Complex-Field Coding for OFDM Over Fading Wireless Channels

Zhengdao Wang, *Member, IEEE,* and Georgios B. Giannakis, *Fellow, IEEE*

***Abstract*—Orthogonal frequency-division multiplexing (OFDM) converts a time-dispersive channel into parallel subchannels, and thus facilitates equalization and (de)coding. But when the channel has nulls close to or on the fast Fourier transform (FFT) grid, uncoded OFDM faces serious symbol recovery problems. As an alternative to various error-control coding techniques that have been proposed to ameliorate the problem, we perform complex-field coding (CFC) before the symbols are multiplexed. We quantify the maximum achievable diversity order for independent and identically distributed (i.i.d.) or correlated Rayleigh-fading channels, and also provide design rules for achieving the maximum diversity order. The maximum coding gain is given, and the encoder enabling the maximum coding gain is also found. Simulated performance comparisons of CFC-OFDM with existing block and convolutionally coded OFDM alternatives favor CFC-OFDM for the code rates used in a HiperLAN2 experiment.**

***Index Terms*—Analog codes, coding gain, complex-field coding (CFC), diversity order, fading, maximum-distance separable (MDS), orthogonal frequency-division multiplexing (OFDM), real-number codes.**

I. Introduction

BY implementing the inverse fast Fourier transform (IFFT) at the transmitter and fast Fourier transform (FFT) at the receiver, orthogonal frequency-division multiplexing (OFDM) converts an intersymbol interference (ISI)-inducing channel with additive white Gaussian noise (AWGN) into parallel ISI-free subchannels, with gains equal to the channel's frequency response values on the FFT grid. Each subchannel can be easily equalized by a single-tap equalizer using scalar division. To avoid interblock (IBI) and interchannel (ICI) interferences between successive IFFT processed blocks, a cyclic prefix (CP) of length greater than or equal to the channel order is inserted per block at the transmitter and discarded at the receiver. In addition to suppressing IBI, the CP also converts linear convolution into cyclic convolution, and thus facilitates diagonalization of the associated channel matrix (see, e.g., [36]).

Manuscript received April 20, 2001; revised November 1, 2002. This work was supported by the NSF under Grant CCR-9805350 and by the NSF under the Wireless Initiative Grant 9979443. The material in this paper was presented in part at the the Workshop on Signal Processing Advances in Wireless Communication, Taoyuan, Taiwan, ROC, March 2001.

Z. Wang is with the Department of Electrical and Computer Engineering, Iowa State University, Ames, IA 50011 USA (e-mail: zhengdao@iastate.edu).

G. B. Giannakis is with the Department of Electrical and Computer Engineering, University of Minnesota, Minneapolis, MN 55455 USA (e-mail: georgios@ece.umn.edu).

Communicated by T. Fuja, Associate Editor At Large.

Digital Object Identifier 10.1109/TIT.2002.808101

Instead of bringing multipath diversity in the form of superimposed (delayed and scaled) replicas of the transmitted symbols as is the case with serial transmissions, OFDM transfers the multipath diversity to the frequency domain in the form of (usually correlated) fading frequency response samples. Each OFDM subchannel has its gain being expressed as a linear combination of the dispersive channel taps. When the channel has nulls (deep fades) close to or on the FFT grid, reliable detection of the symbols carried by these faded subcarriers becomes difficult, if not impossible.

Error-control codes are usually invoked before the IFFT processing to deal with the frequency-selective fading. These include convolutional codes, trellis-coded modulation (TCM) or coset codes, turbo codes, and block codes (e.g., Reed–Solomon (RS) or Bose–Chaudhuri–Hocquenghem (BCH)). Such coded OFDM schemes often incur high complexity and/or large decoding delay [15]. Some of them also require channel state information (CSI) at the transmitter [25], [26], which may be unrealistic or too costly to acquire in wireless applications, where the channel is rapidly changing. Another approach to guaranteeing symbol detectability over ISI channels is to modify the OFDM setup: instead of introducing the CP, each IFFT-processed block can be zero padded (ZP) by at least as many zeros as the channel order [10], [22], [36].

In this paper, we consider robustifying OFDM against random frequency-selective fading by introducing memory into the transmission with *complex-field coding (CFC)* across the subcarriers. We will also abbreviate the complex-field coder as CFC, when no confusion arises. The resulting OFDM system will be termed CFC-OFDM. Specifically, instead of sending uncoded symbols (one per subcarrier), our idea is to send different linear combinations of the information symbols on the subcarriers—an OFDM scheme coded with a complex-field block encoder. This generalizes the notion of *signal space diversity* [3] to encompass redundant encoding. The CFC considered here can also be viewed as a form of real-number, or analog, codes [13], [21], [40]. Analog codes were pursued in [21], [40] for correcting impulsive noise in analog transmission or storage, and later on studied in [12] for multiple error correction. Some coding and decoding aspects of analog codes and numerical issues were treated in [12], [13]. Recently, analog codes have also been used for transmitting continuous valued sources over stationary AWGN channels [4], for peak-to-average ratio reduction [14], and for performance improvement of *fixed* ISI channels as the so-termed modulated codes [10], [41]. In the signal processing literature, sending linear combinations of symbols is also known as *linear precoding*, which has been

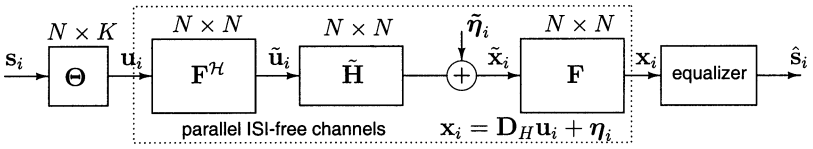

Fig. 1. CFC-OFDM. The blocks within the dotted box correspond to conventional OFDM system.

used for channel identification and equalization, and dates back to the early works of Tomlinson-Harashima precoding [27].

We will design the CFC so that maximum diversity order can be guaranteed without an essential decrease in transmission rate. By performing pairwise error probability analysis, we will upper-bound the diversity order of OFDM transmissions over random frequency-selective fading channels. As expected, and we will also see it in our context, the diversity order is directly related to the Hamming distance between coded symbols. It turns out that CFC can be designed to guarantee maximum diversity order irrespective of the underlying constellation, and with minimum redundancy. The so designed complex-field (CF) codes are maximum-distance separable (MDS) in the real or complex field, which generalizes the well-known MDS concept for Galois field (GF) [20, Ch. 11] codes. We construct two classes of CFC that can achieve MDS and guarantee maximum diversity order: the Vandermonde class, which generalizes the RS codes to the real/complex field, and the Cosine class, which does not have a GF counterpart.

Our CF-coded OFDM system model is presented in Section II. The system performance analysis and optimal design rules are given in Section III. Section V deals with decoder design, while Section VI is devoted to comparisons of the proposed system with other existing schemes by simulations.

Notation: Bold upper case letters denote matrices and bold lower case letters denote vectors; $(\cdot)^T$ and $(\cdot)^{\mathcal{H}}$ denote transpose and Hermitian transpose, respectively; $[\cdot]_{i,j}$ denotes the (i,j)th entry of a matrix; $\boldsymbol{I}_M$ denotes the identity matrix of size M; $\mathrm{diag}(\boldsymbol{x})$ is a diagonal matrix with $\boldsymbol{x}$ on its diagonal; $E[\cdot]$ denotes statistical average. We always index matrix and vector entries starting from 0. Complex, real, GF, and the integer ring will be denoted as $\mathbb{C}, \mathbb{R}, \mathbb{F}$, and $\mathbb{Z}$, respectively. For a vector, $||\cdot||$ denotes the Euclidean norm; for a set, $|\cdot|$ denotes its cardinality.

II. Linear Complex-Field Coded OFDM

A. System Model

Fig. 1 depicts the discrete-time baseband equivalent block model detailed in [36] for a CFC-OFDM system with N subcarriers. Due to CP-insertion at the transmitter and CP-removal at the receiver, the dispersive channel is represented as an $N \times N$ circulant channel matrix $\tilde{\boldsymbol{H}}$, with

$$[\tilde{\boldsymbol{H}}]_{i,j} = h((i-j) \bmod N)$$

where $h(\cdot)$ denotes the channel impulse response that accounts for transmit and receive filters and the physical propagation effects [36]

$$\tilde{\boldsymbol{H}} = \begin{bmatrix} h(0) & 0 & \dots & & 0 & h(L) & \dots & h(1) \\ \vdots & h(0) & 0 & \dots & & \ddots & \ddots & \vdots \\ h(L) & \vdots & \ddots & \ddots & & \dots & 0 & h(L) \\ 0 & h(L) & & \ddots & 0 & & & 0 \\ \vdots & 0 & & & h(0) & \ddots & & \vdots \\ & \vdots & \ddots & \ddots & \vdots & \ddots & & 0 \\ 0 & \dots & & 0 & h(L) & & \dots & h(0) \end{bmatrix}.$$

We assume the channel to be random, with finite impulse response (FIR), consisting of no more than $L+1$ taps. The blocks within the dotted box represent a conventional uncoded OFDM system.

Let $\boldsymbol{F}$ denote the $N \times N$ FFT matrix with entries

$$[\boldsymbol{F}]_{n,k} = (1/\sqrt{N}) \exp(-j2\pi nk/N).$$

Performing IFFT (postmultiplication with the matrix $\boldsymbol{F}^{\mathcal{H}}$) at the transmitter and FFT (premultiplication with the matrix $\boldsymbol{F}$) at the receiver diagonalizes the circulant matrix $\tilde{\boldsymbol{H}}$. So, we obtain the parallel ISI-free model for the ith OFDM symbol as (see Fig. 1): $\boldsymbol{x}_i = \boldsymbol{D}_H \boldsymbol{u}_i + \boldsymbol{\eta}_i$, where

$$\begin{aligned} \boldsymbol{D}_H &:= \mathrm{diag}\left[H(j0), H\left(j2\pi\frac{1}{N}\right), \dots, H\left(j2\pi\frac{N-1}{N}\right)\right] \\ &= \boldsymbol{F}\tilde{\boldsymbol{H}}\boldsymbol{F}^{\mathcal{H}} \end{aligned}$$

with $H(j\omega)$ denoting the channel frequency response at ω; and $\boldsymbol{\eta}_i = \boldsymbol{F}\tilde{\boldsymbol{\eta}}_i$ standing for the FFT-processed AWGN.

In order to exploit the frequency-domain diversity in OFDM, our CFC-OFDM design first linearly encodes (i.e., maps) the $K \leq N$ symbols of the ith block, $\boldsymbol{s}_i \in \mathcal{S}$, where $\mathcal{S}$ is the set of all possible vectors that $\boldsymbol{s}_i$ may belong to (e.g., the binary phase-shift keying (BPSK) set $\{\pm 1\}^{K\times 1}$), by an $N \times K$ matrix $\boldsymbol{\Theta} \in \mathbb{C}^{N\times K}$; and then multiplexes the coded symbols $\boldsymbol{u}_i = \boldsymbol{\Theta}\boldsymbol{s}_i \in \mathbb{C}^{N\times 1}$ using conventional OFDM. In practice, the set $\mathcal{S}$ is always finite, but we allow it to be infinite in our performance analysis. The encoder $\boldsymbol{\Theta}$ considered here does not depend on the OFDM symbol index i. Time-varying encoders may be useful for certain purposes (e.g., power loading), but they will not be pursued here since no CSI is assumed available at the transmitter. Hence, from now on, we will drop our OFDM symbol index i for brevity.

Notice that the matrix–vector multiplication used in defining $\boldsymbol{u} = \boldsymbol{\Theta}\boldsymbol{s}$ takes place in the complex field, rather than a GF.

The matrix $\boldsymbol{\Theta}$ can be naturally viewed as the *generating matrix* of a *complex-field block code*. The *codebook* is defined as $\mathcal{U} := \{\boldsymbol{\Theta s} | \boldsymbol{s} \in \mathcal{S}\}$. By encoding a length-$K$ vector to a length-N vector, some redundancy is introduced that we quantify by the *rate* of the code defined to be $r = K/N$, reminiscent of the GF block code rate definition. The set $\mathcal{U}$ is a subset of the $\mathbb{C}^{N\times 1}$ vector space. More specifically, $\mathcal{U}$ is a subset of the K-dimensional subspace spanned by the columns of $\boldsymbol{\Theta}$. When $\mathcal{S} = \mathbb{Z}^{K\times 1}$, the set $\mathcal{U}$ forms a lattice [5].

Combining the encoder with the diagonalized channel model, each received block after CP removal and FFT processing can be written as (see also Fig. 1)

$$\boldsymbol{x} = \boldsymbol{F}\tilde{\boldsymbol{x}} = \boldsymbol{F}(\tilde{\boldsymbol{H}}\boldsymbol{F}^{\mathcal{H}}\boldsymbol{\Theta s} + \tilde{\boldsymbol{\eta}}) = \boldsymbol{D}_H\boldsymbol{\Theta s} + \boldsymbol{\eta}. \tag{1}$$

We wish to design $\boldsymbol{\Theta}$ so that a large diversity order can be guaranteed, irrespective of the constellation that the entries of $\boldsymbol{s}$ are drawn from, and with a small amount of redundancy.

