CODING AND MODULATION FOR THE GAUSSIAN CHANNEL,
IN THE ABSENCE OR IN THE PRESENCE OF FLUCTUATIONS

CODAGE ET MODULATION POUR LE CANAL GAUSSIEN,
SANS OU AVEC FLUCTUATIONS

Gérard Barmat, Hélène Magalhães de Oliveira and Zhang Weidong

École Nationale Supérieure des Télécommunications,
Département Communications (also URA 850 of C.N.R.S.)
46 rue Barrault, 75634 PARIS CEDEX 13, France

Abstract

Looking for systems which combine coding and multilevel modulation whose Euclidean distance distribution is close to that which results in the average from random coding, we consider the combination of an MDS code over a large-size alphabet and a one-to-one mapping of the alphabet into a symmetric constellation e.g., phase modulation. Its performance in the presence of additive Gaussian noise can be predicted from that of random coding, provided the signal-to-noise ratio is small enough. The results exhibit the sphere hardening phenomenon whether or not amplitude fluctuations are present. Weighted demodulator output and soft decoding should be effected in order to achieve this performance. Such decoding can be done in principle according to previous works by Fang and Barmat. A prohibitive complexity can be avoided only at the expense of strict optimality.

INTRODUCTION AND SUMMARY OF RESULTS

We were recently led to question the relevance of the minimum distance criterion when applied to long block codes i.e., where many errors are likely to occur in each codeword [1]. As a better criterion, we proposed a proximity measure of the code distance distribution with respect to that which results in the average from random coding. The criterion of the minimum distance criterion, as well as the proposed one, were formulated in the case of the Hamming distance, but they are also valid for the Euclidean metric.

Systems which combine coding and multilevel modulation e.g., trellis-coded modulations to be used over the narrow-band Gaussian channel [2], were designed for the Euclidean metric which is natural for this channel but they used the minimum distance criterion. We found it interesting to consider coded-modulation systems whose Euclidean distance distribution is good according to our own criterion.

Looking for such a system, we first notice that the distance distribution of the maximum-distance-separable codes (MDS), a class which especially includes the Reed-Solomon codes, is close
to that which results in the average from random coding if the alphabet size and the code dimension are large [3]. Therefore, these codes are good according to our criterion, as far as the Hamming distance is concerned. In order to define a coded-modulation system using these codes whose Euclidean distance distribution meets our criterion, we must define the mapping of the code symbols into a constellation.

Let us consider a system using an MDS code over a large-size alphabet (whose cardinality is denoted by $q$), associated with a symmetric constellation of same size. We are specially interested in the case of phase modulation because of its robustness against non-linearities and amplitude fluctuations. Let first the mapping of the code symbols into this constellation be random and vary according to the position in the word.

The distance distribution of MDS codes and the random character of the mapping of the code symbols into the constellation result in a distribution of the Euclidean distances close to that obtained using random coding and nonrandom mapping, provided the alphabet size and the code dimension are large enough. Furthermore, the Euclidean distance distribution is not actually modified if the mapping from the code alphabet to the constellation is nonrandom and does not vary with the symbol position. Performance close to that of random coding may thus be expected from this fully deterministic scheme (we already arrived at a similar conclusion via a different approach [4], but the coded-modulation system here is completely explicit). Decoding is much less complex, however, than if random coding were used. Moreover, in the case of phase modulation, this scheme easily achieves rotational invariance in order to cope with an arbitrary phase reference, unlike trellis-coded modulation.

The performance thus obtained can be predicted from that of random coding, using an expansion of Shannon's results [5], provided that the signal-to-noise ratio is small enough (in the range where coding is actually useful). The availability of tables is very helpful for literal computations and, of course, numerical results are easily obtained using digital computers.

These results, as expected, exhibit the "sphere hardening" phenomenon: for a large enough signal-to-noise ratio, the word error probability is extremely small; if the SNR decreases, it increases suddenly and approaches 1. This transition is the steeper, the larger the number of dimensions. It occurs at an SNR close to $2^C - 1$, where $C$ is the channel capacity in binary units. This behaviour is observed whether or not amplitude fluctuations are present.

