On Multidimensional Coded Modulations Having Uniform Error Property for Generalized Decoding and Flat-Fading Channels

Dan Raphaeli, *Member, IEEE*

***Abstract*—We consider the problem of uniform error property (UEP) for a coded modulation with constant energy multidimensional symbols, transmitted over the additive white Gaussian noise (AWGN) or fading channels and received by a broad class of decoders. This class includes coherent, partially coherent, double differential, and noncoherent decoders, decoders designed for fading channels, decoders using one or multiple-symbol observations, and many more. These decoders are described as special cases of a general decoder model. This decoder operates by maximizing an arbitrary likelihood function that its arguments are front-end correlator (matched-filter) outputs. A group code structure that guarantees UEP is developed by using the theory of geometrically uniform codes and applying it to the general decoder. These codes are defined over groups (commonly nonbinary) with isometric mapping to channel symbols. We show the code construction for the specific case of Lth-dimensional M-ary phase-shift keying (MPSK). An additional interesting property of these general uniform error codes is related to the case of noncoherent decoding. We show that when using codes of this family, if a code is noncoherently catastrophic, then it is also rotationally invariant. Then, the use of precoding of the input such that the code becomes rotationally transparent will also make it noncatastrophic.**

***Index Terms*— Geometrically uniform codes, noncoherent detection, trellis-coded modulation.**

I. INTRODUCTION

MOST COMMONLY used channel encoders have a nice property called uniform error property (UEP).[1] UEP means that the error probability is the same for all the transmitted codewords, i.e., $P_r\{\text{error}|x_i\}$ is not dependent on the transmitted codeword x_i. By using this property, the error probability analysis is much simpler. For example, when evaluating the union bound we do not have to check all possible pairs of codewords (transmitted and received), but only assume that a specific convenient word such as the all-0 sequence was transmitted. When the codes to be used are also linear over some field, the UEP and the linearity work together to considerably simplify the analysis, design, and decoder implementation. Moreover, as mentioned first by Ungerboeck [1] and also by Forney [2], good codes are more likely to be found among the class of UEP codes.

In particular, binary linear codes satisfy UEP when they are used over a binary symmetric channel or when they are used with binary phase-shift keying (BPSK) or quaternary phase-shift keying (QPSK) transmitted over the additive white Gaussian noise (AWGN) channel.

Recently, there has been an increased interest in codes for the AWGN channel that satisfy UEP when used with optimal coherent detection. These codes are called geometrically uniform (GU) codes [2] and were shown to include most good known codes. Motivated by their benefits, good GU signal set partitions and trellis codes have been found [3], [4].

If the optimal coherent decoder for the AWGN channel is assumed, then the error probability is determined by the set of all Euclidean distances between the transmitted codeword and all of the other codewords. Various decoders have been proposed over the years that are not based on Euclidean distance [6]–[13]. These include partially coherent, noncoherent, differential, and double differential decoders, and also decoders designed for various forms of fading. The more advanced schemes use multiple-symbol observations. When the Euclidean distance no longer dictates the error probability, the conventional GU codes may no longer satisfy the UEP. This also includes the case of the popular binary coded QPSK. Unlike the linearity of the code, which does not depend on the decoder, the UEP depends on the code, the modulation, the decoder's metric, and the channel.

The objective of this paper is to construct codes that exhibit UEP under much wider channel and decoder conditions than the GU codes designed for the AWGN channel. These codes will be referred to as general uniform error (GUE) codes. The channels that we allow are flat fading with arbitrary correlated or uncorrelated fading statistics. This includes the AWGN channel as a special case. For the decoder, a general model is defined, which is general enough to include most of the types of decoders used today. The transmitted symbols, however, are restricted to have constant energy, i.e., located on a $2D$-dimensional sphere, where $2D$ is the number of dimensions of the symbols. The general decoder is one that maximizes an arbitrary likelihood function that its arguments are the symbol-by-symbol correlation of the received signal with a candidate sequence. This correlation is also equivalent to matched filtering. We call this decoder a *correlator-based decoder* or, equivalently, a *correlator-based receiver*. This

---

Paper approved by S. S. Pietrobon, the Editor for Coding Theory and Techniques of the IEEE Communications Society. Manuscript received July 1, 1996; revised February 3, 1997 and July 18, 1997. This paper was presented in part at the 1995 Communication Theory Mini Conference, GLOBECOM'95, Singapore, November 1995.

The author is with the Electrical Engineering Systems Department, Tel Aviv University, Tel Aviv 69978, Israel (e-mail: danr@eng.tau.ac.il).

Publisher Item Identifier S 0090-6778(98)01061-7.

[1] Not to be confused with the acronym UEP that is sometimes used for "unequal error protection."

decoder also includes the coherent decoder (the one that minimizes the Euclidean distance) as a special case.

The GUE codes are generated using the GU codes concept. We find for the case of the correlator-based decoder a new function to replace the Euclidean distance. Unfortunately, this function is not a proper distance; it is neither symmetric nor transitive, and so it will be called *pseudo-distance*. Nevertheless, we can use it to define "isometries" and "symmetries," and then use most of the important results of GU theory that include the UEP.

For the case of $L \times M$-ary phase-shift keying (MPSK) modulation ($2L$-dimensional space, MPSK in each pair of dimensions) we are able to find "geometrically uniform" signal sets, partitions, and isometric labels appropriate for the pseudo-distance. The result for $L \times$ MPSK signals shows that one should use group codes over $\Pi_{i=0}^{L-1} Z_{R_i}$, the Cartesian product of Z_{R_i}, the groups of integers modulo R_i. R_i must be a divisor of M. These group codes are then naturally matched to a partition of the $L \times$ MPSK constellation. The usefulness of such group codes using MPSK signals, as well as the ease of making them rotationally invariant, have been recognized in the past to some extent [4], [15], [16]. Here, such group codes are shown to have more applications and usefulness by being GUE. For the special case of linear (homomorphic) codes with no set partitioning, the codes presented here can be shown to be equivalent to the codes called "linear noncoherent codes" introduced in [18] and used for noncoherent decoding in [13]. More on the definition and analysis of group codes can be found in [17].