We can conceptually view $\boldsymbol{\Theta}$ together with the OFDM modulation $\boldsymbol{F}^{\mathcal{H}}$ as a combined $N \times K$ encoder $\bar{\boldsymbol{\Theta}} := \boldsymbol{F}^{\mathcal{H}}\boldsymbol{\Theta}$, which in a sense unifies single-carrier and multicarrier block transmissions. Indeed, by proper selection of $\boldsymbol{\Theta}$, hence $\bar{\boldsymbol{\Theta}}$, the system in Fig. 1 can describe various single and multicarrier systems, some of which we will present shortly as special cases of our CFC-OFDM. The received vector $\tilde{\boldsymbol{x}}$ is related to the information symbol vector $\boldsymbol{s}$ through the matrix product $\tilde{\boldsymbol{H}}\bar{\boldsymbol{\Theta}}$. One question concerns the invertibility of this input–output relationship: for what $\bar{\boldsymbol{\Theta}}$, will $\tilde{\boldsymbol{H}}\bar{\boldsymbol{\Theta}}$ have full column rank for *any* realization of the FIR channel coefficients? Another question is: if the channel is modeled with random taps, what is a good choice of $\bar{\boldsymbol{\Theta}}$ for enhancing the average bit error rate (BER) performance? We will answer these closely related (and other) questions in the paper. Although we can even start our description of the system from a general setup using $\bar{\boldsymbol{\Theta}}$, and indeed many of our results apply to general transmissions over multipath channels without specifically relying on OFDM, factoring $\boldsymbol{F}^{\mathcal{H}}$ out from $\bar{\boldsymbol{\Theta}}$ will offer us both mathematical and conceptual convenience.

B. Euclidean Versus Hamming Distance

The *Hamming distance* $\delta(\boldsymbol{u}, \boldsymbol{u}')$ between two vectors $\boldsymbol{u}$ and $\boldsymbol{u}'$ is defined as the number of nonzero entries in the vector $\boldsymbol{u}_e = \boldsymbol{u} - \boldsymbol{u}'$, and the *minimum Hamming distance* of the set $\mathcal{U}$ as

$$\delta_{\min}(\mathcal{U}) := \min\{\delta(\boldsymbol{u}, \boldsymbol{u}') | \boldsymbol{u}, \boldsymbol{u} \in \mathcal{U}\}.$$

When there is no confusion, we will simply use $\delta_{\min}$ for brevity. The minimum Euclidean distance between any two vectors in $\mathcal{U}$ is denoted as $d_{\min}(\mathcal{U})$ or simply $d_{\min}$.

Because our encoding $\boldsymbol{u} = \boldsymbol{\Theta s}$ operates in the complex field, it does not increase the dimensionality of the signal space. This is to be contrasted to the GF encoding: the codeword set of a GF (n, k) code, *when viewed as a real/complex vector*, in general has a higher dimensionality (n) than that of the original uncoded block of k symbols. Exceptions include the repetition code, for which the codeword set has the same dimensionality as that of the encoder input.

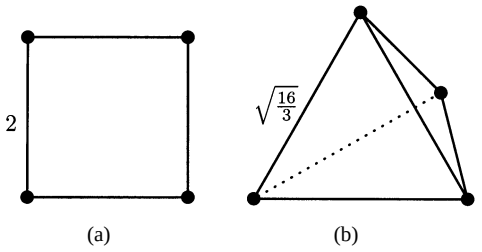

Fig. 2. Uncoded (a) and GF-coded (b) BPSK signals in Example 1.

Example 1: Consider the binary $(3, 2)$ block code generated by the matrix

$$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}^T \tag{2}$$

followed by BPSK constellation mapping (e.g., $0 \rightarrow 1$ and $1 \rightarrow -1$). The codebook consists of four codewords

$$\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} -1 \\ 1 \\ -1 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \\ -1 \end{bmatrix}, \begin{bmatrix} -1 \\ -1 \\ 1 \end{bmatrix}. \tag{3}$$

These codewords span the $\mathbb{R}^{3\times 1}$ (or $\mathbb{C}^{3\times 1}$) space, and therefore the codebook has dimension 3 in the real or complex field; see also Fig. 2. □

In general, an (n, k) binary GF block code is capable of generating 2^k codewords in an n-dimensional space $\mathbb{R}^{n\times 1}$ or $\mathbb{C}^{n\times 1}$. If we view the transmit signal design problem as packing spheres in the signal space (Shannon's point of view), an (n, k) GF block code followed by constellation mapping packs spheres in an n-dimensional space and thus has the potential to be better (larger sphere radius) than a k-dimensional packing. In our example, if we normalize the codewords by a factor $\sqrt{2/3}$ so that the energy per bit E_b is one, the four codewords have *Euclidean* distance $\sqrt{16/3}$, larger than the minimum distance 2 of the signal set of two uncoded BPSK symbols $\{(1, 1), (1, -1), (-1, 1), (-1, -1)\}$. This increase in minimum Euclidean distance leads to improved system performance in AWGN channels, at least for high signal-to-noise ratios (SNR). For fading channels, however, the minimum *Hamming* distance of the codebook dictates high SNR performance in the form of diversity gain (as will become clear later). The diversity gain achieved by the $(3, 2)$ block code in the example equals the minimum Hamming distance 2.

CFC, on the other hand, does not increase signal dimension; i.e., we always have $\dim(U) \leq \dim(S)$. When $\boldsymbol{\Theta}$ has full column rank K, $\dim(U) = \dim(S)$, in which case the codewords span a K-dimensional subspace of the N-dimensional vector space $\mathbb{C}^{N\times 1}$. In terms of sphere packing, *CFC does not yield a packing of dimension higher than K*.

We have the following assertion about the minimum Euclidean distance.

Proposition 1: Suppose $\mathrm{tr}(\boldsymbol{\Theta}\boldsymbol{\Theta}^{\mathcal{H}}) = K$. If the entries of $\boldsymbol{s} \in \mathcal{S}$ are drawn independently from a constellation $\mathcal{A}$ of minimum Euclidean distance of $d_{\min}(\mathcal{A})$, then the codewords in $\mathcal{U} := \{\boldsymbol{\Theta s} | \boldsymbol{s} \in \mathcal{S}\}$ have minimum Euclidean distance no more than $d_{\min}(\mathcal{A})$.

Proof: Under the power constraint $\mathrm{tr}(\boldsymbol{\Theta}\boldsymbol{\Theta}^{\mathcal{H}}) = K$, at least one column of $\boldsymbol{\Theta}$ will have Euclidean norm no more than 1. Without loss of generality, suppose the first column has Euclidean norm no more than 1. Consider $\boldsymbol{s}_\alpha = (\alpha, 0, \ldots, 0)^T$ and $\boldsymbol{s}_\beta = (\beta, 0, \ldots, 0)^T$, where α and β are two symbols from the constellation that are separated by $d_{\min}(\mathcal{A})$. The coded vectors $\boldsymbol{u}_\alpha = \boldsymbol{\Theta}\boldsymbol{s}_\alpha$ and $\boldsymbol{u}_\beta = \boldsymbol{\Theta}\boldsymbol{s}_\beta$ are then separated by a distance no more than $d_{\min}(\mathcal{A})$. □

Due to Proposition 1, CF codes are not effective for improving performance over AWGN channels. But for fading channels, they may have an advantage over GF codes, because they are capable of producing codewords that have large Hamming distance.

Example 2: The complex-field encoder

$$\boldsymbol{\Theta} = \sqrt{\frac{4}{15}} \begin{bmatrix} 1 & 1 & 1 \\ 0.5 & -0.5 & 0.5 \end{bmatrix}^T \tag{4}$$

operating on the BPSK signal set $\mathcal{S} = \{\pm 1\}^2$, produces four codewords of minimum Euclidean distance $\sqrt{4/5}$, and minimum Hamming distance 3. Compared with the GF code in Example 1, this real code has smaller Euclidean distance, but larger Hamming distance. □

Another difference of our CF coding from the GF block coding is that the entries of the CFC output vector $\boldsymbol{u}$ usually belong to a larger (although still finite) alphabet set than do the entries of the input vector $\boldsymbol{s}$; see also [13, Appendix]. This may suggest at first glance lower performance in decoding. However, when viewed (and decoded) as blocks, the number of possible $\boldsymbol{s}$'s is the same as the number of possible $\boldsymbol{u}$'s, which does not degrade performance.

C. Special Cases of CFC-OFDM

Before exploring optimal designs for $\boldsymbol{\Theta}$, let us first look at some special cases of the CFC-OFDM system.

1) Uncoded OFDM: By setting $K = N$ and $\boldsymbol{\Theta} = \boldsymbol{I}_N$, we obtain the conventional uncoded OFDM model. In such a case, the one-tap linear equalizer matrix $\boldsymbol{\Gamma} = \boldsymbol{D}_H^{-1}$ yields $\hat{\boldsymbol{s}} = \boldsymbol{\Gamma}\boldsymbol{x} = \boldsymbol{s} + \boldsymbol{D}_H^{-1}\boldsymbol{\eta}$, where the inverse exists when the channel has no nulls on the FFT grid. When $\tilde{\boldsymbol{\eta}}$ (hence $\boldsymbol{\eta}$) is AWGN, such an equalizer followed by a minimum-distance quantizer is optimum in the maximum-likelihood (ML) sense for a given channel when CSI has been acquired at the receiver. But when the channel has nulls on (or close to) the FFT grid $\omega = 2\pi n/N$, $n = 0, \ldots, N-1$, the matrix $\boldsymbol{D}_H$ will be ill-conditioned and serious noise amplification will emerge if we try to invert $\boldsymbol{D}_H$ (the noise variance can grow unbounded). Although events of channel nulls being close to the FFT grid have relatively low probability, their occurrence is known to have deleterious impact on the average system performance especially at high SNR. Improving the performance of an uncoded transmission thus amounts to robustifying the system against the occurrence of such low-probability but catastrophic events. If CSI is available at the transmitter, power and bit loading can be used and channel nulls can be avoided, as in discrete multitone (DMT) systems [25].

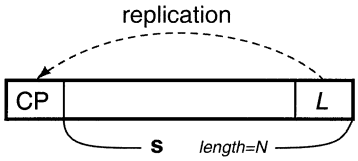

Fig. 3. CP-only transmission.

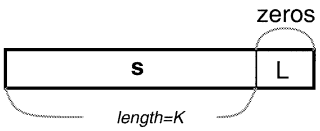

Fig. 4. ZP-only transmission.

2) CP-Only Transmission: If we choose $K = N$ and $\boldsymbol{\Theta} = \boldsymbol{F}$, then since $\boldsymbol{F}^{\mathcal{H}}\boldsymbol{F} = \boldsymbol{I}_N$, the IFFT $\boldsymbol{F}^{\mathcal{H}}$ annihilates the encoding and the resulting system is a single-carrier block transmission with CP insertion (cf. Fig. 3): $\tilde{\boldsymbol{x}} = \tilde{\boldsymbol{H}}\boldsymbol{s} + \tilde{\boldsymbol{\eta}}$. The term CP-only is used to emphasize the fact that no (I)FFT is taken at the transmitter and receiver [6], [36].

3) ZP-Only Transmission: Consider $K = N - L$, and choose $\boldsymbol{\Theta}$ to be an $N \times K$ truncated FFT matrix (the first K columns of $\boldsymbol{F}$); i.e., $[\boldsymbol{\Theta}]_{n,k} = (1/\sqrt{N})\exp(-j2\pi nk/N)$. It can be easily verified that $\boldsymbol{F}^{\mathcal{H}}\boldsymbol{\Theta} = [\boldsymbol{I}_K, \boldsymbol{0}_{K\times L}]^T := \boldsymbol{T}_{\mathrm{zp}}$, where $\boldsymbol{0}_{K\times L}$ denotes a $K \times L$ all-zero matrix, and the subscript "zp" stands for zero padding. The matrix $\boldsymbol{T}_{\mathrm{zp}}$ simply pads zeros at the tail of $\boldsymbol{s}$, and the zero-padded block $\tilde{\boldsymbol{u}} = \boldsymbol{T}_{\mathrm{zp}}\boldsymbol{s}$ is transmitted (see Fig. 4). Notice that $\boldsymbol{H} := \tilde{\boldsymbol{H}}\boldsymbol{F}^{\mathcal{H}}\boldsymbol{\Theta} = \tilde{\boldsymbol{H}}\boldsymbol{T}_{\mathrm{zp}}$ now becomes an $N \times K$ Toeplitz convolution matrix (the first K columns of $\tilde{\boldsymbol{H}}$), which is *always full rank*. The symbols $\boldsymbol{s}$ can thus always be recovered from the received signal $\tilde{\boldsymbol{x}} = \boldsymbol{H}\boldsymbol{s} + \tilde{\boldsymbol{\eta}}$ (perfectly in the absence of noise), and no "catastrophic channels" exist in this case [36] (unless the channel is all-zero). The CP in this case consists of L zeros, which, together with the L zeros from the encoding process, result in $2L$ consecutive zeros between two consecutive uncoded information blocks of length K. But only L zeros are needed in order to separate the information blocks. CP is therefore not necessary because the L zeros created by $\boldsymbol{\Theta}$ already separate successive blocks.