Achieving such performance actually demands that maximum likelihood decoding be employed. In other words, the point representing a codeword to be chosen is the closest to the one which represents the received signal (according to the Euclidean distance). Weighted demodulator output and soft decoding are thus necessary. The algorithm of Feng and Bello enables optimum soft decoding of nonbinary linear codes e.g., Reed-Solomon ones [6-8]. However, a prohibitive complexity can be avoided only by limiting the maximum number of candidate words tried for decoding each received word, at the expense of strict optimality. Another problem which needs further work is quantization in the received signal space.
OUTLINE OF A COMMUNICATION SYSTEM USING MDS CODES

In general, MDS codes need not be linear. However, the most important members of the family i.e., Reed-Solomon (RS) and generalized RS codes, are linear, so that we may restrict ourselves to linear codes. Then, the distance distribution reduces to the weight distribution.

The weight distribution of an MDS code over the field of q elements can be found in many textbooks and is recalled in [3]. Let n be the code length and k its dimension, then the number $A_j$ of words of Hamming weight j is:

$$A_0 = 1,$$

$$A_i = 0, \quad 0 < i < n-k+1,$$

$$A_j = \sum_{i=0}^{n-j} (-1)^i (q^{j-i-(n-k)} - 1), \quad n-k+1 \leq j \leq n. \quad (1)$$

Interestingly, for given values of n and k, this weight distribution is uniquely determined by the fact the code is MDS.

Equality (1) can be rewritten as

$$A_j = q^{j-(n-k)} \sum_{i=0}^{n-j} (-1)^i (q^{j-i-(n-k)} + \sum_{i=0}^{j-1-(n-k)} (-1)^i (q^{j-i-(n-k)})). \quad (2)$$

The first term of the right hand side is the average weight which results from the random choice of $q^k$ q-ary n-tuples. We shall assume in the remainder of this paper that the second term is negligible with respect to the first one at least for the largest values of $A_j$, which occurs if q and k are large enough.

The Hamming distance distribution is then close to that which results from random coding, so the MDS code is not only good according to the conventional criterion (since it achieves the largest possible minimum distance $d = n-k+1$) but also according to the one which we proposed [1].

Notice that the choice of an MDS code limits the word length to a maximum equal to $q+1$, except if $q$ is even and $k$ or $n-k=3$, in which case the maximum length equals $q+2$, if we accept the MDS conjecture [9]. In any case, the maximum code length is close to the alphabet size. Therefore, the use of a long code also means that of a large alphabet which, according to (2), results in a distance distribution close to that of random coding for reasonable values of $k$.

Let us assume that the q-point constellation to be used is symmetric in the sense that the Euclidean distance distribution between some of its points and the other ones does not depend on the point considered (e.g., phase modulation i.e., in 2 dimensions, the set of points on a circle at angles $2\pi x/q$ with respect to the x axis, $x$ an integer such that $0 \leq x \leq q-1$). In order to define the mapping from the code alphabet into the points of this constellation, let us first assume that symbol 0 is
mapped into the point labelled 0 in the constellation, while the other symbols are one-to-one mapped into the other points at random, and differently at each position in the word.

Let us define the Euclidean weight as the squared Euclidean norm, an additive quantity. Consider the Euclidean weight distribution of the combination of MDS coding with the mapping just defined. The closeness of the Hamming weight distribution (2) to the average random weight results in a number of zero Euclidean weights close to that which would have been obtained in the average by random coding and any deterministic mapping. The use of a random and varying mapping for the nonzero symbols further results in a Euclidean weight distribution close to that which would result in the average from random coding where each point of the constellation is chosen at random, independently from the previous choices, at each of the $n$ symbol positions in the word and where $q^k$ words are so chosen, independently from each other, as the codebook.

