymbol{U} \in C^{m \times m}$, with $\boldsymbol{U}\boldsymbol{U}^H = \boldsymbol{I}$, is called fully diverse over the ring $\mathcal{R}$ if its product distance is nonzero over $\boldsymbol{U}\mathcal{R}^m \backslash \{\boldsymbol{0}\}$. In particular, let $\boldsymbol{s} \triangleq (s_1, \dots, s_m)^T \neq \boldsymbol{0} \in \mathcal{R}^m$, and $\boldsymbol{x} \triangleq (x_1, \dots, x_m)^T = \boldsymbol{U}\boldsymbol{s}$, then $\boldsymbol{U}$ is fully diverse if

$$D_{\boldsymbol{U}}(\boldsymbol{s}) \triangleq \tau \prod_{k=1}^{m} |x_k| \neq 0, \qquad \forall\, \boldsymbol{s} \neq \boldsymbol{0} \in \mathcal{R}^m \tag{1}$$

where $\tau \triangleq m^{m/2}$ is a normalization factor introduced here only for the sake of simplification (as evident in the proof of Lemma 3). If $\boldsymbol{U}$ is fully diverse then all constellations carved from $\boldsymbol{U}\mathcal{R}^m$ have the full diversity property. We defined the minimum product distance of $\boldsymbol{U}$ over a multidimensional constellation $\mathcal{S} \subset \mathcal{R}^m$ as

$$d_{\boldsymbol{U}}(\mathcal{S}) \triangleq \min_{\boldsymbol{s} \in \mathcal{S} \backslash (\boldsymbol{0})} D_{\boldsymbol{U}}(\boldsymbol{s}). \tag{2}$$

We call $\boldsymbol{U}$ optimal over $\mathcal{S}$ if for any unitary transformation $\boldsymbol{V}$, we have $d_{\boldsymbol{U}}(\mathcal{S}) \geq d_{\boldsymbol{V}}(\mathcal{S})$. We call $\boldsymbol{U}$ optimal over $\mathcal{R}^m$ if $\exists \mathcal{S}_0 \subset \mathcal{R}^m$ such that for any unitary transformation $\boldsymbol{V}$, we have

$$d_{\boldsymbol{U}}(\mathcal{S}) \geq d_{\boldsymbol{V}}(\mathcal{S}), \qquad \forall \mathcal{S} \subset \mathcal{R}^m \text{ such that } \mathcal{S} \supseteq \mathcal{S}_0. \tag{3}$$

We hasten to stress that the optimality criterion adopted here is inspired by the minimum product distance of unconstrained multidimensional constellations carved from $\mathcal{R}^m$ with $m \in \mathbb{Z}^+$.[2] In the sequel, we will identify the scenarios where this criterion implies the optimality of the minimum product distances of all finite constellations corresponding to inputs carved from $\mathcal{R}$.

III. The Construction

Before stating our main result, we present two lemmas that characterize optimal unitary transformations over number rings.

Lemma 3: Let $\boldsymbol{U}$ be a unitary transformation. When the elements of $\boldsymbol{U}$, u_{kl}, $k, l = 1, \dots, m$, belong to a field $\mathbb{K}$ (or a ring $\mathcal{R}'$) that contains the number ring $\mathcal{R}$, then $\boldsymbol{U}$ is optimal over $\mathcal{R}^m$ if $D_{\boldsymbol{U}}(\boldsymbol{s}) \in \mathcal{R}\backslash\{0\}$, $\forall\, \boldsymbol{s} \neq 0 \in \mathcal{R}^m$.

Proof: Let $\boldsymbol{s} = (s_1, 0, \dots, 0)^T$, then

$$D_{\boldsymbol{U}}(\boldsymbol{s}) = \tau |s_1|^m \prod_{k=1}^{m} |u_{k1}|. \tag{4}$$

[2] Definition 2, though technical, is intended to reflect this fact.

Since $\boldsymbol{U}\boldsymbol{U}^H = \boldsymbol{I}$,, we have

$$\sum_{k=1}^{m} |u_{k1}|^2 = 1. \tag{5}$$

Applying the Cauchy inequality theorem, we obtain

$$\left(\prod_{k=1}^{m} |u_{k1}|^2\right)^{\frac{1}{m}} \le \frac{\sum_{k=1}^{m} |u_{k1}|^2}{m} = \frac{1}{m}. \tag{6}$$

Substituting the above inequality in (4), we conclude

$$D_{\boldsymbol{U}}(\boldsymbol{s}) = \tau |s_1|^m \prod_{k=1}^{m} |u_{k1}| \le |s_1|^m. \tag{7}$$

It follows that $\exists \mathcal{S}_0$ such that $\forall \mathcal{S} \supseteq \mathcal{S}_0$

$$d_U(\mathcal{S}) \le \min\{|s|^m \in \mathcal{S}_{2D}, s \neq 0\} \le \min\{|s| \in \mathcal{S}_{2D}, s \neq 0\}$$

where $\mathcal{S}_{2D}$ is the range (in $\mathcal{R}$) spanned by the components of $\mathcal{S}$ and the last inequality follows since $\mathcal{R}$ contains 1. Therefore, as the constellation $\mathcal{S}$ grows, the best minimum product distance one can attain approaches $\Omega_{\mathcal{R}}$ as $\mathcal{S}$ tends to $\mathcal{R}^m$. Hence, $\boldsymbol{U}$ is optimal if $D_{\boldsymbol{U}}(\boldsymbol{s}) \in \mathcal{R}\backslash\{0\}, \forall \boldsymbol{s} \neq 0 \in \mathcal{R}^m$. □