ZP-only transmission is essentially a simple *single-carrier* block scheme. However, viewing it as a special case of the CFC-OFDM design will allow us to apply the results about CFC-OFDM and gain insights about its performance. It turns out that this special case is indeed very special: it achieves the best high-SNR performance among all members of the CFC-OFDM class (Theorem 6).

III. Performance Criteria and Encoder Design

We will now address the problem of designing $\boldsymbol{\Theta}$ with the goal of improving performance over uncoded OFDM. We will resort to the pairwise error probability (PEP) analysis technique that has also been used recently in a different (space–time) context in [32]. For simplicity, we will first make the following assumption.

AS1) The channel $\boldsymbol{h} := [h(0), h(1), \ldots, h(L)]^T$ has independent and identically distributed (i.i.d.) zero-mean complex

Gaussian taps (Rayleigh fading). The corresponding correlation matrix of $\boldsymbol{h}$ is $\boldsymbol{R}_h := E[\boldsymbol{h}\boldsymbol{h}^{\mathcal{H}}] = \alpha_L^2 \boldsymbol{I}_{L+1}$, where the constant $\alpha_L := 1/(L+1)$ is chosen so as to make the average channel energy one.

Later, we will relax this assumption to allow for correlated fading with possibly rank-deficient autocorrelation matrix $\boldsymbol{R}_h$.

A. Performance Criteria

We suppose ML detection with perfect CSI at the receiver and consider the probability $P(\boldsymbol{s} \to \boldsymbol{s}'|\boldsymbol{h})$, $\boldsymbol{s}, \boldsymbol{s}' \in \mathcal{S}$, that a vector $\boldsymbol{s}$ is transmitted but is erroneously decoded as $\boldsymbol{s}' \neq \boldsymbol{s}$. We define the set of all possible error vectors

$$\mathcal{S}_e := \{\boldsymbol{e} := \boldsymbol{s} - \boldsymbol{s}' | \boldsymbol{s}, \boldsymbol{s}' \in \mathcal{S}, \boldsymbol{s} \neq \boldsymbol{s}'\}.$$

The PEP can be approximated using the Chernoff bound as

$$\boldsymbol{P}(\boldsymbol{s} \to \boldsymbol{s}'|\boldsymbol{h}) \leq \exp\left(\frac{-d^2(\boldsymbol{y}, \boldsymbol{y}')}{4N_0}\right) \tag{5}$$

where $N_0/2$ is the noise variance per real dimension, $\boldsymbol{y} := \boldsymbol{D}_H \boldsymbol{\Theta} \boldsymbol{s}$, $\boldsymbol{y}' := \boldsymbol{D}_H \boldsymbol{\Theta} \boldsymbol{s}'$, and $d(\boldsymbol{y}, \boldsymbol{y}') = \|\boldsymbol{y} - \boldsymbol{y}'\|$ is the Euclidean distance between $\boldsymbol{y}$ and $\boldsymbol{y}'$.

Let us consider the $N \times (L+1)$ matrix $\boldsymbol{V}$ with entries $[\boldsymbol{V}]_{n,l} = \exp(-j2\pi nl/N)$, and use it to perform the N-point discrete Fourier transform $\boldsymbol{V}\boldsymbol{h}$ of $\boldsymbol{h}$. Note that $\boldsymbol{D}_H = \mathrm{diag}(\boldsymbol{V}\boldsymbol{h})$; i.e., the diagonal entries of $\boldsymbol{D}_H$ are those in the vector $\boldsymbol{V}\boldsymbol{h}$. Using the definitions $\boldsymbol{e} := \boldsymbol{s} - \boldsymbol{s}' \in \mathcal{S}_e$, $\boldsymbol{u}_e := \boldsymbol{\Theta}\boldsymbol{e}$, and $\boldsymbol{D}_e := \mathrm{diag}(\boldsymbol{u}_e)$, we can write

$$\boldsymbol{y} - \boldsymbol{y}' = \boldsymbol{D}_H \boldsymbol{u}_e = \mathrm{diag}(\boldsymbol{V}\boldsymbol{h})\boldsymbol{u}_e.$$

Furthermore, we can express the squared Euclidean distance $d^2(\boldsymbol{y}, \boldsymbol{y}') = \|\boldsymbol{D}_H \boldsymbol{u}_e\|^2 = \|\boldsymbol{D}_e \boldsymbol{V}\boldsymbol{h}\|^2$ as

$$d^2(\boldsymbol{y}, \boldsymbol{y}') = \boldsymbol{h}^{\mathcal{H}} \boldsymbol{V}^{\mathcal{H}} \boldsymbol{D}_e^{\mathcal{H}} \boldsymbol{D}_e \boldsymbol{V}\boldsymbol{h} =: \boldsymbol{h}^{\mathcal{H}} \boldsymbol{A}_e \boldsymbol{h}. \tag{6}$$

An upper bound to the average PEP can be obtained by averaging (5) with respect to the random channel $\boldsymbol{h}$ to obtain (see, e.g., [32])

$$\boldsymbol{P}(\boldsymbol{s} \to \boldsymbol{s}') \leq \prod_{l=0}^{L} \frac{1}{1 + \frac{\alpha_L \lambda_{e,l}}{(4N_0)}}, \tag{7}$$

where $\lambda_{e,0}, \lambda_{e,1}, \ldots, \lambda_{e,L}$ are the nonincreasing eigenvalues of the matrix $\boldsymbol{A}_e = \boldsymbol{V}^{\mathcal{H}} \boldsymbol{D}_e^{\mathcal{H}} \boldsymbol{D}_e \boldsymbol{V}$.

If r_e is the rank of $\boldsymbol{A}_e$, then $\lambda_{e,l} \neq 0$ if and only if $l \in [0, r_e - 1]$. Since

$$1 + \alpha_L \lambda_{e,l}/(4N_0) > \alpha_L \lambda_{e,l}/(4N_0)$$

it follows from (7) that

$$\boldsymbol{P}(\boldsymbol{s} \to \boldsymbol{s}') \leq \left(\frac{1}{4N_0}\right)^{-r_e} \left(\prod_{l=0}^{r_e-1} \alpha_L \lambda_{e,l}\right)^{-1}. \tag{8}$$

As in [32], we call r_e the *diversity order*, denoted as $G_{d,e}$, and $\left(\prod_{l=0}^{r_e-1} \alpha_L \lambda_{e,l}\right)^{1/r_e}$ the *coding advantage*, denoted as $G_{c,e}$, for the symbol error vector $\boldsymbol{e}$. The diversity order $G_{d,e}$ determines the slope of the averaged (with respect to (w.r.t.) the random channel) PEP (between $\boldsymbol{s}$ and $\boldsymbol{s}'$) as a function of the SNR at high SNR ($N_0 \to 0$). Correspondingly, $G_{c,e}$ determines the shift of this PEP curve in the SNR relative to a benchmark error rate curve of $(1/4N_0)^{-r_e}$. When $r_e = L+1$, $\boldsymbol{A}_e$ is full rank, the product of eigenvalues becomes the determinant of $\boldsymbol{A}_e$, and therefore the coding gain is given by $\alpha_L[\det(\boldsymbol{A}_e)]^{1/(L+1)}$.

Since both $G_{d,e}$ and $G_{d,c}$ depend on the choice of $\boldsymbol{e}$, we define the *diversity order and coding gain for our CFC-OFDM system*, respectively, as

$$G_d := \min_{e \in \mathcal{S}_e} G_{d,e} = \min_{e \in \mathcal{S}_e} \mathrm{rank}(\boldsymbol{A}_e) \quad \text{and} \quad G_c := \min_{e \in \mathcal{S}_e} G_{c,e}. \tag{9}$$

In this paper, we use diversity order to mean the asymptotic slope of the error probability versus SNR curve in a log-log scale. In the literature, "diversity" sometimes means "*channel diversity*"—roughly the number of degrees of freedom provided by a given channel. To attain a certain diversity order (slope) on the error probability versus SNR curve, three conditions should be satisfied. i) The transmitter is well designed so that the information symbols are encoded with sufficient redundancy (enough *diversification*). ii) The channel is capable of providing enough degrees of freedom. iii) The receiver is well designed so as to sufficiently exploit the redundancy introduced at the transmitter.

B. Encoder Design

Since the diversity order G_d determines how fast the symbol error probability drops as SNR increases, G_d is to be optimized first. We have the following result.

Theorem 1 (Maximum Achievable Diversity Order): For a transmitted codeword set $\mathcal{U}$ with minimum Hamming distance $\delta_{\min}$, over i.i.d. FIR Rayleigh-fading channels of order L, the diversity order is $\min(\delta_{\min}, L+1)$. Thus, the maximum achievable diversity order (MADO) of CFC-OFDM transmissions is $L+1$, and in order to achieve MADO we need $\delta_{\min} \geq L+1$.

Proof: Since the matrix $\boldsymbol{A}_e = \boldsymbol{V}^{\mathcal{H}} \boldsymbol{D}_e^{\mathcal{H}} \boldsymbol{D}_e \boldsymbol{V}$ in (6) is the Gram matrix[1] of $\boldsymbol{D}_e \boldsymbol{V}$, the rank r_e of $\boldsymbol{A}_e$ is the same as the rank of $\boldsymbol{D}_e \boldsymbol{V}$, which is $\min(\delta(\boldsymbol{u}, \boldsymbol{u}'), L+1) \leq L+1$. Therefore, the diversity order of the system is

$$\begin{aligned} G_d &= \min_{\boldsymbol{e} \in \mathcal{S}_e} \mathrm{rank}(\boldsymbol{A}_e) = \min_{\boldsymbol{e} \in \mathcal{S}_e} \min[\delta(\boldsymbol{u}, \boldsymbol{u}'), L+1] \\ &= \min(\delta_{\min}, L+1) \leq L+1 \end{aligned}$$

and the equality is achieved when $\delta_{\min} \geq L+1$. □

Theorem 1 is intuitively reasonable because the FIR Rayleigh-fading channel offers us $L+1$ independent fading taps, which is the maximum possible number of independent replicas of the transmitted signal in the serial transmission mode. In order to achieve the MADO, any two codewords in $\mathcal{U}$ should be different by no less than $L+1$ entries.

For uncoded OFDM, we have $\delta_{\min} = 1$, which verifies the well-known fact that *uncoded OFDM has diversity order one*. Although the underlying channel provides $L+1$ degrees of freedom, uncoded OFDM is unable to harvest this "channel diversity" because of poor transmitter design (recall our remarks at the end of Section III-A).

[1]The Gram matrix of $\boldsymbol{X}$ is the matrix $\boldsymbol{X}^{\mathcal{H}}\boldsymbol{X}$ with $\mathrm{rank}(\boldsymbol{X}^{\mathcal{H}}\boldsymbol{X}) = \mathrm{rank}(\boldsymbol{X})$.

Theorem 1 has also implications to GF-coded/interleaved OFDM systems, when channel coding or interleaving is applied only within a single OFDM symbol and not across successive OFDM symbols. The diversity is again equal to $\min(\delta_{\min}, L+1)$. To see this, it suffices to view $\mathcal{U}$ as the codeword set of GF-coded blocks.

To enable MADO, we need $\boldsymbol{A}_e$ to be full rank and thus positive definite for any $\boldsymbol{e} \in \mathcal{S}_e$. This is true if and only if $\boldsymbol{h}^{\mathcal{H}}\boldsymbol{A}_e\boldsymbol{h} > 0$ for any $\boldsymbol{h} \neq \boldsymbol{0} \in \mathbb{C}^{L+1}$. Equation (6) shows that this is equivalent to $d^2(\boldsymbol{y}, \boldsymbol{y}') = ||\boldsymbol{D}_H\boldsymbol{\Theta}\boldsymbol{e}||^2 \neq 0, \forall\, \boldsymbol{e} \in \mathcal{S}_e$, and $\forall\, \boldsymbol{h} \neq \boldsymbol{0}$. The latter means that any two different transmitted vectors should result in different received vectors in the absence of noise, irrespective of the channel; in such cases, we call the symbols *detectable* or recoverable. The conditions for achieving MADO and channel-irrespective symbol detectability are summarized in the following theorem.

Theorem 2 (Symbol Detectability $\Leftrightarrow$ MADO): Under the channel conditions of Theorem 1, the maximum diversity order is achieved if and only if symbol detectability is achieved; i.e., $||\boldsymbol{D}_H\boldsymbol{\Theta}\boldsymbol{e}||^2 \neq 0, \forall\, \boldsymbol{e} \in \mathcal{S}_e$ and $\forall\, \boldsymbol{h} \neq \boldsymbol{0}$.

The result in Theorem 2 is somewhat surprising: it asserts the equivalence of a deterministic property of the code, namely, symbol detectability in the absence of noise, with a statistical property, the diversity order. It can be explained though, by realizing that in random channels, the performance is mostly affected by the worst channels, despite their small realization probability. By guaranteeing detectability for any, and therefore the worst channels, we are essentially improving the ensemble performance.

The relation between diversity and symbol detectability was also hinted in [39, Sec. IV] for periodic erasure channels, where the diversity (or periodic effective code length) is defined as the number of erasures it takes to render the minimum distance equal to zero, thus preventing detectability.