If now we assume that the one-to-one mapping of the code alphabet into the constellation is non-random and does not vary with the symbol position, the exact computation of the Euclidean distance distribution appears as a very difficult problem but statistical simulation can be used to estimate it. For instance, we considered Reed-Solomon codes over GF(16), with $n = 15$. A large number of information vectors were obtained by random choice of each of their $k$ components with uniform probability over GF(16). Each of these vectors was encoded according to the code already defined. We assumed either a random and variable mapping of the code alphabet into the 16-point phase modulation constellation, either an arbitrary mapping common to all positions, or the "natural" mapping of the symbols 0, $1, \alpha, \alpha^2, \cdots, \alpha^{14}$ into the angles $0, \pi/8, 2\pi/8, \cdots, 15\pi/8$, respectively ($\alpha$ denotes a primitive element of GF(16)). Whatever the mapping chosen, it remained the same for all words. The Euclidean weight corresponding to each word was computed and a histogram of the weights was drawn. A sample of results thus obtained is given in Figure 1. Although $q$ and $k$ are only moderately large, the Euclidean weight distribution thus obtained appears very close to that of random coding.

Figure 1. Squared Euclidean distance distribution of the combination of the (15,8) Reed-Solomon code over GF(16) with 16-phase modulation.

The mapping of the alphabet symbols into the 16 phases was: (1) random and varying with the symbol location; (2) random but the same for all symbols; (3) deterministic. For comparison purpose, the squared distance distribution of randomly chosen 15-uples was also drawn (4). The curves show a histogram where 100,000 words were classified into 100 equally spaced intervals of the full range of possible Euclidean distances. The points are too close to each other to be separated on the graph.
These results also show that almost no change in the Euclidean distance distribution results if the one-to-one mapping of the code alphabet into the constellation is nonrandom and does not vary with the symbol position. Besides the evidence provided by simulation, we believe this statement is true, although we are unable to exhibit a formal proof of it. In brief, this would result from the many symmetries of the MDS codes, which mimic the average regularity of randomness.

**PERFORMANCE PREDICTION USING RANDOM CODING**

We defined in the previous section a nonrandom coded-modulation system where the Euclidean distance distribution is close to that of random coding i.e., which constitutes some discrete approximation of the random coding without any restriction to a finite alphabet, as studied by Shannon [3]. If the average length of the noise vector is large with respect to the average distance between the points of the constellation i.e., if the signal-to-noise ratio is small enough, the discrete location of the signal points may be ignored and Shannon results provide an estimate of the performance the system can achieve.

**Average error probability**

Consider random coding where \( M \) points are chosen at random in an \( n \)-dimensional Euclidean signal space, with uniform density inside the hypersphere corresponding to a limited power, in the presence of additive Gaussian noise. Its exact average error probability was computed by Shannon [5], resulting in:

\[
P_e = 1 + \int_0^{\pi} \left( 1 - \omega_n(\theta) \right)^{M-1} Q_n(\theta) \, d\theta,
\]

(3)

where:

\( Q_n(\theta) \) is defined as the probability that the point which represents the received signal is moved by the noise outside a cone with vertex at the origin, whose axis is colinear with the transmitted vector and whose half-angle is denoted by \( \theta \). We notice that the derivative of \( \Omega_n(\theta) \), denoted by \( Q_n(\theta) \), is negative:

\[
\omega_n(\theta) = \Omega_n(\theta) / \Omega_n(\pi), \quad \text{where} \quad \Omega_n(\theta) \text{ is the solid angle of this cone i.e.,}
\]

\[
\Omega_n(\theta) = C(n) \int_0^\theta \sin^{n-2} x \, dx,
\]

(4)

where \( C(n) \) does not depend on \( \theta \).

We rewrite (3) as

\[
P_e = 1 - \int_0^{\pi} P_n(R;\theta) G_n(\rho;\theta) \, d\theta
\]

(5)
where

\[ F_n(R; \theta) = (1 - \omega_n(\theta))^{\Delta n^{-1}}, \tag{6} \]

where \( R = \frac{1}{n} \ln(M) \) is the information rate per dimension (in nats), and

\[ \Delta \]

\[ C_n(p; \theta) = -C_n^*(p; \theta) \tag{7} \]

where \( p = S/N \) is the channel signal-to-noise ratio. Both factors depend on the number of dimensions \( n \). The first one does not depend on the noise but on the number \( M \) of codewords. According to the above definition, it can be expressed in terms of the rate \( R \), which therefore was written in argument of \( F_n \) in (6). The second factor does not depend on the code but on the channel noise. We now examine each of these two factors.