We note here that full diversity is a necessary condition for optimality. This lemma specifies the notion of optimality of the transformation $\boldsymbol{U}$, especially when one has a lower bound on the minimal absolute value of the elements of $\mathcal{R}$ (e.g., for $\mathcal{R} = \mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[j]$ one has $\Omega_{\mathcal{R}} = 1$). In fact, when $\Omega_{\mathcal{R}} = 1$, the optimal unitary transformation will maximize the minimum product distance for **all** finite constellations carved from $\mathcal{R}$. Since all known digital modulations are carved from the cyclotomic integer rings $\mathbb{Z}[w_n]$ [13], it is important to know the optimal values of the minimum product distances as a function of n. One can easily prove the following [11], [14].

Lemma 4:

$$\Omega_{\mathbb{Z}[w_n]} = 1, \qquad n = 1, 2, 3, 4, 6 \tag{8}$$

$$\Omega_{\mathbb{Z}[w_n]} = 0, \qquad n = 5 \text{ or } n > 6. \tag{9}$$

This result is directly related to the fact that the constellations carved from $\mathbb{Z}$, $\mathbb{Z}[i]$, and $\mathbb{Z}[j]$ have a constant minimum squared Euclidean distance of 1 (within a normalization depending only on the energy of the constellation). In these cases, the optimal unitary transformations will achieve the optimal minimum product distance for any finite constellations.

The phase-shift keying (PSK) constellations carved from $\mathbb{Z}[w_n]$ (with $n = 5$ or $n > 6$), on the other hand, have a minimum Euclidean distance that goes to zero as n increases. The notion of full diversity still holds in these cases as well since $d_U(\mathcal{S})$ tends to zero when increasing the size of the constellation, but can be guaranteed to never attain this value for any finite constellation $\mathcal{S}$. As shown in the following, our construction will guarantee a nonzero lower bound on the minimum product distance that depends on the size of the constellation.

We observe that, in practice, it may not be beneficial to construct rotated multidimensional constellations using PSK inputs since, by doing so, one looses the constant modulus property of these constellations. Nonetheless, proposing good unitary transformations over $\mathbb{Z}[w_n]$ is interesting for other constellations carved from this ring which have good minimal squared Euclidean distances that do not vanish in the limit. Such constellations can arise from rotating m-dimensional constellations over $\mathbb{Z}$ or $\mathbb{Z}[i]$ by unitary transformations with elements in $\mathbb{Q}(w_n)$ as in [3]. Now, we state the main result.

Theorem: Let $\mathcal{R}$ be a number ring, $\phi_1, \ldots, \phi_m \in \mathbb{C}$ with $|\phi_k| = 1$, $k = 1, \ldots, m$, and $\boldsymbol{F}_m$ be the $m \times m$ discrete Fourier transform (DFT) matrix with entries

$$\begin{aligned} f_{kl} &= \frac{1}{\sqrt{m}} e^{-2i\pi(l-1)(k-1)/m} \\ &= \frac{1}{\sqrt{m}} \left(w_m^{(k-1)(l-1)}\right)^*, \qquad l, k = 1, \ldots, m. \end{aligned}$$

Then, the unitary transformation

$$\boldsymbol{U} \triangleq \boldsymbol{F}_m^H \operatorname{diag}(\phi_1, \phi_2, \ldots, \phi_m) \tag{10a}$$

is fully diverse over $\mathcal{R}$ if $\phi_1 = 1, \phi_2 = \phi^{1/m}, \ldots, \phi_m = \phi^{(m-1)/m}$, and ϕ is chosen such that $\{1, \phi, \ldots, \phi^{m-1}\}$ are algebraically independent over $\mathcal{R}$. Such a choice of ϕ includes:

1) ϕ transcendental: $\phi = e^{i\lambda}$, with $\lambda \neq 0 \in \mathbb{R}$ algebraic;

2) ϕ algebraic of degree $\ge m$ over $\mathbb{F}$, the field of fractions of $\mathcal{R}$, such that $\{1, \phi, \ldots, \phi^{m-1}\}$ is a basis or part of a basis of $\mathbb{Q}(\phi)$ over $\mathbb{F}$ (i.e., the degree of ϕ over $\mathbb{F}$ is $m' \ge m$ such that $\{1, \phi, \ldots, \phi^{m'-1}\}$ is a basis of $\mathbb{Q}(\phi)$ over $\mathbb{F}$).

More strongly, when $\mathcal{R} = \mathbb{Z}[w_n]$, our construction yields optimal unitary transformations if and only if

$$\phi = w_n, \text{when } n \text{ is even: } n = 2^{t_0} \times p_1^{t_1} \times \cdots \times p_f^{t_f} \tag{10b}$$

$$\phi = w_{2n}, \text{when } n \text{ is odd: } n = p_1^{t_1} \times \cdots \times p_f^{t_f} \tag{10c}$$

$$m = 2^{r_0} \times p_1^{r_1} \times \cdots \times p_f^{r_f} \tag{10d}$$

where $p_1, \ldots, p_f$ are odd primes and $f, t_0, \ldots t_f, r_0, \ldots, r_f$, are positive integers. In particular, $\mathcal{R} = \mathbb{Z}[i]$ implies that the optimal unitary transformations using our construction in (10a) are only possible for $m = 2^r, r \ge 0$ and $R = \mathbb{Z}[j]$ implies that they only exist for $m = 2^{r_0}3^{r_1}, r_0 \ge 0, r_1 \ge 0$. These two special cases include all the optimal transformations in [5].