The symbol detectability condition in Theorem 2 should be checked against all pairs $\boldsymbol{s}$ and $\boldsymbol{s}'$, which is usually not an easy task, especially when the underlying constellations are large and/or when the size K of $\boldsymbol{s}$ is large. But it is possible to identify sufficient conditions on $\boldsymbol{\Theta}$ that guarantee symbol detectability and that are relatively easy to check. One such condition is provided by the following theorem.

Theorem 3 (Sufficient Condition for MADO): For i.i.d. FIR Rayleigh-fading channels of order L, MADO is achieved when $\mathrm{rank}(\boldsymbol{D}_H\boldsymbol{\Theta}) = K, \forall\, \boldsymbol{h} \neq \boldsymbol{0}$, which is equivalent to the following condition: Any $N-L$ rows of $\boldsymbol{\Theta}$ span the $\mathbb{C}^{1\times K}$ space. The latter in turn requires that $N - L \geq K$.

Proof: First, since $\boldsymbol{\Theta}$ is of size $N \times K$, it cannot have rank greater than K. If MADO is not achieved, there exists at least one channel $\boldsymbol{h}$ and one $\boldsymbol{e} \in \mathcal{S}_e$ such that $\boldsymbol{D}_H\boldsymbol{\Theta}\boldsymbol{e} = \boldsymbol{0}$ by Theorem 2, which means that $\mathrm{rank}(\boldsymbol{D}_H\boldsymbol{\Theta}) < K$. So, MADO is achieved when $\mathrm{rank}(\boldsymbol{D}_H\boldsymbol{\Theta}) = K$. Second, since the diagonal entries of $\boldsymbol{D}_H$ represent frequency response samples of the channel $\boldsymbol{h}$ evaluated at the FFT frequencies, there can be at most L zeros on the diagonal of $\boldsymbol{D}_H$. To have $\mathrm{rank}(\boldsymbol{D}_H\boldsymbol{\Theta}) = K, \forall\, \boldsymbol{h}$, it suffices to have any $N-L$ rows of $\boldsymbol{\Theta}$ span the $\mathbb{C}^{1\times K}$ space. On the other hand, when there is a set of $N-L$ rows of $\boldsymbol{\Theta}$ that are linearly dependent, we can find a channel that has zeros at frequencies corresponding to the remaining L rows. Such a channel will make $\mathrm{rank}(\boldsymbol{D}_H\boldsymbol{\Theta}) < K$. This completes the proof. □

To satisfy Theorem 3 and maintain high rate $r = K/N$, we should have i) $K = N - L$ and ii) any K rows of $\boldsymbol{\Theta}$ be linearly independent. Another equivalent way of saying ii) is: the row k-rank[2] of $\boldsymbol{\Theta}$ is K.

Notice that we had recognized the importance of conditions given in Theorem 3 earlier in, e.g., [36], for channel-irrespective symbol recovery. Based on the equivalence established in Theorem 2, it should not be surprising that they appear here again. Also, if we want to guarantee MADO for *any* possible constellation, i.e., if we allow the entries of $\boldsymbol{s}$ to take any value in $\mathbb{C}$ or $\mathbb{R}$, then the sufficient conditions in Theorem 3 also become necessary.

The natural question that arises at this point is whether there exist CFC matrices $\boldsymbol{\Theta}$ that satisfy the conditions of Theorem 3. The following theorem constructively develops two classes of encoders that satisfy Theorem 3, and thus enable MADO.

Theorem 4 (MADO-Enabling Encoders):

i) *Vandermonde Encoders*: Choose N points $\rho_n \in \mathbb{C}, n = 0, 1, \ldots, N-1$, such that $\rho_m \neq \rho_n, \forall\, m \neq n$. Let

$$\boldsymbol{\rho} := [\rho_0, \rho_1, \ldots, \rho_{N-1}]^T.$$

Then the Vandermonde encoder $\boldsymbol{\Theta}(\boldsymbol{\rho}) \in \mathbb{C}^{N\times K}$ defined by $[\boldsymbol{\Theta}(\boldsymbol{\rho})]_{n,k} = \rho_n^k$ satisfies Theorem 3, and thus achieves MADO.

ii) *Cosine Encoders*: Choose N points $\phi_0, \phi_1, \ldots, \phi_{N-1} \in \mathbb{R}$, such that $\phi_m \neq (2k+1)\pi$ and $\phi_m \pm \phi_n \neq 2k\pi$, $\forall\, m \neq n, \forall\, k \in \mathbb{Z}$. Let $\boldsymbol{\phi} := [\phi_0, \phi_1, \ldots, \phi_{N-1}]^T$. Then the real cosine encoder $\boldsymbol{\Theta}(\boldsymbol{\phi}) \in \mathbb{R}^{N\times K}$ defined by

$$[\boldsymbol{\Theta}(\boldsymbol{\phi})]_{n,k} = \cos\left(k + \frac{1}{2}\right)\phi_n$$

satisfies Theorem 3 and thus achieves MADO.

Proof: We first prove that Vandermonde encoders in i) satisfy the conditions of Theorem 3. Any K rows of the matrix $\boldsymbol{\Theta}(\boldsymbol{\rho})$ form a square Vandermonde matrix with distinct rows. Such a Vandermonde matrix is known to have a determinant different from 0. Therefore, any K rows of $\boldsymbol{\Theta}(\boldsymbol{\rho})$ are linearly independent, which satisfies the conditions in Theorem 3.

To prove Part ii) of the theorem, we need to show that any K rows of $\boldsymbol{\Theta}(\boldsymbol{\phi})$ form a nonsingular square matrix. Without loss of generality, we consider the matrix formed by the first K rows (see the top of the following page).

Let us now evaluate the determinant $\det(\boldsymbol{\Theta}_1)$. Define $z_n := \cos(\frac{1}{2}\phi_n)$. Using Chebyshev polynomials of the first kind

$$T_l(x) := \cos(l\cos^{-1}x) = \sum_{i=0}^{\lfloor l/2\rfloor}\binom{l}{2i}x^{l-2i}(x^2-1)^i$$

[2]A matrix is said to have row k-rank r if *any* of its r rows are linearly independent, but there exist one set of $r+1$ rows that are linearly dependent. k-rank stands for Kruskal-rank and has been widely used in multiway data array decomposition problems (see, e.g., [29]).

$$\boldsymbol{\Theta}_1 := \begin{bmatrix} \cos\left(\frac{1}{2}\phi_0\right) & \cos\left(\frac{3}{2}\phi_0\right) & \dots & \cos\left(\frac{2K-1}{2}\phi_0\right) \\ \cos\left(\frac{1}{2}\phi_1\right) & \cos\left(\frac{3}{2}\phi_1\right) & \dots & \cos\left(\frac{2K-1}{2}\phi_1\right) \\ \vdots & \vdots & \vdots & \vdots \\ \cos\left(\frac{1}{2}\phi_{K-1}\right) & \cos\left(\frac{3}{2}\phi_{K-1}\right) & \dots & \cos\left(\frac{2K-1}{2}\phi_{K-1}\right) \end{bmatrix}.$$

each entry $\cos(\frac{2m+1}{2}\phi_n)$ of $\boldsymbol{\Theta}_1$ is a polynomial $T_{2m+1}(z_n)$ of order $2m+1$ of some $z_n = \cos(\frac{1}{2}\phi_n)$. The determinant $\det(\boldsymbol{\Theta}_1)$ is, therefore, a polynomial in $z_0, \dots, z_{K-1}$ of order $\sum_{n=1}^{K}(2n-1) = K^2$. It is easy to see that when $z_n = 0$, or when $z_m = \pm z_n$, $m \neq n$, $\boldsymbol{\Theta}_1$ has an all-zero row, or, two rows that are either the same or the negative of each other. Therefore, z_n, $z_m - z_n$, and $z_m + z_n$ are all factors of $\det(\boldsymbol{\Theta}_1)$. Hence,

$$g(z_0, z_1, \dots, z_{K-1}) := \prod_n z_n \prod_{m>n} (z_m^2 - z_n^2)$$

is also a factor of $\det(\boldsymbol{\Theta}_1)$. But $g(z_0, z_1, \dots, z_{K-1})$ is of order $K + K(K-1) = K^2$, which means that it is different from $\det(\boldsymbol{\Theta}_1)$ by at most a constant. Using the leading coefficient[3] 2^{l-1} of $T_l(x)$, we obtain the constant as

$$\prod_{n=1}^{K} 2^{(2n-1)-1} = 2^{K(K-1)}$$

that is,

$$\det(\boldsymbol{\Theta}_1) = 2^{K(K-1)} g(z_0, z_1, \dots, z_{K-1}).$$

Since $\phi_m \neq (2k+1)\pi$ and $\phi_m \pm \phi_n \neq 2k\pi$, $\forall\, m \neq n$, $\forall\, k \in \mathbb{Z}$, none of z_n, $z_m - z_n$, and $z_m + z_n$ can be zero. Therefore, $\det(\boldsymbol{\Theta}_1) \neq 0$ and $\boldsymbol{\Theta}_1$ is nonsingular. A similar argument can be applied to any K rows of the matrix $\boldsymbol{\Theta}$, and the proof is complete. □

Special cases of the Vandermonde construction in Theorem 4 include selecting $\rho_n = \exp(-j2\pi n/N)$, which will result in a generating matrix that is a truncated FFT matrix as in the ZP-only transmission case of Section II-C3. This provides a theoretical justification for the robustness of ZP-only transmissions observed earlier in [22], [31], [36]. A special case of the general cosine encoder in ii) is a truncated discrete cosine transform (DCT) matrix defined by choosing $\phi_n = n\pi/N$.

Notice that up to now we have been assuming that the channel consists of i.i.d. zero-mean complex Gaussian taps. Such a model is well suited for benchmarking average system performance in wireless fading channels, but is rather idealistic since the taps may be correlated. For correlated channels, we have the following result.

Theorem 5 (MADO of Correlated Rayleigh Channels): Let the channel $\boldsymbol{h}$ be zero-mean complex Gaussian with correlation matrix $\boldsymbol{R}_h$. The maximum achievable diversity order equals the rank of $\boldsymbol{R}_h$, which is achieved by any encoder that enables MADO with i.i.d. Rayleigh channels. If $\boldsymbol{R}_h$ is full rank and MADO is achieved, then the coding gain is different from the coding gain in the i.i.d. case only by a constant $\det^{\frac{1}{L+1}}(\boldsymbol{R}_h)/\alpha_L$.

Proof: Let $r_h := \operatorname{rank}(\boldsymbol{R}_h)$, and the eigenvalue decomposition of $\boldsymbol{R}_h$ be

$$\boldsymbol{R}_h = [\boldsymbol{U}_1 \quad \boldsymbol{U}_2] \begin{bmatrix} \boldsymbol{\Lambda}_1 & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{\Lambda}_2 \end{bmatrix} \begin{bmatrix} \boldsymbol{U}_1^{\mathcal{H}} \\ \boldsymbol{U}_2^{\mathcal{H}} \end{bmatrix} \tag{10}$$

where $\boldsymbol{U}_1$ is $(L+1) \times r_h$, $\boldsymbol{U}_2$ is $(L+1) \times (L+1-r_h)$, $\boldsymbol{\Lambda}_1$ is $r_h \times r_h$ full-rank diagonal, and $\boldsymbol{\Lambda}_2$ is an $(L+1-r_h) \times (L+1-r_h)$ all-zero matrix. Define $\tilde{\boldsymbol{h}}_1 := \boldsymbol{\Lambda}_1^{-\frac{1}{2}} \boldsymbol{U}_1^{\mathcal{H}} \boldsymbol{h}$, $\tilde{\boldsymbol{h}}_2 := \boldsymbol{U}_2^{\mathcal{H}} \boldsymbol{h}$, and

$$\tilde{\boldsymbol{h}} := \begin{bmatrix} \tilde{\boldsymbol{h}}_1^T & \tilde{\boldsymbol{h}}_2^T \end{bmatrix}^T$$

where $\boldsymbol{\Lambda}_1^{-\frac{1}{2}}$ is defined by $\boldsymbol{\Lambda}_1^{-\frac{1}{2}} \boldsymbol{\Lambda}_1^{-\frac{1}{2}} = \boldsymbol{\Lambda}_1^{-1}$. Since $\tilde{\boldsymbol{h}}_2$ has an autocorrelation matrix $\boldsymbol{R}_{\tilde{h}_2} = \boldsymbol{U}_2^{\mathcal{H}} \boldsymbol{R}_h \boldsymbol{U}_2 = \boldsymbol{\Lambda}_2$, all the entries of $\tilde{\boldsymbol{h}}_2$ are zero almost surely. We can, therefore, write

$$\boldsymbol{h} = \begin{bmatrix} \boldsymbol{U}_1 \boldsymbol{\Lambda}_1^{\frac{1}{2}} & \boldsymbol{U}_2 \end{bmatrix} \tilde{\boldsymbol{h}} = \boldsymbol{U}_1 \boldsymbol{\Lambda}_1^{\frac{1}{2}} \tilde{\boldsymbol{h}}_1. \tag{11}$$

Since

$$\boldsymbol{R}_{\tilde{h}_1} = \boldsymbol{\Lambda}_1^{-\frac{1}{2}} \boldsymbol{U}_1^{\mathcal{H}} \boldsymbol{R}_h \boldsymbol{U}_1 \boldsymbol{\Lambda}_1^{-\frac{1}{2}} = \boldsymbol{I}_{r_h}$$

the entries of $\tilde{\boldsymbol{h}}_1$, which are jointly Gaussian, are i.i.d..