The current application of these codes is in multiple-symbol noncoherent systems. Therefore, we discuss the use of GUE codes in such systems and show some related properties. The *noncoherent decoder* is an interesting special case of the correlator-based decoder. Noncoherent decoding rather than detection means that the decoder does the combined work of noncoherent detection and decoding, like in [13] or [11]. It must be emphasized that the notion of noncoherent detection here (see Section VI) is much wider than the usual definition of a channel phase independent for each symbol. We assume that the channel phase for each symbol is indeed *dependent*.

Not all codes can be decoded noncoherently. Noncoherently catastrophic (NC) codes [13] are codes that cannot be noncoherently decoded. We are going to show that, for the codes belonging to the GUE family, if a pair of codewords in a GUE code differ in a constant phase shift θ then the code is rotational invariant to θ. Thus, in the GUE case, the NC property implies rotational invariance (RI). This provides an easy test for NC. Also, for a code which is found to be NC, the use of differential encoding of the input to the encoder (which we call differential precoding in this paper) such that the code becomes rotationally transparent will also make it non-NC.

The paper is organized as follows. In Section II, the model of the correlator-based decoder is described. In Section III, the error probability of the correlator-based decoder is obtained. Then, in Section IV, we construct the GUE codes. In Section V, we find the generating functions and partitions for the $L \times$ MPSK constellation. Finally, in Section VI, for noncoherent decoders in particular, we discuss which codes can and which cannot be noncoherently decoded and discuss the relation of this property to RI.

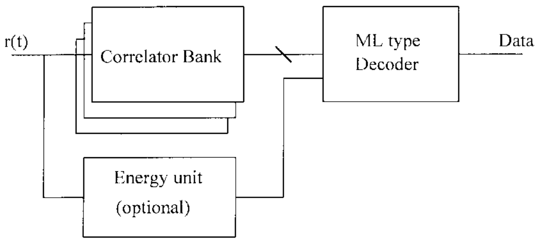

Fig. 1. The general receiver model.

II. CORRELATOR-BASED DECODER MODEL

The correlator-based decoder model consists of a complex correlator front-end (also called matched-filter bank) and a decoder that uses the output of the correlator for making its decisions (see Fig. 1). An option exists to add an energy measurement unit. The energy information may be used by decoders for fading channels which have intrinsic measurement of channel state information (CSI). This model includes almost all of the receiving strategies obtained by using the maximum-likelihood (ML) principle. Some of the most important existing receiver structures (restricted to constant energy symbols) admit our representation. These includes the coherent detection, optimal differential detection, multiple-symbol noncoherent decoder [13], [11], [10], partially coherent receiver [6, eq. 6.59b], receiver coherent with respect to the specular part of the signal in a slow fading Rician channel with no CSI [6, p. 373], optimal coherent receiver for the fading channel with ideal CSI [7, p. 348], double differential detection [6, Ch. 8], and the general ML receiver structure of Makrakis [8] for a fast fading Rician channel extended to D dimensions.

Let T_s be the symbol duration, $r(t)$ be the complex envelope (CE) of the received signal, and $x(t)$ be the CE of one of the possible equally likely transmitted signals. $x(t)$ is a sum of symbols $x_i(t)$ that can be represented as

$$x_i(t) = \sum_{j=0}^{D-1} x_{i,j}\varphi_j(t - iT_s) \tag{1}$$

where $\{\varphi_0, \varphi_1, \cdots, \varphi_{D-1}\}$ is an orthonormal set of complex functions. Let $r_{i,j}$ be the corresponding projections of $r(t)$ on the same basis functions. In a vector form, the transmitted and received symbols are denoted by $\boldsymbol{x}_i = (x_{i,0}, \cdots, x_{i,D-1})^T$ and $\boldsymbol{r}_i = (r_{i,0}, \cdots, r_{i,D-1})^T$. Using vector notation, the correlator is defined as

$$\mu_i = \boldsymbol{r}_i^\dagger \boldsymbol{x}_i \tag{2}$$

where $A^\dagger = (A^T)^*$ and the energy measurement unit consists of the operation

$$\xi_i = \boldsymbol{r}_i^\dagger \boldsymbol{r}_i = \|\boldsymbol{r}_i\|^2. \tag{3}$$

The decoder makes its decisions by maximizing some likelihood function $f(\mu_0, \mu_1, \cdots, \mu_{N-1}, \xi_0, \xi_1, \cdots, \xi_{N-1})$ of the outputs of the correlator, where μ_i and ξ_i are the correlator output and the energy for the ith symbol, respectively. The number of symbols the decoder operates on is N ($N \to \infty$

for convolutional codes). Note that f is an arbitrary real valued function. To summarize, the decoder chooses $\hat{\boldsymbol{x}}$ which maximizes

$$\begin{aligned}\Lambda(\hat{\boldsymbol{x}}) = {} & f(\boldsymbol{r}_0^\dagger \hat{\boldsymbol{x}}_0, \boldsymbol{r}_1^\dagger \hat{\boldsymbol{x}}_1, \cdots, \boldsymbol{r}_{N-1}^\dagger \hat{\boldsymbol{x}}_{N-1}, \\ & \|\boldsymbol{r}_0\|^2, \|\boldsymbol{r}_1\|^2, \cdots, \|\boldsymbol{r}_{N-1}\|^2). \end{aligned} \tag{4}$$

In case of a tie, the decoder has to randomly choose between those sequences attaining maximum. We can write (4) in a more convenient form as

$$\Lambda(\hat{\boldsymbol{x}}) = f(\{\boldsymbol{r}_i^\dagger \hat{\boldsymbol{x}}_i\}, \{\|\boldsymbol{r}_i\|^2\}). \tag{5}$$

Example: In the coherent demodulation of constant energy signals (e.g., [19]), the optimal f is

$$f(\{\boldsymbol{r}_i^\dagger \boldsymbol{x}_i\}) = \sum_{i=0}^{N-1} \operatorname{Re}\{\boldsymbol{r}_i^\dagger \boldsymbol{x}_i e^{-j\phi}\} \tag{6}$$

where ϕ is the known channel phase.