The proof is deferred to the Appendix.

Note that for $\mathcal{R} = \mathbb{Z}[i]$, we obtain the optimal unitary transformations (up to a permutation[3]) found in [5] as the Vandermonde matrix of the roots of $X^m - i$, where the Vandermonde matrix can be easily put in the form given in (10a). In addition, we prove that these are the only possible values of m. For $\mathcal{R} = \mathbb{Z}[j]$, we also find the optimal transformations in [1] for $m = 3 \times 2^{r_1}, r_1 \ge 0$ and propose new optimal constructions for other values $m = 2^{r_0}3^{r_1}, r_0 \ge 0, r_1 \ge 1$. Also, our approach generalizes, and makes precise, the one adopted first in [15] (for multidimensional OFDM signals), and utilized later in [16, Construction B][4] (for space–time signals equivalent to those in [2] over $\mathbb{Z}[i]$), for arbitrary dimensions and arbitrary number rings.

If one restricts $\mathcal{R} = \mathbb{Z}[w_n]$, then full diversity unitary transformations can still be found for m not satisfying (10d) with *good* minimum product distances. Achieving the optimal minimum product distance using our construction is, however, not possible in these scenarios since ϕ should be chosen of a higher degree than the degree of w_n in order to make $d_{\boldsymbol{U}}(\mathcal{S}) \neq 0$ for $\mathcal{S} \subset \mathbb{Z}[w_n]^m$. From the proof of the Theorem, one can see that this implies $d_{\boldsymbol{U}}(\mathcal{S}) \notin \mathbb{Z}[w_n]$ for arbitrary $\mathcal{S} \in \mathbb{Z}[w_n]^m$; indeed, its value expresses the simultaneous Diophantine approximation of $\{1, \phi, \ldots, \phi^{m-1}\}$ by numbers from $\mathbb{Z}[w_n]$.

[3] In fact, the construction (10a) is a direct extension of the construction in [5] since the relation between the DFT and Vandermonde matrices is well established in standard textbooks such as [8]. The latter relation was also considered in [19] when $\boldsymbol{m}$ is a power of $\mathbf{2}$.

[4] The so-called Construction A in [16] is, in fact, the cyclotomic construction of Giraud *et al.* [5] using Vandermonde matrices, and therefore, is also a special case of our construction for $\boldsymbol{m}$ powers of $\mathbf{2}$ and $\boldsymbol{\mathcal{S}} \subset \mathbb{Z}[\boldsymbol{i}]^m$.

Therefore, choosing ϕ such that $\{1, \phi, \dots, \phi^{m-1}\}$ are badly approximated over $\mathbb{Z}[w_n]$ *enhances* the minimum product distance. One possible choice of ϕ is an algebraic integer with the smallest degree that satisfies the Theorem [17, Liouville's Approximation Theorem]. In this case, by choosing ϕ to be algebraic such that $\{1, \phi, \dots, \phi^{m-1}\}$ is a basis or part of a basis of $\mathbb{Q}(\phi)$ over $\mathbb{Z}[w_n]$, one has the following lower bound on minimum product distance of a finite constellation $\mathcal{S} \subset \mathbb{Z}[w_n]^m$ [17]:

$$d_{\boldsymbol{U}}(\mathcal{S}) \geq \frac{1}{(2 + m\nu)^{m(d-1)}} \tag{11}$$

where d is the minimal degree of the number field that contains ϕ and the entries of $\mathcal{S}$ (i.e., d is the maximum of the degrees of ϕ and w_n), and ν is a quantity that depends only on the maximum absolute value of the components of the vectors in the finite constellation $\mathcal{S}$ [17], [3], [4]. The proof is directly related to the simultaneous approximation of algebraic numbers by other algebraic numbers [17, p. 34]. This proof is presented in [3], [4], and is omitted here for brevity. In order to maximize this lower bound (11), one needs to choose ϕ algebraic with the smallest possible degree which satisfies the main theorem. For example, for $m = 5$ and $n = 4$, one needs to choose $\phi = w_q$ of degree $\Phi(q) \geq m$. One can readily verify that the smallest number satisfying this is $q = 7$. Indeed, we have found that $\phi = w_7$ gives a local optimal value, with respect to the possible choices of ϕ, for the minimum product distance when using a 4-QAM constellation carved from $\mathbb{Z}[i]$. Although $d_{\boldsymbol{U}}(\mathcal{S})$ may decrease when increasing the size of the constellation in this case, one can easily see from our result that this choice of ϕ gives a fully diverse transformation over all constellations carved from $\mathbb{Z}[i]$. As a general rule, to maximize the lower bound in (11) for $n = 4$ (when m is not a power of 2), one should choose $\phi = w_q$ with $\mathbb{Q}$ the first prime such that $q - 1 \geq m$. This rule also applies for n and m not satisfying (10d), where one chooses $\phi = w_q$ with q the smallest prime such that $\{1, \phi, \dots, \phi^{m-1}\}$ are independent over $\mathbb{Z}[w_n]$. This rule, however, does not always give the (global) optimal ϕ for a given finite constellation carved from $\mathbb{Z}[w_n]$. In Table I we present the minimum product distances achieved by the proposed unitary transformation with a normalized 4-QAM input for different values of m. For $m = 5, 6, 7$, ϕ chosen by the above rule is found to give local optima of the minimum product distances; however, this is not the case when choosing $\phi = w_5$ for $m = 3$.[5] As expected, for m satisfying (10d), $\phi = w_4$ gives global optima. In Table II, we report the minimum product distances of the proposed rotations with $m = 2$ and n-PSK input constellations (with $n = 4, 8, 16, 32, 64$). As predicted by the optimality criterion of Lemma 3, we found $\phi = w_n$ to yield global optima in all these cases. Also, note that the exponent in the lower bound in (11), $m(d-1)$, is minimized when ϕ and m satisfy the constraints (10b)–(10d), i.e., when the optimality criterion in Lemma 3 is satisfied.