Substituting (11) in (6), we obtain

$$d^2(\boldsymbol{y}, \boldsymbol{y}') = \boldsymbol{h}^{\mathcal{H}} \boldsymbol{A}_e \boldsymbol{h} = \tilde{\boldsymbol{h}}_1^{\mathcal{H}} \boldsymbol{\Lambda}_1^{\frac{1}{2}} \boldsymbol{U}_1^{\mathcal{H}} \boldsymbol{A}_e \boldsymbol{U}_1 \boldsymbol{\Lambda}_1^{\frac{1}{2}} \tilde{\boldsymbol{h}}_1 := \tilde{\boldsymbol{h}}_1^{\mathcal{H}} \tilde{\boldsymbol{A}}_e \tilde{\boldsymbol{h}}_1$$

where $\tilde{\boldsymbol{A}}_e = \boldsymbol{\Lambda}_1^{\frac{1}{2}} \boldsymbol{U}_1^{\mathcal{H}} \boldsymbol{A}_e \boldsymbol{U}_1 \boldsymbol{\Lambda}_1^{\frac{1}{2}}$ is an $r_h \times r_h$ matrix.

Following the same derivation as in (6)– (9), with $\boldsymbol{A}_e$ replaced by $\tilde{\boldsymbol{A}}_e$ and $\boldsymbol{h}$ replaced by $\tilde{\boldsymbol{h}}_1$, we can obtain the diversity order and coding gain for the error event $\boldsymbol{e}$ as

$$G_{d,e} = \operatorname{rank}(\tilde{\boldsymbol{A}}_e) := \tilde{r}_e \leq r_h \quad \text{and} \quad G_{c,e} = \left(\prod_{l=0}^{\tilde{r}_e - 1} \tilde{\lambda}_{e,l} \right)^{1/\tilde{r}_e} \tag{12}$$

where $\tilde{\lambda}_{e,l}$, $l = 1, \dots, r_h$, are the eigenvalues of $\tilde{\boldsymbol{A}}_e$.

When $\boldsymbol{\Theta}$ is designed such that MADO is achieved with i.i.d. channels, $\boldsymbol{A}_e$ is full rank for any $\boldsymbol{e} \in \mathcal{S}_e$. Then $\boldsymbol{A}_e$ is positive definite Hermitian symmetric, which means that there exists an $(L+1) \times (L+1)$ matrix $\boldsymbol{B}_e$ such that $\boldsymbol{A}_e = \boldsymbol{B}_e^{\mathcal{H}} \boldsymbol{B}_e$. It follows that $\tilde{\boldsymbol{A}}_e = \boldsymbol{\Lambda}_1^{\frac{1}{2}} \boldsymbol{U}_1^{\mathcal{H}} \boldsymbol{B}_e^{\mathcal{H}} \boldsymbol{B}_e \boldsymbol{U}_1 \boldsymbol{\Lambda}_1^{\frac{1}{2}}$ is the Gram matrix of $\boldsymbol{B}_e \boldsymbol{U}_1 \boldsymbol{\Lambda}_1^{\frac{1}{2}}$, and, thus, $\tilde{\boldsymbol{A}}_e$ has rank equal to

$$\operatorname{rank}\left(\boldsymbol{B}_e \boldsymbol{U}_1 \boldsymbol{\Lambda}_1^{\frac{1}{2}} \right) = \operatorname{rank}(\boldsymbol{U}_1 \boldsymbol{\Lambda}_1^{\frac{1}{2}}) = r_h$$

the MADO for this correlated channel.

When the MADO r_h is achieved, the coding gain in (12) for $\boldsymbol{e}$ becomes $G_{c,e} = \det(\tilde{\boldsymbol{A}}_e)^{1/r_h}$. If in addition $\boldsymbol{R}_h$ has full rank $r_h = L+1$, then

$$\det(\tilde{\boldsymbol{A}}_e)^{1/r_h} = \det(\boldsymbol{A}_e)^{1/(L+1)} \det(\boldsymbol{R}_h)^{1/(L+1)}$$

[3]This can be seen by taking the limit

$$\lim_{\cos\phi \to \infty} \cos(l\phi) / \cos^l(\phi) = \lim_{j\phi \to \infty} 2^{l-1} \frac{e^{jl\phi} + e^{-jl\phi}}{(e^{j\phi} + e^{-j\phi})^l} = 2^{l-1}.$$

which means that for full-rank channel correlation matrices, the full-diversity coding gain is different from the coding gain in the i.i.d. case, only by a constant $\det(\boldsymbol{R}_h)^{1/(L+1)}/\alpha_L$. □

Theorem 5 asserts that the $\mathrm{rank}(\boldsymbol{R}_h)$ is the MADO for CFC-OFDM systems as well as for GF coded OFDM systems that do not code or interleave across OFDM symbols. Also, MADO-enabling transmissions, designed for i.i.d. channels, can also enable the MADO for correlated channels.

In addition to the diversity order, coding gain G_c is another parameter that needs to be optimized among the MADO-enabling encoders (cf. (8)). Since for MADO-enabling encoders, the coding gain is given by

$$G_c = \min_{\boldsymbol{e}\neq\boldsymbol{0}} G_{c,e} = \alpha_L \min_{\boldsymbol{e}\neq\boldsymbol{0}} \det(\boldsymbol{A}_e)^{1/r_e}$$

we need to maximize the minimum determinant of $\boldsymbol{A}_e$ over all possible error vectors $\boldsymbol{e}$ among the MADO-enabling encoders. The following theorem asserts that the ZP-only transmission is one of the coding gain maximizers. For the proof, we refer the reader to [37].

Theorem 6 [37] (ZP-Only: Maximum Coding Gain): Suppose the entries of $\boldsymbol{s}(i)$ are drawn independently from a finite constellation $\mathcal{A}$ with minimum distance $d_{\min}(\mathcal{A})$. Then the maximum coding advantage (cf. (8)) of a CFC-OFDM for i.i.d. Rayleigh-fading channels under **AS1)** is $G_{c,\max} = \alpha_L d^2_{\min}(\mathcal{A})$. The maximum coding advantage is achieved by ZP-only transmissions with any K.

Besides the diversity order and coding gain that affect average error probability, other pertinent criteria such as minimum mean-square error (MMSE) or maximum information rate might also be optimized. These will not be treated here due to space limitations. Some related aspects are treated in [23] for redundant encoders and in [42] for "nonredundant" (rate 1 symbol per dimension) encoders.

IV. Links With GF Codes

In order to achieve high rate, we have adopted $K = N - L$, and found two classes of encoders that enable MADO in Theorem 4. The Vandermonde encoders are reminiscent of the parity-check matrix of BCH codes, RS codes, and Goppa codes [11]. It turns out that the MADO-enabling encoders and these codes are closely related.

Let us now take $\mathcal{S} = \mathbb{C}^{K\times 1}$. We call the codeword set $\mathcal{U}$ that is generated by $\boldsymbol{\Theta}$ of size $N \times K$ *maximum-distance separable* (MDS) if $\delta_{\min}(\mathcal{U}) = N - K + 1$. The fact that $N - K + 1$ is the maximum possible minimum Hamming distance of $\mathcal{U}$ is due to the Singleton bound [30]. Although the Singleton bound was originally proposed and mostly known for GF codes, its proof can be easily generalized to the real/complex field as well; see also [16, Theorem 1]. In our case, it asserts that $\delta_{\min} \leq N - K + 1$ when $\mathcal{S} = \mathbb{C}^{K\times 1}$.

Notice that the assumption $\mathcal{S} = \mathbb{C}^{K\times 1}$ is not often applicable in communication systems, because the entries of $\boldsymbol{s}$ are usually chosen from a finite-alphabet set, e.g., quadrature phase-shift keying (QPSK) or quadrature amplitude modulation (QAM). But such an assumption greatly simplifies the system design task: once we can guarantee $\delta_{\min} = N-K+1$ for $\mathcal{S} = \mathbb{C}^{K\times 1}$, we can choose any constellation based on other considerations, without worrying about the diversity performance. However, for a finite constellation, i.e., when $\mathcal{S}$ has finite cardinality, the result on $\delta_{\min}$ can be improved. In fact, it can be shown that even with a square unitary $K \times K$ matrix $\boldsymbol{\Theta}$, it is possible to have $\delta_{\min} = K$. The proof can be found in [42] for a multiantenna space–time diversity setup. The rate in that case is one symbol per dimension, because $K = N$ symbols can be transmitted with a length-N block. Adding $N - K = L$ redundant symbols in the transmission instead of using a square unitary encoder as in [42] offers constellation-irrespective diversity assurance, and possibly a higher coding gain for finite constellations.

To satisfy the condition in Theorem 2 with the highest rate for a given N, we need $K = N - L$ and $\delta_{\min} = L + 1 = N-K+1$. In other words, *to achieve constellation-irrespective full diversity with highest rate, we need the code to be MDS.* According to our Theorem 4, such MDS encoders always exist for any N and $K < N$.

In a GF, there also exist MDS codes; see [20, Ch. 11] for a fairly comprehensive treatment. Examples of GF MDS codes written in the form of $(N, K, \delta_{\min})$ include the following.

i) For any field: $(N, 1, N)$ (no coding), $(N, N - 1, 2)$ (single parity-check coding), and $(N, N, 1)$ (repetition coding). These are called *trivial MDS codes*.

ii) For $\mathbb{F}(q)$, q being a power of a prime: (generalized) RS coding $(q-1, K, q-K)$, extended RS coding $(q, K, q-K+1)$, and doubly extended RS coding $(q+1, K, q-K+2)$. It is shown in [28] that $(q+1, K, q-K+2)$ codes with $2 \leq K \leq \lfloor q/2 \rfloor + 1$ ($K \neq 3$ if q is even) do not have further MDS extensions.

iii) Some sporadic MDS codes, e.g., the $(6, 3, 4)$ algebraic-geometry code constructed using an elliptic curve [33, p. 32].

When $\delta_{\min}$ falls short of the Singleton bound by 1, the corresponding code is often called a quasi- or almost-MDS code, and most of the algebraic-geometry codes derived from elliptic curves belong to this category [2].

When a GF MDS code exists, we may use it to replace our CF linear code, and achieve the same (maximum) diversity order at the same rate. But such GF codes *do not always exist* for a given field and N, K. For $\mathbb{F}_2$, only trivial MDS codes exist [20]. This means that it is impossible to construct, for example, binary (and thus simply decodeable) MDS codes that have $\delta_{\min} \geq 2$, except for the repetition code. Another restriction of the GF MDS code is on the input and output alphabet. Although RS codes are the least restrictive among them in terms of the number of elements in the field, they are *constrained on the code length and the alphabet size*. Our encoders $\boldsymbol{\Theta}$, on the other hand, operate over the complex field with no restriction on the input symbol alphabet or the coded symbol alphabet. The fact that coded symbols do not necessarily belong to a given constellation should not be viewed as undesirable in OFDM, simply because the IFFT will be applied to yield a transmitted signal with values over the complex field, anyway.

From known results on GF MDS codes, we can obtain analogous results on our complex field MDS codes needed for enabling MADO. We list them below as theorems (their proofs follow easily from [20, Ch. 11]).

Theorem 7 (Dual MDS Code): For an MDS code generated by $\boldsymbol{\Theta} \in \mathbb{C}^{N\times K}$, the code generated by the matrix $\boldsymbol{\Theta}_\perp$ is also MDS, where $\boldsymbol{\Theta}_\perp$ is an $N\times(N-K)$ matrix such that $\boldsymbol{\Theta}_\perp^T\boldsymbol{\Theta} = \mathbf{0}$.

A generator $\boldsymbol{\Theta}$ for an MDS code is called *systematic* if it is in the form $[\boldsymbol{I}_K, \boldsymbol{P}]^T$ where $\boldsymbol{P}$ is a $K \times (N-K)$ matrix.

Theorem 8 (Systematic MDS Code): A code generated by $[\boldsymbol{I}, \boldsymbol{P}]^T$ is MDS if and only if every square submatrix of $\boldsymbol{P}$ is nonsingular.

To construct systematic MDS codes using Theorem 8, the following two results can be useful [20, p. 323].

i) Every square submatrix of a Vandermonde matrix with real, positive entries is nonsingular.

ii) A $K\times(N-K)$ matrix $\boldsymbol{P}$ is called a *Cauchy matrix* if its (i,j)th element $[\boldsymbol{P}]_{ij} = 1/(x_i + y_j)$ for some elements $x_1, x_2, \ldots, x_K$, $y_1, y_2, \ldots, y_{N-K}$, such that the x_i's are distinct, the y_j's are distinct, and $x_i + y_j \neq 0$ for all i, j. Any square submatrix of a Cauchy matrix is nonsingular. The relation between Cauchy- and Vandermonde-based constructions is dealt with in [24].

V. Decoding Schemes

In this section, we discuss decoding options for CFC. For this purpose, we restrict our attention to the case that $\mathcal{S}$ is a finite set, e.g., a finite constellation carved from (possibly scaled and shifted) $\mathbb{Z}^K$. This includes BPSK, QPSK, and QAM as special cases. Since the task of the receiver involves both channel equalization and decoding of the CFC, we will consider the combined task jointly, and will use the words decoding, detection, and equalization interchangeably.