III. DETERMINATION OF THE ERROR PROBABILITY

The flat-fading channel model we are using is defined as follows. Let $\boldsymbol{x}_i, i = 0, \cdots, N-1$ be the transmitted signal with constant symbols energy $\boldsymbol{x}_i^\dagger \boldsymbol{x}_i = 1$ (for simplicity), and let $\boldsymbol{r}_i = \alpha_i \boldsymbol{x}_i + \boldsymbol{n}_i$ be the received signal components where $\boldsymbol{n}_{i,j}, i = 0, \cdots, N-1, j = 0, \cdots, D-1$ are independent complex Gaussian random variables with zero mean and variance σ_i^2. The complex random variables α_i represent the possible fading and are independent of $\boldsymbol{n}_k$ or $\boldsymbol{x}_k$ $\forall k$. It is assumed that no intersymbol interference (ISI) is present, and the fading is sufficiently slow to not distort the transmitted pulse shape. Let $\boldsymbol{x}$ and $\boldsymbol{y}$ be two codewords. Let us define the operation

$$\begin{aligned}\rho(\boldsymbol{x}, \boldsymbol{y}) &= (\rho_0, \rho_1, \cdots, \rho_{N-1}) \\ &= (\boldsymbol{x}_0^\dagger \boldsymbol{y}_0, \boldsymbol{x}_1^\dagger \boldsymbol{y}_1, \cdots, \boldsymbol{x}_{N-1}^\dagger \boldsymbol{y}_{N-1}) \end{aligned} \tag{7}$$

which is the sequence of symbol-by-symbol complex correlations between $\boldsymbol{x}$ and $\boldsymbol{y}$. Note that $\rho(\boldsymbol{x}, \boldsymbol{y})$ is not commutative—switching the order of the arguments leads to complex conjugation. The main result of this section is the following theorem.

Theorem: Let us have a constant energy coded system $\{\boldsymbol{x}^{(m)}\}$ with M equally likely codewords. The error probability of the system over the flat-fading channel with the correlator-based decoder is completely determined by the set of M^2 vectors $\rho(\boldsymbol{x}^{(m)}, \boldsymbol{x}^{(n)}), m = 0, \cdots, M-1, n = 0, \cdots, M-1$ and by the channel parameters.

The channel parameters are the noise variance sequence $\{\sigma_i^2\}$ and the statistics of $\{\alpha_i\}$. In particular, the *pairwise* error probability $P_e(\boldsymbol{x} \to \boldsymbol{y})$ is completely determined by $\rho(\boldsymbol{x}, \boldsymbol{y})$.

Proof: Let $\boldsymbol{x}^{(l)}$ be the transmitted sequence. The probability that the decoder makes an incorrect decision by choosing another sequence is

$$\begin{aligned} P_e(\boldsymbol{x}^{(l)}) &= P_r[\arg\max_m\{f(\{\boldsymbol{r}_i^\dagger \boldsymbol{x}_i^{(m)}\}, \{\|\boldsymbol{r}_i\|^2\}) \neq l] \\ &= P_r[\arg\max_m\{f(\{\alpha_i(\boldsymbol{x}_i^{(l)})^\dagger \boldsymbol{x}_i^{(m)} + \boldsymbol{n}_i^\dagger \boldsymbol{x}_i^{(m)}\}, \\ &\qquad \{\|\alpha_i \boldsymbol{x}_i^{(l)} + \boldsymbol{n}_i\|^2\})\} \neq l] \\ &= P_r[\arg\max_m\{f(\{\alpha_i(\boldsymbol{x}_i^{(l)})^\dagger \boldsymbol{x}_i^{(m)} + \boldsymbol{n}_i^\dagger \boldsymbol{x}_i^{(m)}\}, \\ &\qquad \{|\alpha_i|^2 + 2\operatorname{Re}[\alpha_i \boldsymbol{n}_i^\dagger \boldsymbol{x}_i^{(l)}] + \|\boldsymbol{n}_i\|^2\})\} \neq l]. \end{aligned} \tag{8}$$

Now let $\{\boldsymbol{a}^{(m)}\}$ be another constant energy coded system satisfying

$$\rho(\boldsymbol{x}^{(m)}, \boldsymbol{x}^{(n)}) = \rho(\boldsymbol{a}^{(m)}, \boldsymbol{a}^{(n)}) \quad \forall\, m, n. \tag{9}$$

We will show that the error probability of the new system is the same as our system, and the proof of the theorem will be implied. As shown in the Appendix, for each symbol i there exists a unitary transformation A_i that satisfies

$$\boldsymbol{a}_i^{(m)} = A_i \boldsymbol{x}_i^{(m)} \quad \forall\, m. \tag{10}$$

Let us define $\boldsymbol{w}_i = A_i^\dagger \boldsymbol{n}_i$ and substitute (9) and (10) into (8) and obtain the error probability of $\boldsymbol{a}^{(l)}$ transmitted:

$$\begin{aligned} P_e(\boldsymbol{a}^{(l)}) &= P_r[\arg\max_m\{f(\{\boldsymbol{r}_i^\dagger \boldsymbol{a}_i^{(m)}\}, \{\|\boldsymbol{r}_i\|^2\})\} \neq l] \\ &= P_r[\arg\max_m\{f(\{\alpha_i(\boldsymbol{a}_i^{(l)})^\dagger \boldsymbol{a}_i^{(m)} + \boldsymbol{n}_i^\dagger \boldsymbol{a}_i^{(m)}\}, \\ &\qquad \{|\alpha_i|^2 + 2\operatorname{Re}[\alpha_i \boldsymbol{n}_i^\dagger \boldsymbol{a}_i^{(l)}] + \|\boldsymbol{n}_i\|^2\})\} \neq l] \\ &= P_r[\arg\max_m\{f(\{\alpha_i(\boldsymbol{x}_i^{(l)})^\dagger \boldsymbol{x}_i^{(m)} + \boldsymbol{w}_i^\dagger \boldsymbol{x}_i^{(m)}\}, \\ &\qquad \{|\alpha_i|^2 + 2\operatorname{Re}[\alpha_i \boldsymbol{w}_i^\dagger \boldsymbol{x}_i^{(l)}] + \|\boldsymbol{n}_i\|^2\})\} \neq l]. \end{aligned} \tag{11}$$