Remarks:

1) The general construction in (10a) allows for more degrees of freedom by simultaneously optimizing $\phi_1, \dots, \phi_m$, especially for the dimensions m that are not powers of the primes dividing n. This line of research is under investigation. The transcendental choice of ϕ can be of interest in some cases. For example, selecting ϕ randomly over the unit circle gives a fully diverse unitary transformation with probability 1. This is because the probability that ϕ will be algebraic is zero since the algebraic numbers are of measure zero in $\mathbb{C}$ [18]. Such random unitary transformations where considered in [19].

TABLE I
THE MINIMUM PRODUCT DISTANCES WHEN USING CONSTRUCTION (10a) OVER DIFFERENT ROTATED $\boldsymbol{m}$-DIMENSIONAL 4-QAM CONSTELLATIONS $\subset \mathbb{Z}[\boldsymbol{i}]$

m	2	3	4	5	6	7	8
$d_{\mathbf{U}}(\mathcal{S})$	1	0.0403	1	0.0543	0.0568	0.0024	1

TABLE II
THE MINIMUM PRODUCT DISTANCES WHEN USING CONSTRUCTION (10a) OVER DIFFERENT ROTATED 2-DIMENSIONAL $\boldsymbol{n}$-PSK CONSTELLATIONS $\subset \mathbb{Z}[\boldsymbol{w}_n]$

n	4	8	16	32	64
$d_{\mathbf{U}}(\mathcal{S})$	1	0.2241	0.0297	0.0037	$4.7255e-04$

TABLE III
THE MINIMUM PRODUCT DISTANCES WHEN USING CONSTRUCTION (10a) OVER DIFFERENT ROTATED $\boldsymbol{m}$-DIMENSIONAL 8-QAM CONSTELLATIONS $\subset \mathbb{Z}[\boldsymbol{i}] \cup \mathbb{Z}[\boldsymbol{j}]$

m	2	3	4
$d_{\mathbf{U}}(\mathcal{S})$	0.2188	0.0287	0.0248

2) Instead of choosing $\phi_1, \dots, \phi_m$ on the unit circle, one can allow them to be chosen from $\mathbb{C}$, where $\boldsymbol{U}$ is normalized by the norm of the vector $(\phi_1, \dots, \phi_m)$ to ensure constant average power. This can be useful, for example, if one wishes to use full diversity real constellations [2], [12], [4] or to allocate different powers to different symbols as in signal space coding for multiuser applications [20]. For example, when $m = 2$, the product distance is given by

$$D_{\boldsymbol{U}}(\boldsymbol{s}) = |\phi_1^2 s_1^2 - \phi_2^2 s_2^2| \tag{12}$$

with $\boldsymbol{s} \in \mathbb{Z}^2$. It is clear that choosing ϕ_1 and ϕ_2 such that $\frac{\phi_1^2}{\phi_2^2}$ is not a square in $\mathbb{Q}$ guarantees the full diversity property. As discussed in Lemma 3, if one can further guarantee that $D_{\boldsymbol{U}}(\boldsymbol{s}) \in \mathbb{Z}^+$ for all $\boldsymbol{s} \neq (0,0)^T$, then one optimizes the minimum product distance. Such choice includes $\phi_1 = 1$ and ϕ_2 any quadratic residue $(\sqrt{2}, \sqrt{3}, \dots)$.

3) Some important digital modulations may belong to a union of cyclotomic number rings, e.g., the most energy-efficient 8-QAM constellation given by

$$\{1+i, 1-i, -1+i, -1-i, \alpha, -\alpha, \alpha i, -\alpha i\} \subset \mathbb{Z}[i] \cup \mathbb{Z}[j]$$

with $\alpha = 1 + \sqrt{3}$ [13]. It is straightforward to apply our construction to this case using the rules above. For example, Table III lists the minimum product distances of the proposed rotated m-dimensional constellations with inputs from the above (normalized) 8-QAM constellation. Local optima are obtained for $\phi = w_4 w_6$, $w_5 w_6$, and $w_4 w_6$, respectively.

IV. CONCLUDING REMARKS

We have proposed a systematic construction of fully diverse unitary transformations for constellations carved from number rings, which include all PAM, QAM, and PSK constellations. Multidimensional constellations carved from number rings are anticipated to arise in future high data rate wireless communication systems, especially those that employ multiple antennas [4]. Given a multidimensional constellation from a number ring that is optimized for the additive white Gaussian noise channel, one can apply the unitary transformations proposed here in order to make it suitable for fading channels.