A. ML Detection

To collect the MADO, CFC-OFDM requires ML decoding. For the input–output relationship in (1) and under the AWGN assumption, the minimum Euclidean distance detection rule becomes ML and can be formulated as follows:

$$\hat{\boldsymbol{s}} = \underset{\boldsymbol{s}\in\mathcal{S}}{\operatorname{argmin}} \|\boldsymbol{x} - \boldsymbol{D}_H\boldsymbol{\Theta}\boldsymbol{s}\|. \tag{13}$$

ML decoding of CFC transmissions belongs to a general class of lattice decoding problems, as the matrix product $\boldsymbol{D}_H\boldsymbol{\Theta}$ in (1) gives rise to a discrete subgroup (lattice) of the $\mathbb{C}^N$ space under the vector addition operation. In its most general form, finding the optimum estimate in (13) requires searching over $|\mathcal{S}|$ vectors. For large block sizes and/or large constellations, it is practically prohibitive to perform exhaustive search since the complexity depends exponentially on the number of symbols in the block.

A relatively less complex ML search is possible with the sphere decoding (SD) algorithm (cf. Fig. 5), which only searches coded vectors that are within a sphere centered at the received block $\boldsymbol{x}$ (cf. (1)) [35]. Denote the QR decomposition of $\boldsymbol{D}_H\boldsymbol{\Theta}$ as $\boldsymbol{D}_H\boldsymbol{\Theta} = \boldsymbol{Q}\boldsymbol{R}$, where $\boldsymbol{Q}$ has size $N \times K$ and satisfies $\boldsymbol{Q}^{\mathcal{H}}\boldsymbol{Q} = \boldsymbol{I}_{K\times K}$, and $\boldsymbol{R}$ is an upper triangular $K \times K$ matrix. The problem in (13) then becomes equivalent to the following problem:

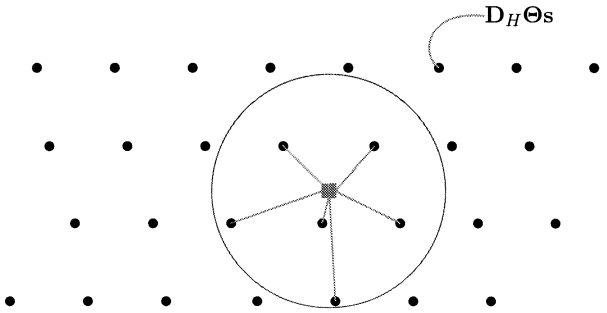

Fig. 5. Illustration of SD; the filled square represents the noise-corrupted received codeword.

$$\hat{\boldsymbol{s}} = \underset{\boldsymbol{s}\in\mathcal{S}}{\operatorname{argmin}} \left\|\boldsymbol{Q}^{\mathcal{H}}\boldsymbol{x} - \boldsymbol{R}\boldsymbol{s}\right\|. \tag{14}$$

SD starts its search by looking only at vectors $\boldsymbol{s}$ such that

$$\left\|\boldsymbol{Q}^{\mathcal{H}}\boldsymbol{x} - \boldsymbol{R}\boldsymbol{s}\right\| < C \tag{15}$$

where C is the search radius, a decoding parameter. Since $\boldsymbol{R}$ is upper triangular, in order to satisfy the inequality in (15), the last entry of $\boldsymbol{s}$ must satisfy $|[\boldsymbol{R}]_{K,K}[\boldsymbol{s}]_K| < C$, which reduces the search space, if C is small. For each value of the last entry, possible candidates of the last-but-one entry are found, and one candidate is taken. The process continues until a vector $\boldsymbol{s}_0$ is found that satisfies (15). Then the search radius C is set equal to $\left\|\boldsymbol{Q}^{\mathcal{H}}\boldsymbol{x} - \boldsymbol{R}\boldsymbol{s}_0\right\|$, and a new search round is initiated. If no other vector is found inside the radius, then $\boldsymbol{s}_0$ is the ML solution. Otherwise, if $\boldsymbol{s}_1$ is found inside the sphere, the search radius is again reduced to $\left\|\boldsymbol{Q}^{\mathcal{H}}\boldsymbol{x} - \boldsymbol{R}\boldsymbol{s}_1\right\|$, and so on. If no $\boldsymbol{s}_0$ is ever found inside the initial sphere of radius C, then C is too small. In this case, either a decoding failure is declared or C is increased.

The complexity of the SD is polynomial in K (e.g., $\mathcal{O}(K^6)$) [8], which is better than exponential but still too high for practical purposes. Indeed, it is not suitable for codes of block size greater than, say, 16. When the block size is small, the SD can be considered as an option to achieve near-ML performance at manageable complexity.

In the special case of ZP-only transmissions, the received vector is given by $\tilde{\boldsymbol{x}} = \boldsymbol{H}\boldsymbol{s} + \tilde{\boldsymbol{\eta}}$ (cf. Section II). Thanks to the ZP, the full linear (as opposed to cyclic) convolution of the transmitted block $\boldsymbol{s}$ with the FIR channel is preserved, and the channel is represented as the banded Toeplitz matrix $\boldsymbol{H}$. In such a case, Viterbi decoding can be used at a complexity of $\mathcal{O}(Q^L)$ per symbol, where Q is the constellation size of the symbols in $\boldsymbol{s}$ [9].

B. Low-Complexity Linear Detection

Zero-forcing (ZF) and MMSE detectors (equalizers) offer low-complexity alternatives. The block ZF and MMSE equal-

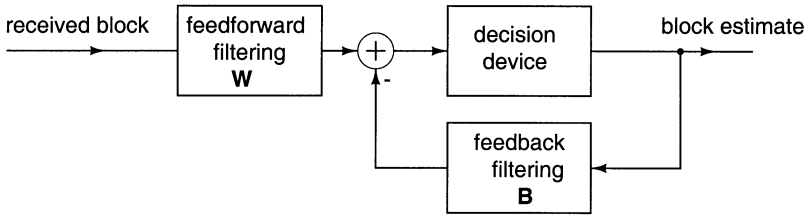

Fig. 6. Block DFE structure.

izers based on the input–output relationship (1) can be written as, respectively (see, e.g., [27])

$$\boldsymbol{G}^{zf} = (\boldsymbol{D}_H \boldsymbol{\Theta})^{\dagger}$$

and

$$\boldsymbol{G}^{mmse} = \boldsymbol{R}_s \boldsymbol{\Theta}^{\mathcal{H}} \boldsymbol{D}_H^{\mathcal{H}} \left(\sigma_\eta^2 \boldsymbol{I}_N + \boldsymbol{D}_H \boldsymbol{\Theta} \boldsymbol{R}_s \boldsymbol{\Theta}^{\mathcal{H}} \boldsymbol{D}_H^{\mathcal{H}} \right)^{-1}$$

where $(\cdot)^{\dagger}$ denotes pseudoinverse, σ_η^2 is the variance of entries of noise $\boldsymbol{\eta}$, and $\boldsymbol{R}_s$ is the autocorrelation matrix of $\boldsymbol{s}$. ZF and MMSE equalizers involve $\mathcal{O}(NK)$ operations per K symbols. So per symbol, they require only $\mathcal{O}(N)$ operations. To construct the ZF or MMSE equalizers, inversion of an $N \times N$ matrix is involved, which has complexity $\mathcal{O}(N^3)$. However, the equalizers only need to be recomputed when the channel changes. The performance of ZF and MMSE detectors are, in general, inferior to decision-directed detectors, especially at high SNRs.

C. Decision-Directed Detection

The ML detection schemes of Section V-A in general have high complexity, while the linear detectors in Section V-B have relatively poor performance. The class of decision-directed detectors lie in between these two categories, both in terms of complexity and in terms of performance.

Decision-directed detectors capitalize on the finite alphabet property that is almost always available in practice. In the equalization scenario, they are more commonly known as decision feedback equalizers (DFEs). In a single-user *block* (as opposed to serial) formulation, the DFE has a structure as shown in Fig. 6, where the feed-forward filter is represented as a matrix $\boldsymbol{W}$ and the feedback filter is represented as $\boldsymbol{B}$ [31]. Since we can only feed back decisions in a causal fashion, $\boldsymbol{B}$ is usually chosen to be a strictly upper or lower triangular matrix with zero diagonal entries. Although the feedback loop is represented as a matrix, the operations happen in a serial fashion: the estimated symbols are fed back serially as their decisions are formed one by one. The matrices $\boldsymbol{W}$ and $\boldsymbol{B}$ can be designed according to ZF or MMSE criteria [1], [31]. When $\boldsymbol{B}$ is chosen to be triangular and the mean square error between the block estimate *before* the decision device is minimized, the feed-forward and feedback filtering matrices can be found from the following equations [1], [31]:

$$\boldsymbol{R}_s^{-1} + \boldsymbol{\Theta}^{\mathcal{H}} \boldsymbol{D}_H^{\mathcal{H}} \boldsymbol{R}_\eta^{-1} \boldsymbol{D}_H \boldsymbol{\Theta} = \boldsymbol{U}^{\mathcal{H}} \boldsymbol{\Lambda} \boldsymbol{U} \tag{16}$$

$$\boldsymbol{W} = \boldsymbol{U} \boldsymbol{R}_s \boldsymbol{\Theta}^{\mathcal{H}} \boldsymbol{D}_H^{\mathcal{H}} \left(\boldsymbol{R}_\eta + \boldsymbol{D}_H \boldsymbol{\Theta} \boldsymbol{R}_s \boldsymbol{\Theta}^{\mathcal{H}} \boldsymbol{D}_H^{\mathcal{H}} \right)^{-1} \tag{17}$$

$$\boldsymbol{B} = \boldsymbol{U} - \boldsymbol{I} \tag{18}$$

where the $\boldsymbol{R}_s = E[\boldsymbol{s}\boldsymbol{s}^{\mathcal{H}}]$, $\boldsymbol{R}_\eta = E[\boldsymbol{\eta}\boldsymbol{\eta}^{\mathcal{H}}]$, (16) is obtained using Cholesky decomposition, and $\boldsymbol{U}$ is an upper triangular matrix with unit diagonal entries. Since the feed-forward and feedback filtering entails only matrix–vector multiplications, the complexity of such decision directed schemes is comparable to that of linear detectors. Because decision directed schemes capitalize on the finite-alphabet property of the information symbols, their performance is usually (much) better than linear detectors, especially at moderate to high SNR values, where decision errors are less likely to propagate.

TABLE I
APPROXIMATE DECODING COMPLEXITY FOR $K = 16$, $N = 20$, AND BPSK SYMBOLS

Decoding Scheme	order of Flops/symbol
Exhaustive ML	$> 2^K = 2^{14} = 16,384$
Sphere Decoding	≈ 800 (empirical)
ZF/MMSE	$\approx N = 16$
Decision-Directed	$\approx N = 16$
Viterbi for ZP-only	$2^L = 2^2 = 4$

As an example, we list in Table I the approximate number of flops needed for different decoding schemes when $K = 14$, $L = 2$, $N = 16$, and BPSK modulation is deployed; i.e., $\mathcal{S} = \{\pm 1\}^K$.

D. Iterative Detectors

This is another category with promising decoding performance that also applies to CF decoding. Existing methods include successive interference cancellation with iterative least squares (SIC-ILS) [18], and multistage cancellation [34]. These methods are similar to DFE in that interference from symbols that are decided in a block is canceled before a decision on the current symbol is made. In SIC-ILS, least squares is used as the optimization criterion and at each step or iteration, the cost function (least squares) will decrease or remain the same. In multistage cancellation, the MMSE criterion is often used to render matched filter optimum after the interference is removed (supposing that the noise is white). The difference between a multistage cancellation scheme and the block DFE is that the DFE symbol decisions are made serially; and for each undecided symbol, only interference from symbols that have been decided is canceled; while in multistage cancellation, all symbols are decided simultaneously before their mutual interferences are removed in a parallel fashion.

In addition to existing iterative approaches, it may also be possible to adopt for CFC-OFDM equalization the iterative "sum–product" decoding algorithm, which is also used in turbo decoding and other interesting problems [17]. The idea is to represent the coded system using a factor graph, which describes the interdependence of the encoder input, the encoder output, and the noise-corrupted coded symbols.

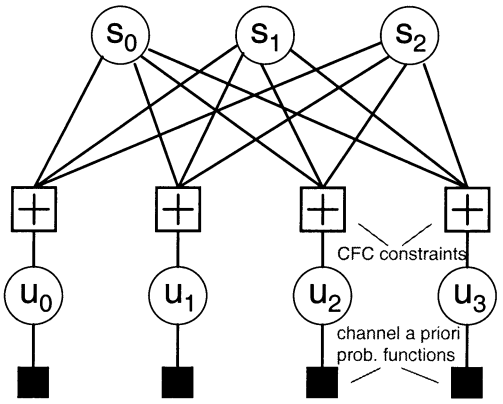

Fig. 7. Factor graph representation of CFC.