Since A_i is unitary, $\boldsymbol{w}_i$ has exactly the same distribution as $\boldsymbol{n}_i$, and also $\|\boldsymbol{n}_i\|^2 = \|\boldsymbol{w}_i\|^2$. There is an identity between (11) and (8). As a result $P_e(\boldsymbol{a}^{(l)}) = P_e(\boldsymbol{x}^{(l)})$. ☐

For all of the mentioned decoders the function f will get the same value if we conjugate all of its arguments. It is easy to show that in this case a code with only two codewords satisfies UEP. This also implies that under the above assumption pairwise error probabilities are always symmetric.

IV. DEFINING THE GUE CODES

The GUE codes are obtained by defining GU codes based on a function denoted by *pseudo-distance*, replacing the Euclidean distance. Let us consider a signal constellation in complex D-dimensional space $\boldsymbol{C}^D$ and two signals $x, y \in \boldsymbol{C}^D$. The pseudo-distance between x and y is $\rho(x, y) \triangleq (x^\dagger y)$ and is a complex number. Note that the new function cannot be called a distance since it does not satisfy any distance property. It is neither symmetric nor a positive real number nor transitive. Nevertheless, we can use it to define isometries which will be called *pseudo-isometries*.

A pseudo-isometry is a mapping $\gamma{:}\boldsymbol{C}^D \to \boldsymbol{C}^D$ such that, given any two points $x, y \in \boldsymbol{C}^D, \rho(\gamma(x), \gamma(y)) = \rho(x, y)$. If such a pseudo-isometry is applied to the symbols $\boldsymbol{x}_k, \boldsymbol{y}_k$ of two codewords $\boldsymbol{x}$ and $\boldsymbol{y}$ then $\rho(\boldsymbol{x}, \boldsymbol{y})$ will not change. Then, as the result of the theorem proved in the previous section, if all of the codewords of a system are transformed by a pseudo-isometry, then the error probability will not change. As a result, a GU code in which isometries are replaced by pseudo-isometries will exhibit UEP, as desired.

Following [2], the definition of GU codes has three constituents: a GU signal constellation S or its partition S/S', an

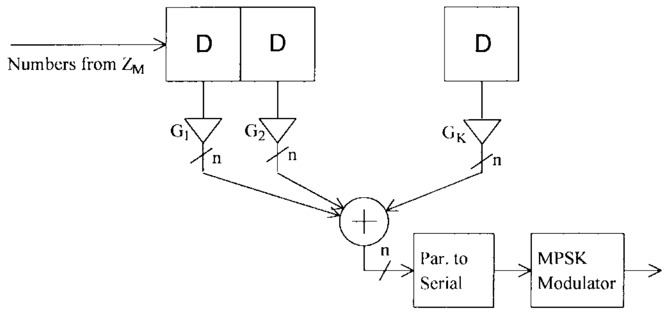

Fig. 2. The simple but useful case of linear noncoherent trellis-coded modulation.

isometric labeling A of S/S', and a group code C over A. The GUE codes are defined in the same way, where the symmetry group for the definition of the GU signal constellation is redefined to contain all of the pseudo-isometries (instead of isometries) mapping a constellation S to itself, and will be called a *pseudo-symmetry* group.

If MPSK modulation is used, the generating function is simply R_M (the group of M possible rotations). Thus, the isometric labeling is Z_M (the group of integers modulo M) and a group code over Z_M completes the GUE definition. This simplest, but very useful, GUE codes are the so-called linear noncoherent codes (see Section I). The binary linear codes with BPSK modulation are found in this family as a special case. This structure has been used in [13], where good codes for noncoherent decoding were found for $M = 2$, 4, and 8. An encoder for a rate $1/n$ convolutional linear code over Z_M mapped to MPSK (no partitions) is shown in Fig. 2. The constraint length is K and each coefficient G_k is a vector of length n with coefficients from Z_M. A multiplication in Z_M is a multiplication modulo M. Note that this structure, although intuitive, sometimes generates nonminimal or even catastrophic codes. To avoid this problem, the minimal canonical encoder structure of [17] should be used.

Removing the limitation of MPSK symbols, the following example shows that not only rotations are allowed in a pseudo-symmetry group.

Example: Consider a two-dimensional complex space (four real dimensions) and signal points $(0, e^{j(2\pi M)n})$ or $(e^{j(2\pi/M)n}, 0), n = 0 \cdots M - 1$, a total of $2M$ points. This represents the following modulator. We take $1 + \log_2 M$ bits of information. One bit is used as an input to an orthogonal frequency-shift keying (FSK) modulator. The other bits are used as input to an MPSK modulator, with the FSK modulator as a carrier. Let P_L denote the group of permutations between L complex dimensions, and $R_M^{(i)}$ denote the group R_M operating only on the ith complex dimension. Then $\Gamma(S) = R_M^{(0)} \cdot R_M^{(1)} \cdot P_2$ where '$G_1 \cdot G_2$' denotes all of the compositions of elements from group G_1 with elements from group G_2. The generating groups are $R_M^{(0)} \cdot P_2$ or $R_M^{(1)} \cdot P_2$, both isomorphic to $Z_2 \times Z_M$.

V. GENERATING FUNCTIONS AND PARTITIONS FOR $L \times$ MPSK

In this section we consider the specific and useful case of $L \times$ MPSK (L complex dimensions, MPSK constellation in each dimension). The easiest way to generate an $L \times$ MPSK symbol is to use L consecutive MPSK symbols. The receiver has to be able to synchronize correctly on these blocks of L symbols. In [3], the symmetry groups for $L \times$ MPSK for the Euclidean distance were found, and algorithms (in a general form) were described for finding all of the generating groups. GU partition tables and codes were given in [3] and [4]. We will show that a large portion of these results apply to our case.