[5] In this special case, we have found $\boldsymbol{\phi} = \boldsymbol{w}_3$ and $\boldsymbol{\phi} = \boldsymbol{w}_{35}^3$ to give local optima of the minimum product distance over this constellation of $\mathbf{0.268}$ and $\mathbf{0.4854}$, respectively.

APPENDIX
PROOF OF THE THEOREM

Before giving the proof, we need the following results on cyclotomic number fields [1].

Lemma 5: The degree of $\mathbb{Q}(w_n)$ over $\mathbb{Q}$ equals $[\mathbb{Q}(w_n):\mathbb{Q}] = \Phi(n)$, the Euler-$\Phi$ function, which satisfies the relations

$$\Phi(p \times q) = \Phi(p) \times \Phi(q), \qquad \text{for } (p|q) = 1 \tag{13}$$

$$\Phi(p^{\alpha}) = p^{\alpha - 1} \times (p-1), \qquad \text{for } p \text{ prime.} \tag{14}$$

Further, every conjugate of w_n is an nth root of unity and not an mth root of unity for any $m < n$. If n is even, then the only roots of unity in $\mathbb{Q}(w_n)$ are the nth roots of unity (i.e., $w_n^k, k \geq 1$). If n is odd, then the only ones (in addition to $w_n^k, k \geq 1$) are the $2n$th roots of unity $(w_{2n}^k, k \geq 1)$. Furthermore, the nth cyclotomic fields, for n even, are all distinct and pairwise nonisomorphic.

Lemma 6: All w_n^k, $1 \leq k \leq n$, $(k|n) = 1$ are conjugates of w_n. It follows that $\mathbb{Q}(w_n)$ contains all the conjugates of w_n, thus, $\mathbb{Q}(w_n)$ is a Galois *extension* of $\mathbb{Q}$ (i.e., $\mathbb{Q}(w_n^k) = \mathbb{Q}(w_n)$ for $1 \leq k \leq n$, $(k|n) = 1$). Furthermore, $\{1, (w_n^k), (w_n^k)^2, \ldots, (w_n^k)^{\phi(n)-1}\}$ is a basis of $\mathbb{Q}(w_n)$ over $\mathbb{Q}$, for $1 \leq k \leq n$, $(k|n) = 1$.

Proof of the Theorem

Let $\boldsymbol{s} \triangleq (s_1, \ldots, s_m)^T \in \mathcal{R}^m$, then the product distance of $\boldsymbol{U}s$ is given by

$$D_{\boldsymbol{U}}(\boldsymbol{s}) = \prod_{k=1}^{m} \left| \phi_1 s_1 + \cdots + \phi_m s_m (w_m^k)^{m-1} \right|. \tag{15}$$

First, define the following threaded space–time matrix [4]:

$$\boldsymbol{M}(\boldsymbol{s}) = \begin{pmatrix} \phi_1 s_1 & \phi_m s_m & \ldots & \phi_2 s_2 \\ \phi_2 s_2 & \phi_1 s_1 & \ldots & \phi_3 s_3 \\ \vdots & \vdots & \ddots & \vdots \\ \phi_m s_m & \phi_{m-1} s_{m-1} & \ldots & \phi_1 s_1 \end{pmatrix}. \tag{16}$$

Since $\boldsymbol{M}(\boldsymbol{s})^T$ is circulant, it is diagonalizable using the DFT as follows [21], [22]:

$$\boldsymbol{M}(\boldsymbol{s})^T = \boldsymbol{F}_m^H \operatorname{diag}(\lambda_1, \ldots, \lambda_m) \boldsymbol{F}_m \tag{17}$$

where

$$\lambda_k = \phi_1 s_1 + \phi_2 s_2 (w_m^k) + \cdots + \phi_m s_m (w_m^k)^{m-1}, \quad k = 1, \ldots, m$$

are the eigenvalues of $\boldsymbol{M}(\boldsymbol{s})$. Therefore, one clearly has

$$|\det(\boldsymbol{M}(\boldsymbol{s}))| = D_{\boldsymbol{U}}(\boldsymbol{s}).$$

On the other hand, using the results for threaded matrices from [4, Lemma 3], it follows that by choosing $\phi_1 = 1, \phi_2 = \phi^{1/m}, \ldots, \phi_m = \phi^{(m-1)/m}$, one has

$$\det \boldsymbol{M}(\boldsymbol{s}) = \epsilon_1 X_1 + \epsilon_2 X_2 \phi + \cdots + \epsilon_m X_m \phi^{m-1}, \tag{18}$$

where $X_1 = s_1^m$, $X_m = s_m^m \in \mathcal{R}$, the terms X_k contain the crossing terms of $\prod_{l=1}^{m} s_{k_l} \in \mathcal{R}$, $k_l \in \{1, \ldots, m\}$, and $\epsilon_k = \pm 1$, $k = 1, \ldots, m$, is the signature of thread ℓ_k which depends on its positions in the matrix $\boldsymbol{M}(\boldsymbol{s})$ (the thread ℓ_k is defined here by the positions of s_k in the threaded matrix $\boldsymbol{M}(\boldsymbol{s})$ [4]). One also proves that setting $\bar{\boldsymbol{s}}_l \triangleq (s_1, s_2, \ldots, s_{l-1}, 0, \ldots, 0)^T$ gives [4, Lemma 1]