As a simple example, suppose the encoder takes a block of three symbols $\boldsymbol{s} := [s_0, s_1, s_2]^T$ as input, and linearly encodes them by a 4×3 matrix $\boldsymbol{\Theta}$ to produce the coded symbols $\boldsymbol{u} := [u_0, u_1, u_2, u_3]$. After passing through the channel (OFDM modulation/demodulation), we obtain the channel output $x_i = H(e^{j2\pi i/4})u_i$, $i = 0, 1, 2, 3$. The factor graph for such a coded system is shown in Fig. 7, where the CFC is represented by linear constraints between the CFC input symbols $\boldsymbol{s}$ and the CFC output symbols $\boldsymbol{u}$.

The analysis and verification of such a sum–product algorithm constitute interesting future research topics. But we remark that our decoding problem in its full generality has the same level of difficulty as the lattice decoding problem (so, we expect these topics to be difficult).

E. Parallel (or Subgroup) Encoding for Low Complexity Decoding

When the number of carriers N is very large (e.g., 1,024), it is desirable to keep the decoding complexity manageable. To achieve this we can split the encoder into several smaller encoders. Specifically, we can choose $\boldsymbol{\Theta} = \boldsymbol{P}\boldsymbol{\Theta}'$, where $\boldsymbol{P}$ is a permutation matrix that interleaves the subcarriers, and $\boldsymbol{\Theta}'$ is a block diagonal matrix: $\boldsymbol{\Theta}' = \mathrm{diag}(\boldsymbol{\Theta}_0, \boldsymbol{\Theta}_1, \ldots, \boldsymbol{\Theta}_{M-1})$. This is a essentially a form of coding for interleaved OFDM, except that coding here is performed in the complex domain. The matrices $\{\boldsymbol{\Theta}_m\}_{m=0}^{M-1}$ are of smaller size than $\boldsymbol{\Theta}$, and all of them can even be chosen to be identical. With such a $\boldsymbol{\Theta}$, decoding $\boldsymbol{s}$ from the noisy $\boldsymbol{D}_H\boldsymbol{\Theta}\boldsymbol{s}$ is equivalent to decoding M coded subvectors of smaller sizes, which reduces the overall decoding complexity considerably. Such a decomposition is particularly important when a high complexity near-ML decoder such as SD is to be deployed.

The price paid for low decoding complexity is a decrease in transmission rate. When such parallel encoding is used, we should make sure that each of the $\boldsymbol{\Theta}_m$ matrices can guarantee full diversity, which requires $\boldsymbol{\Theta}_m$ to have L redundant rows. The overall $\boldsymbol{\Theta}$ will then have ML redundant rows, which corresponds to an M-fold increase in redundancy relative to a full single encoder of size $N \times K$. If a fixed constellation is used for entries in $\boldsymbol{s}$, then *square* $\boldsymbol{\Theta}_m$'s can be used, which does not lead to loss of efficiency. Research in this direction has been pursued in [19].

VI. Simulation Results

In this section, we study the performance of the CFC-OFDM system via computer simulation. We will compare the proposed system with existing coded OFDM systems that employ existing GF block and convolutional codes. In all cases, a BPSK constellation is used; i.e., $\mathcal{S} = \{\pm 1\}^K$, and in Test Cases 2 and 3, the binary encoded symbols are mapped to ± 1's before OFDM modulation.

Test Case 1 (Decoding of CFC-OFDM): We first test the performance of different decoding algorithms. The CFC-OFDM system has parameters $K = 14$, $N = 16$, $L = 2$. The channel is i.i.d. Rayleigh and BERs for 200 random channel realizations according to **AS1)** are averaged. Fig. 8 shows the performance of ZF, MMSE, DFE, and sphere decoding (near-ML). We notice that at BER of 10^{-4}, DFE performs about 2 dB better than the MMSE detectors, while at the same time it is only less than 1 dB inferior to SD, which virtually achieves the ML decoding performance. The complexity of ZF, MMSE, and DFE is about $N = 16$ flops per symbol, which is much less than the complexity of SD, which empirically needs about 800 flops per symbol in this case.

Test Case 2 (Comparing CFC- With BCH-Coded OFDM): For demonstration and verification purposes, we first compare CFC-OFDM with coded OFDM that relies on GF block coding. The channel is modeled as FIR with five i.i.d. Rayleigh distributed taps. In Fig. 9, we depict BER performance of CF coded OFDM with the Vandermonde code of Theorem 4, along with BER of binary BCH-coded OFDM. The system parameters are $K = 26$, $N = 31$. The generating polynomial of the BCH code is $g(D) = 1 + D^2 + D^5$. Since we can view this BCH as a rate 1 convolutional code with the same generator and with termination after 26 information symbols (i.e., the code ends at the all-zero state), we can use the Viterbi algorithm for soft-decision ML BCH decoding. For CFC-OFDM, since the transmission is essentially a ZP-only single-carrier scheme, the Viterbi algorithm is also applicable for exact ML decoding.

Since the binary $(26, 31)$ BCH code has minimum Hamming distance 3, it possesses a diversity order of 3, which is only half of the maximum possible $(L + 1 = 6)$ that CFC-OFDM achieves with the same spectral efficiency. This explains the difference in their performance. We can see that when the optimum ML decoder is adopted by both receivers, CFC-OFDM outperforms BCH-coded OFDM considerably. The slopes of the corresponding BER curves also confirm our theoretical results.

Test Case 3 (Comparing CFC-OFDM With Convolutionally Coded OFDM) : In this test, we compare (see Fig. 10) our CFC-OFDM system with convolutionally coded OFDM (with a rate $1/2$ code punctured to rate $3/4$ followed by interleaving) that is deployed by the HiperLAN2 standard [7] over the channels used in Test Case 2. The rate $1/2$ mother code has its generator in octal form as $(133, 171)$, and there are 64 states in its trellis. Every third bit from the first branch and every second bit from the second branch of the mother code are punctured to obtain the rate $3/4$ code, which results in a code whose weight enumerating function is $8W^5 + 31W^6 + 160W^7 + \cdots$. So the free distance is 5, which means that the achieved diversity is 5, less than the diversity order 6 achieved by CFC-OFDM.

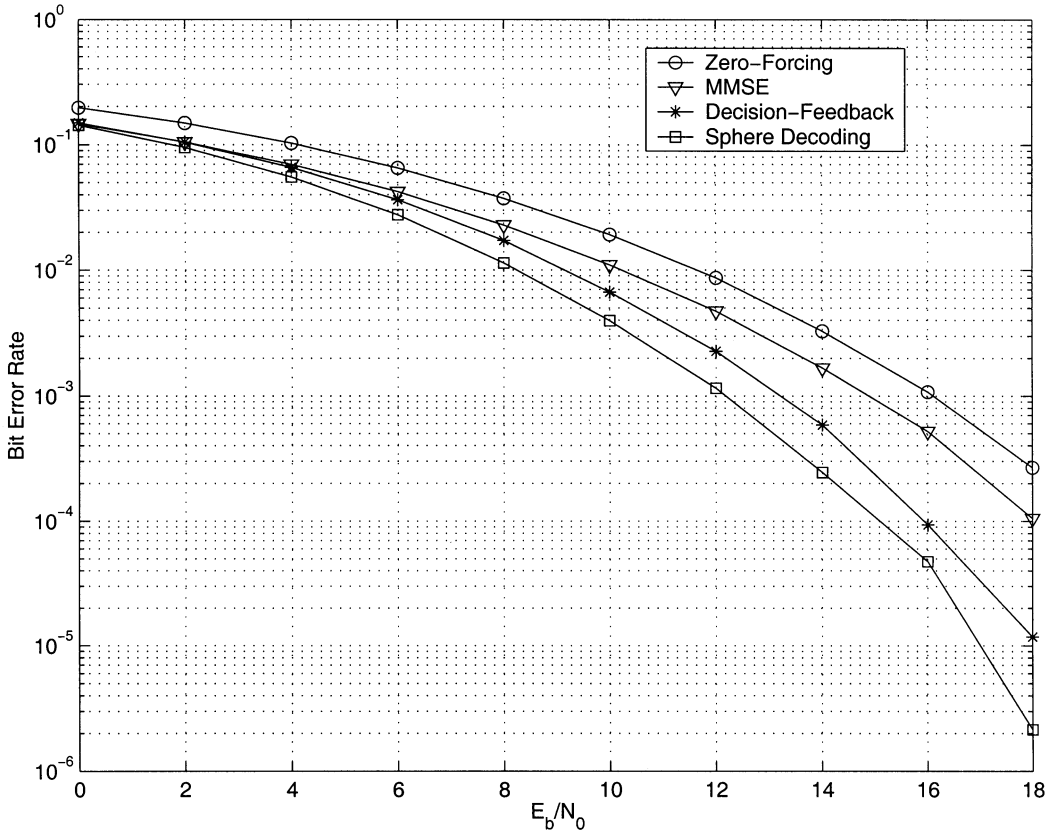

Fig. 8. Decoding of CFC-OFDM.

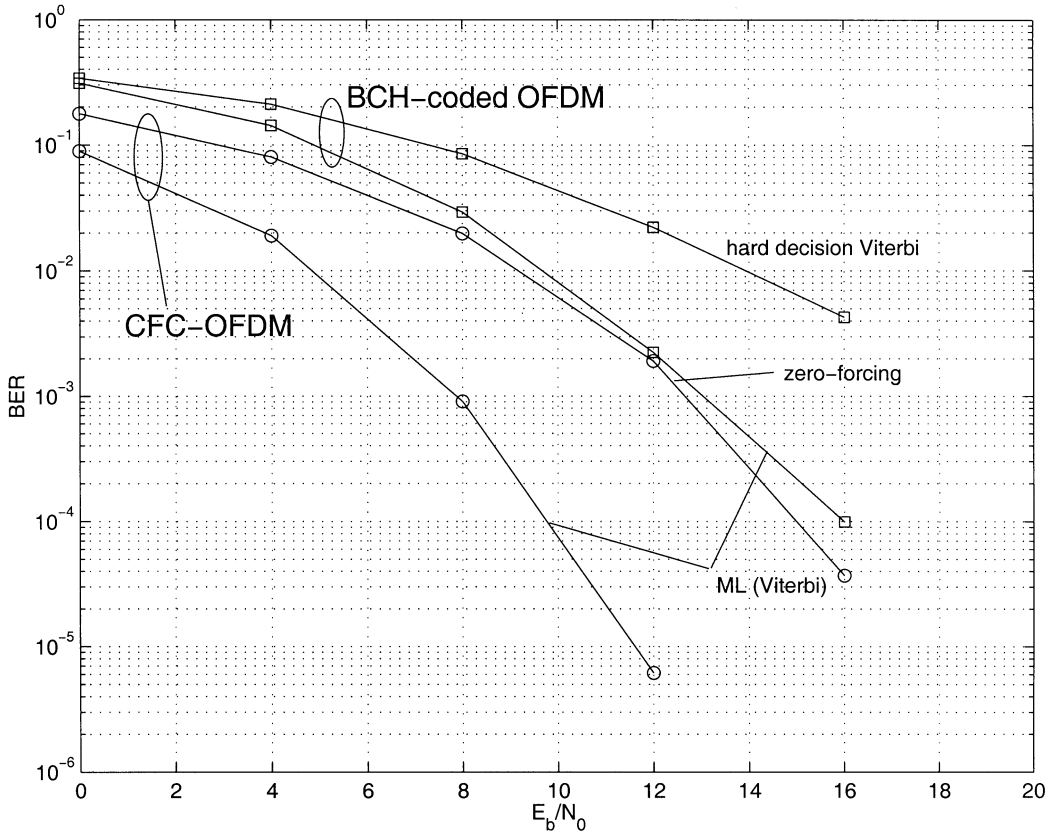

Fig. 9. CFC-OFDM versus BCH coded OFDM.

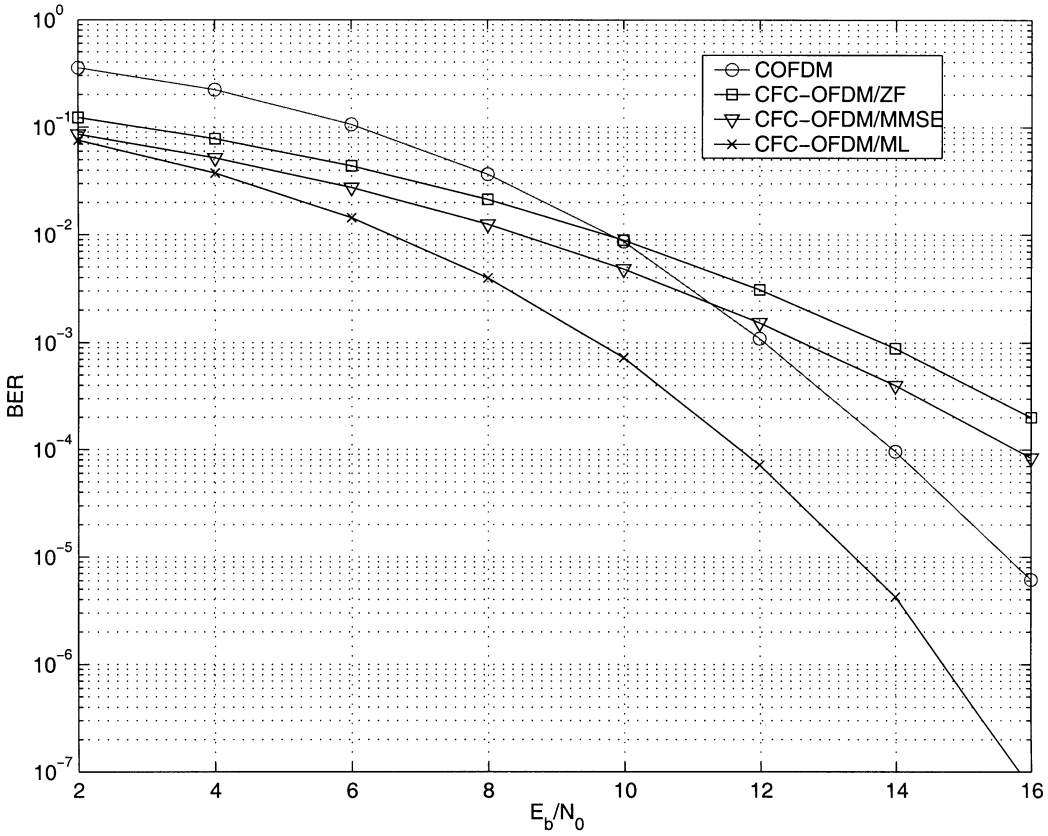

Fig. 10. CFC-OFDM versus convolutionally coded OFDM in HiperLAN2.