The symmetry group of $L \times$ MPSK for the Euclidean distance is isomorphic to $P_{2L} \cdot (Z_2)^{2L}$ for $M = 4$ and to $P_L \cdot (D_M)^L$ for $M > 4$ [4], where D_M is the composition of the rotation group R_M with the group containing the identity and the reflection about the x axis. It can be shown that rotations preserve the pseudo-distance (pointwise correlation) but reflections do not.

Since the set of pseudo-symmetries defined by the pseudo-distance is a subset of the set of symmetries defined by the Euclidean distance, we can start with the symmetry group given above and eliminate all the reflections from it. The additional symmetries that exist for the Euclidean distance in the 4-PSK case results from the fact that the real and imaginary coordinates become independent. Using the pseudo-distance, $M = 4$ is no longer a special case. As a result, for every M, the pseudo-symmetry group is $\Gamma(S) = P_L \cdot (R_M)^L$. Theorem 3 of [3] gives us the recipe for obtaining the generating group. By this theorem, a generating group G is any subgroup of $\Gamma(S)$ of order M^L, which satisfies the condition that no symmetry in G leaves an element of S unchanged. Therefore, the only generating group for $L \times$ MPSK is $(R_M)^L$. Fortunately, this generating group, which is also the most intuitive, is very useful for other applications, among them obtaining RI. A list of partitions for $(R_M)^L, L = 1, 2, 3, 4$ and $M = 4, 8, 16$, and an algorithm to find more partitions, can be found in [3]. Note that the definition of the GU partitions only relies on the group properties of the generating group and is independent of the way the isometries are defined. In particular, among the list of codes given in [4], those built over $(R_M)^L$ are GUE. As an example, a nonhomomorphic group code over $(Z_4)^3$ with 32 states from [4], shown in Fig. 3, is a GUE code. It encodes three bits into $3 \times$ QPSK symbols, i.e., a rate of 1 b/MPSK symbol.

VI. APPLICATION OF GUE CODES IN NONCOHERENT DECODING

In this section we will concentrate on the case of noncoherent decoders. A noncoherent decoder is a decoder designed to accept the received symbols demodulated by a free-running carrier reference and provide the output decoded data. It ignores the phase shift $\phi(t)$ of the channel, with the restriction that the phase is slowly varying (relative to the symbol rate). The noncoherent decoder is built under the assumption that we have no information about $\phi(t)$, except its slow variation. When some information is available about the phase, for example if $\phi(t)$ is the residual phase error of a phase-locked loop (PLL), then the resulting decoder is called partially coherent. Mathematically, noncoherent decoders imply the class of likelihood functions that are insensitive to a constant phase shift of the input.

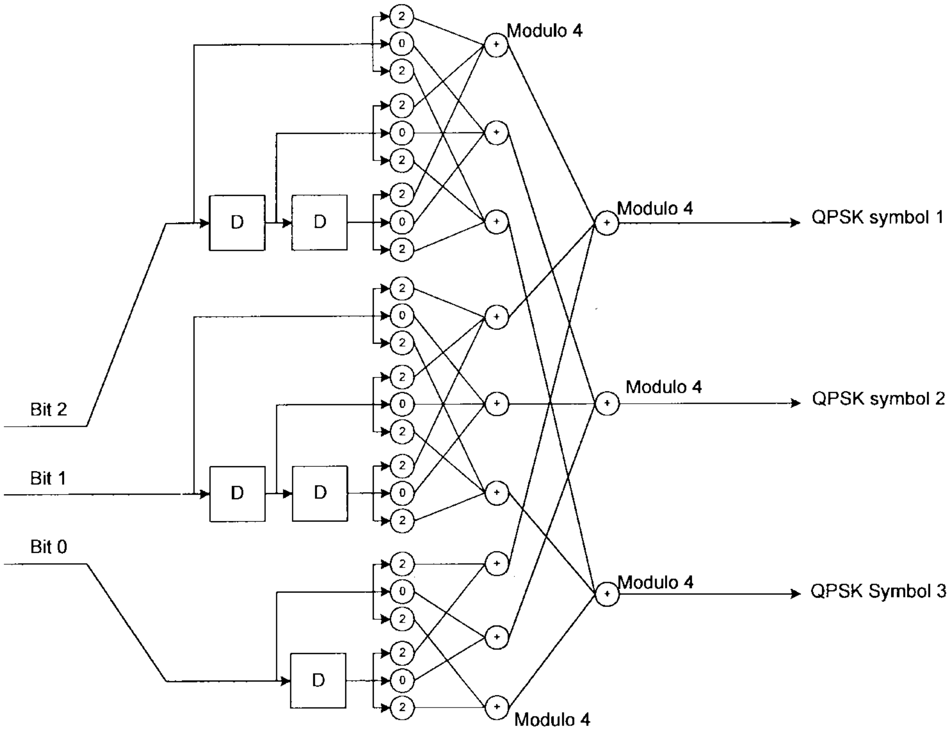

Fig. 3. An example of a high performance six-dimensional GUE code for 3 × QPSK modulation. Binary equivalent rate is 1/2.

Some coded modulations cannot be decoded noncoherently. First, if there are partitions of the signal set, there might be a symbol that is a phase shift of another symbol in the same partition. This case is easily solved by an appropriate scrambling (e.g., differential encoding) of the uncoded input symbol that select a point in the coset. Second, there are codes that are NC [13].

If the code is non-NC it is possible to decode the information without a phase reference by any decoder which uses all phase transitions in its decisions, like [8], [11], and [13]. Note that even in the case of PSK symbols, if the code is non-NC, differential encoding of the output symbols is not needed. Encoders with explicit differential encoding of the coded symbols are only a special case of non-NC encoders. A simple example for both NC and non-NC codes is shown in Fig. 5. The code in Fig. 5(b) is NC since a phase shift (in this case inversion) of a codeword produces a valid codeword, but with different (in this case inverted) corresponding encoded word. The code in Fig. 5(a) is non-NC since no phase shift of a codeword produces a valid codeword.