$$\det \boldsymbol{M}(\bar{\boldsymbol{s}}_l) = \epsilon_1 \bar{X}_{1,l} + \epsilon_2 \bar{X}_{2,l} \phi + \cdots + \epsilon_l \bar{X}_{l,l} \phi^{l-1} \tag{19}$$

where $\bar{X}_{1,l} = s_1^m$, $\bar{X}_{l,l} = s_l^m$, and the terms $\bar{X}_{k,l}$ contain the crossing terms of $\prod_{t=1}^{m} s_{k_t} \in \mathcal{R}$, $k_t \in \{1, \ldots, l\}$, and $\epsilon_t = \pm 1, t = 1, \ldots, l$, is defined as above.

We first prove the full diversity property of transformation $\boldsymbol{U}$ (10a) over $\mathcal{R}$. Suppose now that $\phi_1 = 1$, $\phi_2 = \phi, \ldots, \phi_m = \phi^{(m-1)/m}$, and ϕ is chosen such that $\{1, \phi, \phi^2, \ldots, \phi^{m-1}\}$ are algebraically independent over $\mathcal{R}$. Further, suppose that $D_{\boldsymbol{U}}(\boldsymbol{s}) = 0$ for a given $\boldsymbol{s} \neq \boldsymbol{0} \in \mathcal{R}^m$. Then, (18) gives $X_k = 0$, $k = 1, \ldots, m$. Particularly, one has $X_m = s_m^m = 0$ giving $s_m = 0$. Substituting in (19) gives

$$D_{U}(\boldsymbol{s}) = |\det \boldsymbol{M}(\bar{\boldsymbol{s}}_{m-1})| = 0, \text{ gives} \tag{20}$$

$$= \epsilon_1 \bar{X}_{1,m-1} + \cdots + \epsilon_{m-1} \bar{X}_{m-1,m-1} \phi^{m-2} = 0 \tag{21}$$

which, in turns, implies $\bar{X}_{m-1,m-1} = 0$ giving $s_{m-1} = 0$. Re-performing this substitution in (19) gives successively $s_{m-2} = s_{m-3} = \cdots = s_1 = 0$, which contradicts the hypothesis. Therefore, $\boldsymbol{U}$ is a fully diverse unitary transformation over $\mathcal{R}$ if $\{1, \phi, \phi^2, \ldots, \phi^{m-1}\}$ are algebraically independent over $\mathcal{R}$. To ensure that $\boldsymbol{U}$ is fully diverse, the Diophantine number ϕ can be chosen either transcendental or algebraic. Let $\phi = e^{i\lambda}$ with $\lambda \neq 0$ real, then $\{0, i\lambda, 2i\lambda, \ldots, (m-1)i\lambda\}$ are all distinct algebraic numbers. Therefore, [17, Lindemann theorem, pp. 51-71] states that $\{1, e^{i\lambda}, e^{2i\lambda}, \ldots, e^{(m-1)i\lambda}\}$ are transcendental and algebraically independent over any set of algebraic numbers, and particularly over $\mathcal{R}$. Similarly, choosing ϕ such that $\mathbb{Q}(\phi)$ is an extension of $\mathbb{F}$, the field of fractions of $\mathcal{R}$, with $\{1, \phi, \phi^2, \ldots, \phi^{m-1}\}$ as a basis or part of a basis of $\mathbb{Q}(\phi)$ over $\mathcal{R}$ yields the desired full diversity property. This proves the first part of the theorem which is related to guaranteeing a nonzero minimum product distance.

To prove the second part, which is related to the maximization of the minimum product distance (optimal transformations), we restrict ourselves to consider $\mathcal{R} = \mathbb{Z}[w_n]$, and we quantify n, m, and ϕ that give us the optimal transformations. The main idea in the proof is to use (18) in order to test the choices of ϕ which make $d_{\boldsymbol{U}}(\mathcal{S}) \in \mathcal{R}$, and then to look for the possible choices of m that make $d_{\boldsymbol{U}}(\mathcal{S}) \neq 0$ using (15). Note that from (18) we can see that in order to have $D_{\boldsymbol{U}}(\boldsymbol{s}) \in \mathbb{Z}[w_n]$, one needs $\phi \in \mathbb{Z}[w_n]$. Since $|\phi| = 1$, one chooses $\phi = w_n$ when n is even, and $\phi = w_{2n}$ for n odd[6] (using Lemma 5). Now, we examine the eigenvalues of matrix $\boldsymbol{M}(\boldsymbol{s})$(15) for this choice of ϕ for both possibilities of n.