Next, we use two parallel truncated DCT encoders with parameters $K = 36$ and $N = 48$; that is, $\mathbf{\Theta} = \boldsymbol{I}_{2\times 2} \otimes \mathbf{\Theta}_0$, where $\otimes$ denotes Kronecker product, and $\mathbf{\Theta}_0$ is a 24×18 encoder obtained by taking the first 18 columns of a 24×24 DCT matrix. With ML decoding, CFC-OFDM performs about 2 dB better than convolutionally coded OFDM. From the ML performance curves in Fig. 10, it also appears that CFC-OFDM achieves a larger coding advantage than the punctured convolutional code used.

Surprisingly, even with linear MMSE equalization, the performance of CFC-OFDM is better than coded OFDM for SNR values less than 11 dB. The complexity of ML decoding for CFC-OFDM is quite high—in the order of 1000 flops per symbol. But the ZF and MMSE decoders have comparable or even lower complexity than the Viterbi decoder for the convolutional code.

When a low rate (e.g., $1/2$) convolutional code with larger d_{free} is used instead of the punctured code used here, the performance of convolutionally coded OFDM is expected to improve and eventually surpass CFC-OFDM due to the convolutional code's stronger error-correcting capability. We have verified this through simulations in [37].

The complexity of CFC-OFDM can be dramatically reduced using the parallel encoding method of Section V-E with square encoders; see [19] for further details. It is also possible to combine CF coding with conventional GF coding, in which case only small square encoders of size 2×2 or 4×4 are enough to achieve near optimum performance [38].

VII. Conclusion and Discussion

To improve the average performance of OFDM over random frequency-selective channels, we developed in this paper a complex field coding technique which linearly encodes the information symbols through a matrix that introduces a small amount of redundancy in order to robustify the system against frequency-selective fading. Using pairwise error probability analysis, we derived expressions for the diversity and coding gains. Next, we identified conditions for achieving the maximum diversity order. It turned out that the conditions are also closely related to those involved in the design of MDS codes in GF codes such as RS codes. The advantage of our real/complex field linear coding scheme is twofold: i) it can guarantee maximum diversity order irrespective of the underlying symbol constellations; and ii) MDS (N, K) linear complex field codes always exist for any $N \geq K$.

Several constructions were provided for obtaining maximum diversity encoders. For a given constellation, we quantified the maximum achievable coding gain. The maximum coding gain can be achieved by a zero-padded single-carrier transmission, which can be viewed as a special case of our complex field coded OFDM.

We also provided several decoding options, including ML, ZF, MMSE, DFE, and iterative detectors. Decision directed detectors strike the best tradeoff between complexity and performance.

There are several possible directions to pursue. One is to investigate the coding gain of various (including square) linear

encoders, and compare it with existing GF codes. From our simulated comparisons of CFC-OFDM with GF-coded OFDM (Test Case 3), we expect CFC-OFDM to have larger coding advantage compared to high rate GF codes, but this needs to be quantified. Another promising direction is the combination of GF codes with CF codes. It appears that GF codes are more appropriate for random errors introduced by channel noise or by very fast random fading which can be realized via interleaving, while CF codes are more powerful in coping with structured errors such as those introduced by channel ISI or, in the OFDM case, by frequency selectivity. With the goal of improving the system performance against all these impairments—noise, frequency- and time-selectivity—that wireless transmissions suffer from, a combined approach that integrates CF and GF coding has been recently pursued in [38]. Using our results here as a starting point, [38] establishes that joint GF-CF coding can offer multiplicative diversity, while the complexity is only additive.

ACKNOWLEDGMENT

The authors thank Yongwu Shao for his suggestions in the proof of Theorem 4, Dr. W. Henkel for his helpful feedback, and for providing [12], [13], and the reviewers for valuable comments that helped us improve the paper.

REFERENCES

[1] N. Al-Dhahir and A. H. Sayed, "The finite-length multi-input multi-output MMSE-DFE," *IEEE Trans. Signal Processing*, vol. 48, pp. 2921–2936, Oct. 2000.

[2] I. Blake, C. Heegard, T. Høholdt, and V. Wei, "Algebraic-geometry codes," *IEEE Trans. Inform. Theory*, vol. 44, pp. 2596–2618, Oct. 1998.

[3] 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.

[4] B. Chen and G. W. Wornell, "Analog error-correcting codes based on chaotic dynamical systems," *IEEE Trans. Commun.*, vol. 46, pp. 881–890, July 1998.

[5] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices, and Groups*, 3rd ed. New York: Springer-Verlag, 1998.

[6] A. Czylwik, "OFDM and related methods for broadband mobile radio channels," in *Proc. Int. Zurich Seminar on Broadband Communications*, Zürich, Switzerland, 1998, pp. 91–98.

[7] ETSI, "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2 Technical Specification Part 1—Physical Layer," Tech. Rep., DTS/BRAN030003-1, 1999.

[8] U. Fincke and M. Pohst, "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis," *Math. Comput.*, vol. 44, pp. 463–471, Apr. 1985.

[9] G. D. Forney Jr, "Maximum-likelihood sequence estimation of digital sequences in the presence of intersymbol interference," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 363–378, May 1972.

[10] G. B. Giannakis, "Filterbanks for blind channel identification and equalization," *IEEE Signal Processing Lett.*, vol. 4, pp. 184–187, June 1997.

[11] V. D. Goppa, *Geometry and Codes*. Norwell, MA: Kluwer Academic, 1988.

[12] W. Henkel, "Multiple error correction with analog codes," in *Proc. AAECC-6 (Lecture Notes in Computer Science)*. Berlin, Germany: Sspringer-Verlag, 1988, vol. 357, pp. 239–249.

[13] ——, "Zur Decodierung algebraischer Blockcodes über komplexen Alphabeten," Ph.D. dissertation, VDI-Verlag, Düsseldorf, Germany, 1989.

[14] ——, "Analog codes for peak-to-average ratio reduction," in *Proc. 3rd ITG Conf. Source and Channel Coding*, Munich, Germany, Jan. 2000.

[15] Y. H. Jeong, K. N. Oh, and J. H. Park, "Performance evaluation of trellis-coded OFDM for digital audio broadcasting," in *Proc. IEEE Region 10 Conf*, vol. 1, 1999, pp. 569–572.

[16] R. Knopp and P. A. Humblet, "On coding for block fading channels," *IEEE Trans. Inform. Theory*, vol. 46, pp. 189–205, Jan 2000.

[17] F. R. Kschischang, B. J. Frey, and H.-A. Loeliger, "Factor graphs and the sum-product algorithm," *IEEE Trans. Inform. Theory*, vol. 47, pp. 498–519, Feb 2001.

[18] T. Li and N. D. Sidiropoulos, "Blind digital signal separation using successive interference cancellation iterative least squares," *IEEE Trans. Signal Processing*, vol. 48, pp. 3146–3152, Nov. 2000.

[19] Z. Liu, Y. Xin, and G. B. Giannakis, "Linear constellation precoding for OFDM with maximum multipath diversity and coding gains," in *Proc. Asilomar Conf. Signals, Systems & Computers*, Pacific Grove, CA, Nov. 4–7, 2001, pp. 1445–1449.

[20] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[21] T. G. Marshall Jr, "Coding of real-number sequences for error correction: A digital signal processing problem," *IEEE J. Select. Areas Commun.*, vol. 2, pp. 381–392, Mar. 1984.

[22] B. Muquet, Z. Wang, G. B. Giannakis, M. de Courville, and P. Duhamel, "Cyclic prefixing or zero padding for wireless multicarrier transmissions?," *IEEE Trans. Commun.*, vol. 50, pp. 2136–2148, Dec. 2002.

[23] S. Ohno and G. B. Giannakis, "Optimal training and redundant precoding for block transmissions with application to wireless OFDM," in *Proc. Int. Conf. Accoustics, Speech, and Signal Processing*, vol. 4, Salt Lake City, Utah, May 7–11, 2001, pp. 2389–2392.

[24] R. M. Roth and G. Seroussi, "On generator matrices of MDS codes," *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 826–830, Nov. 1985.

[25] A. Ruiz, J. M. Cioffi, and S. Kasturia, "Discrete multiple tone modulation with coset coding for the spectrally shaped channel," *IEEE Trans. Commun.*, vol. 40, pp. 1012–1029, June 1992.

[26] H. R. Sadjadpour, "Application of turbo codes for discrete multi-tone modulation schemes," in *Proc. Int. Conf. Comunications*, vol. 2, Vancouver, BC, Canada, 1999, pp. 1022–1027.

[27] A. Scaglione, G. B. Giannakis, and S. Barbarossa, "Linear precoding for estimation and equalization of frequency-selective channels," in *Signal Processing Advances in Wireless and Mobile Communications*, G. B. Giannakis, Y. Hua, P. Stoica, and L. Tong, Eds. Upper Saddle River, NJ: Prentice Hall, 2001, vol. I, ch. 9.

[28] G. Seroussi and R. M. Roth, "On MDS extensions of generalized Reed-Solomon codes," *IEEE Trans. Inform. Theory*, vol. IT-32, pp. 349–354, May 1986.

[29] N. Sidiropoulos, G. Giannakis, and R. Bro, "Blind PARAFAC receivers for DS-CDMA systems," *IEEE Trans. Signal Processing*, vol. 48, pp. 810–823, Mar. 2000.

[30] R. C. Singleton, "Maximum distance q-nary codes," *IEEE Trans. Inform. Theory*, vol. IT-10, pp. 116–118, Apr. 1960.

[31] A. Stamoulis, G. B. Giannakis, and A. Scaglione, "Block FIR decision-feedback equalizers for filterbank precoded transmissions with blind channel estimation capabilities," *IEEE Trans. Commun.*, vol. 49, pp. 69–83, Jan. 2001.

[32] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communication: Performance criterion and code construction," *IEEE Trans. Inform. Theory*, vol. 44, pp. 744–765, Mar. 1998.

[33] G. van der Geer, "Codes and elliptic curves," in *Effective Methods in Algebraic Geometry*, T. Mora and C. Traverso, Eds, Basel, Switzerland: Birkhäuser, 1991.

[34] S. Verdú, *Multiuser Detection*. Cambridge, U.K.: Cambridge Univ. Press, 1998.

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

[36] Z. Wang and G. B. Giannakis, "Wireless multicarrier communications: where Fourier meets Shannon," *IEEE Signal Processing Mag.*, vol. 47, pp. 29–48, May 2000.

[37] Z. Wang, X. Ma, and G. B. Giannakis, "OFDM or single-carrier zero-padded block transmissions?," *IEEE Trans. Commun.*, accepted Aug. 2002. See also "Optimality of single-carrier zero-padded block transmission," in *Proc. Wireless Comm. and Networking Conf.*, pp. 660--664, 2002, Orlando, FL.

[38] Z. Wang, S. Zhou, and G. B. Giannakis, "Joint coding-precoding with low-complexity turbo-decoding," *IEEE Trans. Wireless Commun.*, Oct. 2002 (revised), submitted for publication.

[39] R. D. Wesel, X. Liu, and W. Shi, "Trellis codes for periodic erasures," *IEEE Trans. Commun.*, vol. 48, pp. 938–947, June 2000.

[40] J. K. Wolf, "Redundancy, the discrete Fourier transform, and impulse noise cancellation," *IEEE Trans. Commun.*, vol. COM-31, pp. 458–461, Mar. 1983.

[41] X.-G. Xia, P. Fan, and Q. Xie, "A new coding scheme for ISI channels: Modulated codes," in *Proc. Intl. Conf. Communications*, vol. 2, Vancouver, BC, Canada, 1999, pp. 828–832.

[42] Y. Xin, Z. Wang, and G. B. Giannakis, "Space-time diversity systems based on unitary constellation-rotating precoders," in *Proc. Int. Conf. Accoustics, Speech, and Signal Processing*, vol. 4, Salt Lake City, UT, May 7–11, 2001, pp. 2249–2432.