First factor of the integrand in (5)

The integral in (4) can explicitly be found in [10], which results in:

\[ \omega_n(\theta) = \frac{1}{\pi} \left[ 0 + 2 \sum_{i=0}^{n-2} (-1)^{n-2-i} \frac{C^{i}_{n-2}}{C^i_{n-2}} \sin((n-2i-2)\theta) \right], \quad n \text{ even,} \tag{8a} \]

\[ \omega_n(\theta) = \frac{1}{2} \left[ 1 - \sum_{i=0}^{\lfloor (n-2)/2 \rfloor} (-1)^i \frac{C^{i}_{n-2}}{C^i_{n-2}} \frac{\cos((n-2i-2)\theta)}{n-2i-2} \right], \quad n \text{ odd.} \tag{8b} \]

These expressions are exact. If we look for an approximation of \( F_n(R; \theta) \), we may write \( \theta = \sin^{-1}(z) \) and \( \omega_n(\sin^{-1}(z)) = a_{n-1} z^{n-1} + \epsilon z^n, \) where \( \epsilon \) approaches 0 as \( \theta \) vanishes. The first nonzero term \( a_{n-1} z^{n-1} \) is actually the dominant term of a series which converges provided \( x < 1 \) i.e., for any \( \theta < \pi/2 \).

If we furthermore neglect 1 with respect to \( M \), we may write:

\[ F_n(R; \theta) \approx (1 - a_{n-1} \sin^{n-1}(\theta))^{\Delta n^{-1}}. \]

From (8a) and (8b) it results that

\[ a_{n-1} = \frac{2}{\pi(n-1)!} \sum_{i=0}^{n-2} (-1)^i \frac{C^{i}_{n-2}}{C^i_{n-2}} (n-2i-2)^{n-2}, \quad n \text{ even,} \]

\[ a_{n-1} = \frac{1}{2(n-1)!} \sum_{i=0}^{\lfloor (n-2)/2 \rfloor} (-1)^i \frac{C^{i}_{n-2}}{C^i_{n-2}} (n-2i-2)^{n-2}, \quad n \text{ odd.} \]
It can be shown, using Euler's gamma function, that:
\[
a_n = \frac{2^{n-1} \Gamma^2(n/2)}{\pi \Gamma(n)},
\]
(9) regardless of the parity of \(n\).

For \(n\) large enough, Stirling formula results in:
\[
a_n \approx 1/\sqrt{2\pi n},
\]
(10) so we have
\[
F_n(R, \Theta) = \exp \left( -\frac{\exp[n(R + \ln(\tan\Theta))]}{\sin\Theta \sqrt{2\pi n}} \right). \tag{11}
\]
For large \(n\) this function varies fast as \(\Theta\) increases, from nearly 1 to nearly 0, near the angle such that the argument in (11) equals 1:
\[
\Theta = \sin^{-1}([2\pi n]^{1/2} \exp(-2\pi n/(n-1))). \tag{12}
\]
If we let \(n\) approach infinity, \(F_n(R, \Theta)\) becomes a step function with its transition at
\[
\Theta_R = \sin^{-1}(-\exp(-R)). \tag{13}
\]
a result already obtained by Shannon [5].

Second factor of the integrand in (5)

Shannon [5] has shown that
\[
Q_n(\Theta) = P(n-1, \sqrt{n \sin(N/n), \sqrt{n-1 \cos(\Theta))}, \tag{14}
\]
where \(S\) and \(N\) denote the average power of signal and noise, respectively, and \(P(\cdot, \cdot)\) denotes the non-central \(t\)-distribution i.e.,
\[
P(m, a, t) = \Pr \left( |Z + a| \leq t \sqrt{\frac{1}{m} \sum_{i=1}^{m} x_i^2} \right), \tag{15}
\]
where \(z\) and \(x_i\), \(1 \leq i \leq m\), are mutually independent Gaussian random variables, with zero mean and variance 1; \(a\) and \(t\) are constant parameters.