Examples to coded modulation suitable to noncoherent decoding, based on GUE structure, are given in Fig. 3 (which has already been mentioned) and Fig. 4. It is easy to verify by the help of the theorem to follow that these codes are non-NC. In Fig. 4 a code over Z_4 is matched to the isometric labeling of a four-way partition of 8-PSK (see [4, Fig. 1]). A rate 1/2 convolutional code over Z_4 chooses a partition of an 8-PSK symbol and an additional information bit, differentially encoded, chooses a point in the partition. No other differential encoding is necessary. A rate of 2 b/MPSK symbol is obtained. We evaluated the performance of these codes on AWGN using the noncoherent decoding technique of [13] in order to show the usefulness of the GUE codes to noncoherent decoding [14]. At the point $P_b = 10^{-5}$ and with observations (length of coherent integration) spanning three trellis branches, the degradation relative to coherent decoding of the code of Fig. 3 is only 0.5 dB. At the same conditions the degradation of the code of Fig. 4 is only 0.4 dB. Note that these codes are also optimal for coherent decoding, and in the coherent case achieves coding gain of 4.9 and 2.9 dB, respectively, where the coding gain is measured w.r.t. uncoded modulation carrying the same information rate.

In many *coherent* systems, RI codes are desired as a convenient solution to ambiguities in the carrier phase. RI codes are useful if they can be made to be rotationally transparent (RT) through suitable precoding of the input to the encoder. Definitions of these terms are found in [4]. In an RT code the overall code produces the same decoded symbols after a phase rotation at the channel. If the encoder is linear (homomorphic) over some group and minimal, differential precoding is the appropriate operation [4], [20]. Otherwise, for group codes, the suitable precoding is described in [22].

RI codes which are not RT are clearly NC [see, for example, Fig. 5(b)], but we will show that for a non-GUE code the converse may not be true. Let us define *partial* RI as the situation where the code is not RI to an angle θ but there still exists in the code at least one pair of codewords which differ by a constant phase shift θ. Clearly such situation can cause NC if these pairs are not decoded to the same information bits (see Fig. 6, for example). The following theorem shows that partial RI does not exist in GUE codes. Therefore, for GUE codes, the problem of NC can always be solved by precoding. In addition, it provides an easy test for NC.

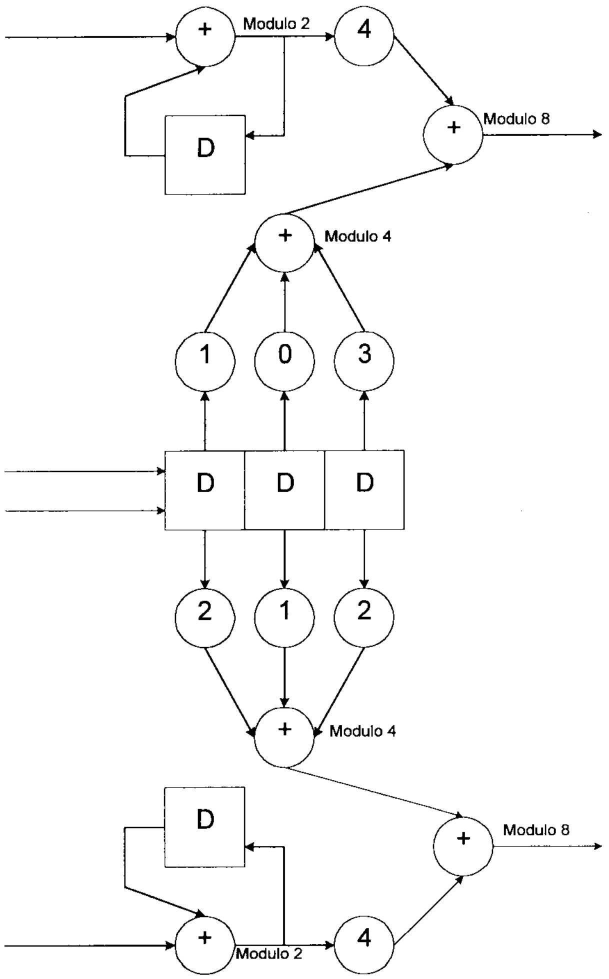

Fig. 4. A high performance GUE code for 2 × 8-PSK modulation having low degradation in noncoherent detection. Binary equivalent rate is 2/3.

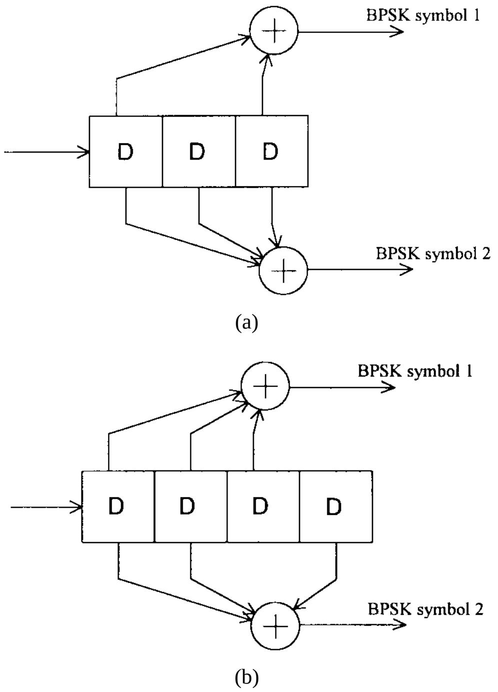

Fig. 5. (a) A non-NC convolutional code for BPSK modulation. (b) An NC convolutional code for BPSK modulation.

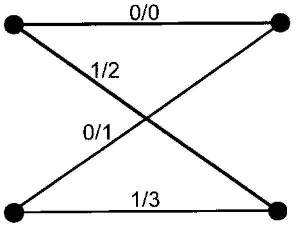

Fig. 6. A trellis section of a trellis-coded modulation code with rate 1/2 and QPSK (signals labels in a clockwise fashion). This code is not rotationally invariant, but it is partially rotationally invariant and also NC.