1) When n is even: then, the eigenvalues of matrix $\boldsymbol{M}(\boldsymbol{s})$(15) are given by

$$\begin{aligned} \lambda_k &= s_1 + s_2 w_n^{\frac{1}{m}} (w_m^k) + \cdots + s_m w_n^{\frac{m-1}{m}} (w_m^k)^{m-1}, \quad && k = 1, \ldots, m \\ &= s_1 + s_2 w_{nm}^{nk+1} + \cdots + s_m \left(w_{nm}^{nk+1}\right)^{m-1}, && k = 1, \ldots, m. \end{aligned} \tag{22}$$

Therefore, it becomes clear that, for this choice of ϕ, the only possible values of m are the ones that allow for

$$\left\{1, w_{nm}^{nk+1}, \left(w_{nm}^{nk+1}\right)^2, \ldots, \left(w_{nm}^{nk+1}\right)^{m-1}\right\}$$

to be algebraically independent over $\mathbb{Z}[w_n]$ for $k = 1, \ldots, m$. In other words, it is necessary to have $\mathbb{Q}(w_{nm})$ as an *extension* of degree m over $\mathbb{Q}(w_n)$. Using the Galois theorem [11], we obtain

$$[\mathbb{Q}(w_{nm}) : \mathbb{Q}] = [\mathbb{Q}(w_{nm}) : \mathbb{Q}(w_n)] \times [\mathbb{Q}(w_n) : \mathbb{Q}] \tag{23}$$

[6] Choosing $\boldsymbol{\phi} = \boldsymbol{w}_n$ in this case makes $\boldsymbol{D_U(s)} \in \mathbb{Z}[\boldsymbol{w}_n]$, but it does guarantee the full diversity property only for particular values of $\boldsymbol{m}$ that are included in the case $\boldsymbol{\phi} = \boldsymbol{w}_{2n}$ as proved later.

which, by using Lemma 5, implies the following necessary condition on m:

$$\Phi(nm) = m\Phi(n). \tag{24}$$

To resolve (24) one writes $n = p_0^{t_0} \times \cdots \times p_f^{t_f}$, with $p_0 = 2,\ p_1, \ldots, p_f$ primes different from 2, and $f, t_0, \ldots, t_f$ positive integers. One also writes $m = p_0^{r_0} \times \ldots \times p_f^{r_f} \times q_0^{v_0} \times \cdots \times p_g^{v_g}$, with $q_0, \ldots, q_g$ primes different from $p_0, \ldots, p_f$, and $g, r_0, \ldots, r_f, v_0, \ldots, d_g$ positive integers. Using Lemma 5, the condition on m in (24) implies

$$\begin{aligned} &p_0^{t_0+r_0-1}(p_0-1) \times \cdots \times p_f^{t_f+r_f-1}(p_f-1) \\ &\quad \times q_0^{v_0-1}(q_0-1) \times \cdots \times q_g^{v_g-1}(q_g-1) = \\ &p_0^{t_0-1}(p_0-1) \times \cdots \times p_f^{t_f-1}(p_f-1) \times p_0^{r_0} \times \cdots \times p_f^{r_f} \\ &\quad \times q_0^{v_0} \times \cdots \times p_g^{v_g} \end{aligned} \tag{25}$$

which implies that $q_0 = \cdots = q_g = 1$, and the only possibility is that m contains powers of the primes that divide n, i.e., $m = p_0^{r_0} \times \ldots \times p_f^{r_f}$. Given this necessary condition on m, one needs to verify that

$$\left\{1, w_{nm}^{nk+1}, \left(w_{nm}^{nk+1}\right)^2, \ldots, \left(w_{nm}^{nk+1}\right)^{m-1}\right\}$$

are algebraically independent over $\mathbb{Z}[w_n]$ for $k = 1, \ldots, m$. For that, one first observes that w_{nm}^{nk+1} is a root of the minimal polynomial $\mu(X) = X^m - w_n$ over $\mathbb{Z}[w_n]$ for $k = 1, \ldots, m$. Therefore, it suffices to prove that they are conjugate in order to prove the Theorem for n even. To this end, one observes that for this choice of m

$$(nk+1 | nm) = 1, \qquad \forall\, k = 1, \ldots, m$$

because $nk + 1$ is not divisible by $2, p_1, \ldots, p_f$, since

$$\operatorname{mod}(nk+1, p_l) = 1, \qquad \text{for } l = 1, \ldots, f.$$

Therefore, using Lemma 6 implies that $w_{nm}^{nk+1}, k = 1, \ldots, m$ are conjugates. Hence, $d_{\boldsymbol{U}}(\mathcal{S}) \neq 0 \in \mathcal{R}$ for n even and m chosen such that it only contains powers of the primes that divide n.

2) When n is odd: then, the eigenvalues of matrix $\boldsymbol{M}(\boldsymbol{s})$(15) are given by

$$\begin{aligned} \lambda_k &= s_1 + s_2 w_{2n}^{\frac{1}{m}}(w_m^k) + \cdots + s_m w_{2n}^{\frac{m-1}{m}}(w_m^k)^{m-1}, \qquad k=1,\ldots,m \\ &= s_1 + s_2 w_{2nm}^{2nk+1} + \cdots + s_m \left(w_{2nm}^{2nk+1}\right)^{m-1}, \qquad k=1,\ldots,m. \end{aligned} \tag{26}$$