**Absence of amplitude fluctuations**

We first assume the received signal amplitude is constant. The variable \(r\) defined as
\[
r = n^{-1/2} \sqrt{\sum_{i=1}^{m} x_i^2}
\]
has a \(\chi^2\) distribution i.e., its density is
\[
p_r(r) = \frac{m^{m/2}}{2^{m/2} \Gamma(m/2)} r^{m-1} \exp(-mr^2/2). \tag{16}
\]
Using this density to express the probability in (15) results in:

$$P(a, u, \theta) = \int_0^1 \rho_a(u) \, du,$$

(17)

where the following expression of \( \rho_a(u) \) can be found with the help of (10):

$$\rho_a(u) = \frac{(\frac{\mu^2}{2})^{\frac{n-1}{2}} \exp\left(-\frac{\mu^2}{2}\right)}{(u^2+n-1)^{\frac{n-1}{2}} \sqrt{n}} \sum_{i=0}^m b_i u^i,$$

(18)

where \( u = \sqrt{n} \frac{\mu}{\sqrt{2(n^2+n-1)}} \). The coefficients of the series are:

$$b_0 = \frac{\Gamma\left(\frac{n}{2}\right)}{\Gamma\left(\frac{n-1}{2}\right)} \quad b_1 = n-1 \quad b_2 = \frac{n+1}{2} \quad \ldots$$

(19)

and, for \( m \) a positive integer:

$$b_{2m} = b_0 \cdot \frac{(n+2)(n+4) \cdots (n+2m-2)}{1.3.5 \cdots (2m-1)} \frac{1}{m!} = \frac{b_{2m-1} n+2m-2}{m(2m-1)},$$

$$b_{2m+1} = b_1 \frac{(n+1)(n+3)(n+5) \cdots (n+2m-1)}{3.5.7 \cdots (2m+1)} \frac{1}{m!} = \frac{b_{2m} n+2m-1}{m(2m+1)}.$$

We thus may write

$$Q_n(\theta) = \int_{-\infty}^{\infty} \rho_a(u) \, du$$

(20)

and

$$G_a(p; \theta) = -\frac{Q_n(\theta)}{Q_n(\theta)} = \sqrt{n-1} (1 + \cos^2 \theta) \rho_a(\sqrt{n-1} \cos \theta).$$

(21)

For \( n \) large enough, the density (16) can be approximated by the Gaussian density which has same mean \( \mu \) and variance \( v \). These are shown to be:

$$\mu = \sqrt{\frac{2}{n-1}} b_0,$$

(22)

where \( b_0 \) is given by (19), and

$$v = 1 - \mu^2.$$

(23)

Applying Stirling formula to (19) shows that \( b_0 \) varies approximately as \((1 - 3/4n) \sqrt{n/2}\), so the corresponding values of \( \mu \) and \( v \) are \( \mu = (1 - 1/4n) \) and \( v = 1/2n \). Thus, as \( n \) approaches infinity, \( \mu \) approaches 1 and \( v \) vanishes.

Replacing (16) by its Gaussian approximation transforms (18) into:

$$\rho_a(u) = \frac{1}{2\pi \sqrt{v}} \exp\left(-\frac{\mu^2}{2v} - \frac{u^2}{2} \right) \frac{1}{\mu^2 + 1/\nu} +$$

(24)
\[
+ \frac{1}{\sqrt{\pi \nu}} \left( \frac{\alpha \mu + \nu}{2(\alpha^2 + 1/\nu)} \right)^{1/2} \exp\left\{ - \frac{\pi - \mu}{2(\alpha^2 + 1/\nu)} \right\} \frac{\left( \frac{\alpha \mu + \nu}{2(\alpha^2 + 1/\nu)} \right)^{1/2}}{\sqrt{2(\alpha^2 + 1/\nu)}}.
\]

An approximation of the factor \( G_p(p;0) \) results by substituting (24) for \( p_a(n) \) in (17) and (14). Its maximum occurs at approximately

\[
\theta_2 = \tan^{-1} \left( \frac{\sqrt{n-1}}{\sqrt{np}} \right) = \tan^{-1} \left( \theta_0 \sqrt{\frac{2}{np}} \right)
\]

and its variance is equal to:

\[
\nu_2 = \frac{(n-1)(\beta\sigma + \mu^2) + \mu^2}{((n-1)i\mu^2 + np)^2} = \frac{1}{(2b_0^2 + np)^2} - \frac{a(n-1)p - 2b_0^2(np-1)}{(2b_0^2 + np)^2}.
\]