The inclusion of the differential precoder does not increase the number of states for ML sequence detection purposes. However, transparent codes may not be the optimal codes to be used with noncoherent decoding. There are two reasons for this statement. The first obvious reason is that the best code (for noncoherent decoding) may not be found to be RT. The second reason is that a noncoherent decoder will tend to suffer a larger degradation relative to a coherent one due to the inclusion of new types of error events. These additional error events are transitions from the transmitted codeword to the shifted version of it [13].

Theorem: If a pair of codewords in a GUE code differ in a constant phase shift θ then the code is RI to θ.

Proof: If the Cartesian product label map $\boldsymbol{m}$:$A^Z \rightarrow (S/S')^Z$ is an isometric labeling, then for all $\boldsymbol{a} \in A^Z$ there exists an isometry $u_{\boldsymbol{a}}$ such that

$$\boldsymbol{m}(\boldsymbol{a} \circ \boldsymbol{b}) = u_{\boldsymbol{a}}[\boldsymbol{m}(\boldsymbol{b})] \quad \forall\, \boldsymbol{b} \in A^Z \tag{12}$$

where '$\circ$' is the group operation of A extended to sequences. Let $\boldsymbol{x}, \boldsymbol{y} \in A^Z$ be two infinite length label sequences of two codewords α, β that differ in a constant phase shift θ. Let γ be an arbitrary codeword and $\boldsymbol{u}$ be its label sequence, i.e., $\gamma \in \boldsymbol{m}(\boldsymbol{u})$. Let $\boldsymbol{s} = \boldsymbol{x} \circ \boldsymbol{u}^{-1}$ and $\boldsymbol{v} = \boldsymbol{s}^{-1} \circ \boldsymbol{y}$, then by (12), $u_{\boldsymbol{s}}$ will bring $\boldsymbol{m}(\boldsymbol{u})$ to $\boldsymbol{m}(\boldsymbol{x})$ and $\boldsymbol{m}(\boldsymbol{v})$ to $\boldsymbol{m}(\boldsymbol{y})$. Since the pseudo-isometry preserves pseudo-distance, the set of pseudo-distances between all the points of $\boldsymbol{m}(\boldsymbol{u})$ and $\boldsymbol{m}(\boldsymbol{v})$ is the same as the set of pseudo-distances between all the points of $\boldsymbol{m}(\boldsymbol{x})$ and $\boldsymbol{m}(\boldsymbol{y})$. The pseudo-distance between α and β is $\rho(\alpha, \beta) = (e^{j\theta}, \cdots, e^{j\theta})$. Thus, there exists a codeword $\delta \in \boldsymbol{m}(\boldsymbol{v})$ with the same pseudo-distance to $\gamma \in \boldsymbol{m}(\boldsymbol{u})$, i.e., $\rho(\gamma, \delta) = (e^{j\theta}, \cdots, e^{j\theta})$. It is left to show that a pseudo-distance of $e^{j\theta}$ between two symbols s, s' is only possible when $s' = se^{j\theta}$. This is a result of the Schwartz inequality, and is easily proven by showing that $\|s' - se^{j\theta}\| = 0$. Therefore, RI to θ is satisfied. □

In particular, letting $\boldsymbol{u} = \boldsymbol{0}$ and assuming that the $\gamma = \{1, 1, \cdots, 1\}$ codeword exists and is in $\boldsymbol{m}(\boldsymbol{0}) = (S')^Z$, there exists the codeword $\delta = \{e^{j\theta}, e^{j\theta}, \cdots, e^{j\theta}\}$. We call this codeword *constant sequence*. The existence of a constant sequence is a simple check for RI.

VII. CONCLUSION

We have shown how to construct codes that have the UEP not only for coherent detection but also for a much wider class of detection techniques. A list of examples of various detection techniques demonstrates the generality and wideness of the defined correlation-based decoder. It was shown that the error probability of this decoder is a function of a pseudo-distance between the pairs of codewords. Using this pseudo-distance as the basis of the construction of geometrically uniform codes, we have created a framework for generating codes with the desired uniform error property. For M-ary PSK, codes over the group Z_M and its partitions with natural mapping are simple and useful example of such codes. When multidimensional modulations like $L \times$ MPSK are used, more interesting structures exist. The theorems described in this article are especially useful for the design of new coded modulation schemes that are designed to be decoded by the emerging class of noncoherent decoders using multiple-symbol observations. In particular, aspects of applying noncoherent decoding to GUE codes was addressed.

APPENDIX

The following construction for the matrix A_i in (10) will show its existence. Let us compose the $D \times M$ matrices

$$P = [\boldsymbol{a}_i^{(0)}, \boldsymbol{a}_i^{(1)}, \cdots, \boldsymbol{a}_i^{(M-1)}]$$
$$Q = [\boldsymbol{x}_i^{(0)}, \boldsymbol{x}_i^{(1)}, \cdots, \boldsymbol{x}_i^{(M-1)}].$$

Then, we should find A_i such that

$$P = A_i Q. \tag{13}$$

The relation (9) becomes

$$P^\dagger P = Q^\dagger Q. \tag{14}$$

We can make a singular value decomposition (SVD) to P and Q

$$P = U_P \Lambda_P V_P^\dagger, \qquad Q = U_Q \Lambda_Q V_Q^\dagger \tag{15}$$

where $U_{P,Q}$ are $D \times D$ orthonormal matrices, $\Lambda_{P,Q}$ are $D \times D$ diagonal matrices with positive or zero elements (the singular values) and $V_{P,Q}$ are column orthonormal $M \times D$ matrices. The decomposition is unique up to (1) the ordering of the singular values (2) forming linear combinations of columns of U and V whose corresponding singular values are equal. Using (14) we obtain

$$P^\dagger P = V_P \Lambda_P^\dagger \Lambda_P V_P^\dagger = V_Q \Lambda_Q^\dagger \Lambda_Q V_Q^\dagger = Q^\dagger Q. \tag{16}$$

Hence, Λ_P and Λ_Q are the square root of the diagonal eigenvalues matrix of the same Hermitian matrix, and are equal up to the order of the eigenvalues. Since the ordering of the singular values are free, we can choose them to be equal, i.e., $\Lambda_Q = \Lambda_P$. The columns of V_Q and V_P as eigenvectors of the same matrix are unique up to the case of equal eigenvalues. In the latter case, a linear combination of columns is possible, the same as in the SVD decomposition. Hence it is possible to choose $V_Q = V_P$. Now we can set $A_i = U_P U_Q^\dagger$ and one can verify that (13) is satisfied.