We follow exactly the same approach as above, where one has the new necessary condition

$$\Phi(2nm) = m\Phi(n) \tag{27}$$

since one needs $\mathbb{Q}(w_{2nm})$ to be an *extension* of degree m over $\mathbb{Q}(w_n)$. To solve (27), one decomposes n and m into primes, where in this case, one obtains the only solution for m satisfying (27), that is, $m = 2^{r_0} \times p_1^{r_1} \times \ldots \times p_f^{r_f}$, where $p_1, \ldots, p_f$ are all the primes (different from 2) that divide n. Note that one can still have 2 among the primes dividing m in this case, because $\Phi(2^{r_0}) = 2^{r_0-1}(2-1) = 2^{r_0-1}$. Given this necessary choice of m, one verifies that

$$\left\{1, w_{2nm}^{2nk+1}, \left(w_{2nm}^{2nk+1}\right)^2, \ldots, \left(w_{2nm}^{2nk+1}\right)^{m-1}\right\}$$

are algebraically independent over $\mathbb{Z}[w_n]$ for $k = 1, \ldots, m$. For that, one again notes that w_{2nm}^{nk+1} is a root of the minimal polynomial $\mu(X) = X^m - w_{2n}$ over $\mathbb{Z}[w_n]$ for $k = 1, \ldots, m$. Therefore, it suffices to prove that these numbers are conjugate in order to prove the Theorem for n odd. Observe that for this choice of m

$$(2nk+1 | 2nm) = 1, \qquad \forall\, k = 1, \ldots, m$$

because $nk + 1$ is not divisible by $2, p_1, \ldots, p_f$, since $\operatorname{mod}(nk + 1, p_l) = 1$ for $l = 1, \ldots, f$. Therefore, using Lemma 6 implies that $w_{nm}^{nk+1}, k = 1, \ldots, m$ are conjugates. Therefore, $d_{\boldsymbol{U}}(\mathcal{S}) \neq 0 \in \mathcal{R}$ for n odd and m chosen such that it only contains powers of the primes that divide n in addition to powers of 2. Finally, note that choosing $\phi = w_n$ gives the same results as $\phi = w_{2n}$, but limits the choice of m to only contain powers of primes that divide n if m and n satisfy (24), since one needs now to have $\mathbb{Q}(w_{nm})$ as an extension of degree m over the cyclotomic field $\mathbb{Q}(w_n)$. □

References

[1] K. Boullé and J.-C. Belfiore, "Modulation schemes designed for the Rayleigh fading channel," in *Proc. Conf. Informotion Science and Systems*, Princeton, NJ, Mar. 1992, pp. 288–293.

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

[3] M. O. Damen, A. Tewfik, and J.-C. Belfiore, "A construction of a space-time code based on number theory," *IEEE Trans. Inform. Theory*, vol. 48, pp. 753–761, Mar 2002.

[4] H. El Gamal and M. O. Damen, "Universal space-time coding," *IEEE Trans. Inform. Theory*, vol. 49, pp. 1097–1119, May 2003.

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

[6] J. Boutros, E. Viterbo, C. Rastello, and J.-C. Belfiore, "Good lattice constellations for both Rayleigh fading and Gaussian channels," *IEEE Trans. Inform. Theory*, vol. 42, pp. 502–518, May 1996.

[7] J.-C. Belfiore, X. Giraud, and J. Rodriguez, "Optimal linear labeling for the minimization of both source and channel distortion," in *Proc. IEEE Int. Symp. Information Theory*, Sorrento, Italy, June 2000, p. 404.

[8] G. Golub and C. Van Loan, *Matrix Computations*, 3 ed. Baltimore, MD: John Hopkins Univ. Press, 1996.

[9] V. M. DaSilva and E. S. Sousa, "Fading-resistant modulation using several transmitter antennas," *IEEE Trans. Commun.*, vol. 45, pp. 1236–1244, Oct. 1997.

[10] Y. Xin, Z. Wang, and G. B. Giannakis, "Linear unitary precoders for maximum diversity gains with multiple transmit and receive-antennas," in *Proc. 34th Asilomar Conf. on Signals, Systems, and Computers*, Pacific Grove, CA, Oct. 29–Nov. 1, 2000, pp. 1553–1557.

[11] D. A. Marcus, *Number Fields*. New York: Springer-Verlag, 1977.

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

[13] J. G. Proakis, *Digital Communications*, 4th ed. New York: McGraw-Hill, 2000.

[14] W. M. Schmidt, *Diophantine Approximation*. Berlin, Germany: Springer-Verlag, 1980.

[15] D. L. Goeckel and G. Ananthaswamy, "On the design of multi-dimensional signal sets for OFDM," *IEEE Trans. Commun.*, vol. 50, pp. 442–452, Mar. 2002.

[16] Y. Xin, Z. Wang, and G. B. Giannakis, "Space-time diversity systems based on linear constellation precoding," *IEEE Trans. Wireless Commun.*, vol. 2, pp. 294–309, Mar. 2003.

[17] A. B. Shidlovskii, *Transcendental Numbers*. New York: W. de Gruyter, 1989.

[18] A. Khinchin, *Continued Fractions*. Chicago , IL: Univ. Chicago Press, 1964.

[19] C. Lamy and J. Boutros, "On random rotations diversity and minimum mse decoding of lattices," *IEEE Trans. Inform. Theory*, vol. 46, pp. 1584–1589, July 2000.

[20] M. O. Damen, "Joint Coding Decoding in a Multiple Access System, Application to Mobile Communications," Ph.D. dissertation, ENST de Paris, Paris, France, 1999.

[21] C. F. Van Loan, *Computational Frameworks for the Fast Fourier Transform*. Philadelphia, PA: SIAM, 1992.

[22] R. A. Horn and C. R. Johnson, *Matrix Analysis*. Cambridge, U.K: Cambridge Univ. Press, 1993.