As \( n \) approaches infinity, the factor \( G_p(p;0) \) becomes the Dirac density \( \delta(0 - \theta) \), since its variance vanishes and

\[
\theta_2 \to \tan^{-1} \left( \frac{1}{\sqrt{S/N}} \right) = \sin^{-1} \left( \frac{1}{\sqrt{1 + S/N}} \right) = \theta_C.
\]

The angle \( \theta_C \) is thus such that

\[
\sin(\theta_C) = \exp(-C),
\]

where \( C = \frac{1}{2} \ln(1 + S/N) \) is the channel capacity, expressed in bits per dimension. If \( \theta_2 > \theta_C \), where \( \theta_n \) is given by (13) (which obviously implies \( R < C \), then according to (3) the error probability vanishes. On the other hand, it approaches 1 if \( \theta_2 < \theta_C \) (or \( R > C \)).

**Presence of amplitude fluctuations**

In the presence of amplitude fluctuations, the parameter \( a \) in (15) becomes a random variable. We shall only consider the case where we assume plane constellations, with the signal amplitude distributed according to the Rayleigh density. Moreover, we assume perfect interleaving in the sense that the amplitudes associated with the symbols of a code word are mutually independent random variables.

We then have \( n = 2i \), where \( i \) is the code length, and the probability density of \( a \) is:

\[
p_a(a) = \frac{1}{2^{i-1}i^2 \Gamma(i)} \ a^{2i-1} \ \exp(-a^2/2i) \ .
\]

where \( \rho \) denotes the average signal-to-noise ratio, so the error function becomes, instead of (14):

\[
Q_a(0) = \int_0^\infty p(n-1, \ a, \sqrt{n-1} \ \text{c.d.f.}) \ \frac{2^{i-1} \ 
\ a^{2i-1} \ / \Gamma(i) \ \exp(-a^2/2i) \ \text{d}a.
\]

The mean and variance of the random variable \( a \) are:

\[
\mu_a = \int_0^\infty \frac{\Gamma(i+1/2)}{\Gamma(i)} \ a \sqrt{2i} \ \sqrt{2} \ = \ \frac{(2i-1) \ \sqrt{2}}{\sqrt{2} \ b_0},
\]

\[
\sigma_a^2 = \int_0^\infty \frac{\Gamma(i+1/2)}{\Gamma(i)} \ a^2 \sqrt{2i} \ \sqrt{2} \ = \ \frac{(2i-1) \ \sqrt{2}}{\sqrt{2} \ b_0}.
\]
and

\[ v_n = 2 \rho \left[ 1 - \frac{1}{4} \left( \frac{t + 1/2}{\sqrt{t}} \right) \right] = 2 \rho \left( \frac{2t - 1}{4 \Delta_0} \right)^2. \]

(32)

where \( \Delta_0 \) is given by (19), with \( n = 2t \).

As \( n \) grows indefinitely, \( v_n \) vanishes and the density (29) approaches a Dirac density at \( \eta = \sqrt{2t} \rho \), i.e., the same as in the absence of fluctuations. The same asymptotic behavior as already described thus occurs, whether or not fluctuations are present.

All these results have been summarized in Figure 2, which shows the first factor in (5) \( F_n(R, \theta) \) as given by its approximation (11) and the second one \( G_n(\rho, \theta) \) computed according to (21) in the absence of fluctuations or numerically computed in the presence of Rayleigh fluctuations.

![Figure 2. First and second factor in the integrand of equality (5).](image)

**Figure 2.a.** The number of dimensions of the signal space is \( n = 16 \). The first factor (1) was plotted for \( R = \ln 2 \); the second one for SNR = 6.0 dB with no fluctuations (2) and with Rayleigh fluctuations (3). Since the capacity is larger than the rate \( R \), the integral of the product of the factors is close to 1 and thus the error probability is small. The angle \( \theta \), in radians, was plotted on the x-axis.