ACKNOWLEDGMENT

It is a pleasure for me to acknowledge Dr. D. Divsalar for reviewing this manuscript and for his helpful comments and suggestions.

REFERENCES

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

[2] G. D. Forney, "Geometrically uniform codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 1241–1260, Sept. 1991.

[3] S. Benedetto, R. Garello, M. Mondin, and G. Montorsi, "Geometrically uniform partitions of $L \times$ MPSK constellations and related binary trellis codes," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1773–1798, Nov. 1993.

[4] ———,, "Geometrically uniform TCM codes over groups based on $L \times$ MPSK constellations," *IEEE Trans. Inform. Theory*, vol. 40, pp. 137–152, Jan. 1994.

[5] S. Benedetto, M. A. Marsan, G. Albertengo, and E. Giachin, "Combined coding and modulation: Theory and applications," *IEEE Trans. Inform. Theory*, vol. 34, pp. 223–236, Mar. 1988.

[6] M. K. Simon, M. S. Hinedi, and W. C. Lindsey, *Digital Communication Techniques, Signal Design and Detection*. Englewood Cliffs, NJ: Prentice-Hall, 1995.

[7] E. Biglieri, D. Divsalar, P. J. McLane, and M. K. Simon, *Introduction to Trellis Coded Modulation with Applications*. New York:Macmillan,1991.

[8] D. Makrakis, P. T. Mathiopoulos, and D. P. Bouras, "Optimal decoding of coded PSK and QAM signals in correlated fast fading channels and AWGN: A combined envelope, multiple differential and coherent detection approach," *IEEE Trans. Commun.*, vol.42, pp.63–75, Jan. 1994.

[9] D. Divsalar and M. K. Simon, "Multiple-symbol differential detection of MPSK," *IEEE Trans. Commun.*, vol. 38, pp. 300–308, Mar. 1990.

[10] D. Makrakis, K. Feher, "Optimal noncoherent detection of PSK signals," *Electron. Lett.*, vol. 26, pp. 398–400, Mar. 1990.

[11] D. Divsalar, K. M. Simon, and M. Shahshahani, "The performance of trellis-coded MDPSK with multiple symbol detection," *IEEE Trans. Commun.*, vol. 38, pp. 1391–1403, Sept. 1990.

[12] H. Leib and S. Pasupathy, "Optimal noncoherent block demodulation of differential phase shift keying (DPSK)," *AEU*, vol. 45, no. 5, pp. 299–305, Sept. 1991.

[13] D. Raphaeli, "Noncoherent coded modulation," *IEEE Trans. Commun.*, vol. 44, pp. 172–183, Feb. 1996.

[14] Y. Tsudkevich and D. Raphaeli, "Noncoherent decoding of geometrically uniform trellis codes," M.Sc. thesis, Tel Aviv Univ., Tel Aviv, Israel, 1996.

[15] J. L. Massey, T. Mittelholzer, T. Riedel, and M. Vollenweider, "Ring convolutional codes for phase modulation," *Int. Symp. Information Theory*, San Diego, CA, Jan. 1990.

[16] H.-A. Loeliger, "Signal set matched to groups," *IEEE Trans. Inform. Theory*, vol. 37, pp. 1675–1682, Nov. 1991.

[17] G. D. Forney Jr. and M. D. Trott, "The dynamics of group codes: State spaces, trellis diagrams, and canonical encoders," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1491–1513, Sept. 1993.

[18] D. Raphaeli, "Uniform error linear coded modulation for noncoherent channels," in *Conf. Information Sciences and Systems*, Princeton, NJ, Mar. 1994, pp. 650–655.

[19] J. G. Proakis, *Digital Communications*. New York: McGraw-Hill, 1989.

[20] L. F. Wei, "Rotationally invariant trellis-coded modulations with multidimensional M-PSK," *IEEE J. Select. Areas Commun.*, vol. 7, pp. 1281–1295, Dec. 1989.

[21] S. S. Pietrobon, R. H. Deng, A. Lafanechere, G. Ungerboeck, and D. J. Costello, "Trellis-coded multidimensional phase modulation," *IEEE Trans. Inform. Theory*, vol. 36, pp. 63–89, Jan. 1990.

[22] S. Benedetto, R. Garello, M. Mondin, and M. D. Trott, "Rotational invariance of trellis codes—Part I and II," *IEEE Trans. Inform. Theory*, vol. 42, pp. 751–778, May 1996.

Dan Raphaeli (M'92) was born in Israel in 1967. He received the B.Sc. degree in electrical and computer engineering from Ben Gurion University, Israel, in 1986, and the M.S. and Ph.D. degrees in electrical engineering from the California Institute of Technology, Pasadena, CA, in 1992 and 1994, respectively.

From 1986 to 1991 he was a Research Member at the Electronic Research Institute of the Israel Defense Ministry. From 1992 to 1994 he was a Research Scientist at the Jet Propulsion Laboratory, Pasadena, CA, where he was involved in the design of the communication subsystems of future spacecrafts, including the Advanced Transponder studies. Since 1994 he has been an Assistant Professor with the Department of Electrical Engineering Systems, Tel Aviv University, Tel Aviv, Israel. His research subjects include digital modulation and demodulation, coding and decoding algorithms, spread spectrum, mobile communication, satellite communication, synchronization, equalization, and digital signal processing.