**Figure 2.b.** Same as Fig. 2.a except that the number of dimensions is now \( n = 64 \).
WEIGHTED DECODING OF MDS CODES

The conventional hard decoding of codes does not take into account the Euclidean distance of the signal representing the codeword with respect to the received signal. No loss of information would result only if weighted decoding is performed i.e., which takes into account the a priori probabilities of the symbols (which is equivalent to use the Euclidean metric).

We already described an algorithm for the optimum weighted decoding of linear block codes [6, 7]. It can be thought of as a kind of sequential decoding but the finite context of blocks avoids the overflow problems encountered with convolutional codes. Although binary codes were mainly considered in [6, 7], the algorithm can be extended to deal with nonbinary codes. This case was studied with more detail in [8], assuming some preliminary quantization of the received signal space in order to convert the actually continuous (e.g., Gaussian) channel into a discrete one.

Let us denote by \( A \) and \( B \) the channel input and output alphabets, respectively, with \( \text{card}(A) = q < \text{card}(B) = Q \). We may assume that \( B \) results from quantization of the continuous channel output. The channel is then characterized by the \( qQ \) transition probabilities \( \Pr(b_j|a) \) that \( b_j \in B \) is received when \( a_j \in A \) is transmitted.

We define the hard decision \( h(j) \) on \( b_j \) as the symbol of \( A \) such that

\[
\Pr(b_j|h(j)) = \max_{a \in A} \Pr(b_j|a) \tag{33}
\]

and introduce the non-negative quantities

\[
v(a, b_j) = \log[\Pr(b_j|h(j))] - \log[\Pr(b_j|a)], \tag{34}
\]

where the logarithms are to an arbitrary base.

Now, if \( e^i \in A^n = [e_1^i \cdots e_n^i] \) denotes the \( i \)-th codeword and \( r \in B^n = [r_1 \cdots r_n] \) denotes a received vector, the generalized distance of \( r \) and \( e^i \) is defined as

\[
Z(r, e^i) = \sum_{j=1}^{n} v(r_j, e^i_j) \tag{35}
\]

Let us assume that the code is in systematic form. Since the generalized distance is additive with respect to the symbols, we may write (35) as the sum of two terms namely

\[
Z(r, e^i) = Z_v(r, e^i) + Z_c(r, e^i), \tag{36}
\]

where \( Z_v(r, e^i) \) is the contribution of the information symbols and \( Z_c(r, e^i) \) that of the check symbols. Optimum decoding consists of determining \( i^* \) such that \( Z(r, e^{i^*}) < Z(r, e^i) \) for any \( i \neq i^* \). \( Z_v(r, e) \) is immediately determined once the information vector \( u \) corresponding to \( e \) is given. On the other hand, \( Z_c(r, e) \) can be obtained only after the check symbols of \( e \) are computed i.e., after \( u \) has been encoded. The algorithm is designed in order to minimize the number of encodings necessary to determine \( i^* \).
The received symbols are first reordered by decreasing reliability of the corresponding hard decisions. The first $k$ symbols after reordering are taken as the information symbols, which is always possible for MDS codes. The vector $\mathbf{r}^b = (r_1^b \cdots r_k^b)$ determines at first codeword $c^b$ such that $Z_0(r, c^b) = 0$. Encoding $\mathbf{r}^b$ enables computing $Z(r, c^b)$ according to (36) and a threshold is set at this value. Now, other information vectors $\mathbf{r}^a$, corresponding to code vectors $c^a$, are tried in the order of increasing $Z_0(r, c^a)$ and the corresponding $Z(r, c^a)$ is computed. If $Z(r, c^a)$ is found for some $c^a$ smaller than the current threshold, then the new one is set to this value. The corresponding codeword $c^a$ becomes the last provisional candidate to optimum decoding. The provisional candidate becomes the finally decoded word when the next $Z_0(r, c^a)$ exceeds the current threshold.

The complexity of this algorithm is small in the average, but exactly optimum decoding can result in a large amount of computation for certain (unfrequently met) received vectors. Therefore, suboptimum decoding should be preferred in any practical situation. It can result from stopping to try codewords before it becomes sure that the best one was found.

CONCLUSION

It is known that MDS codes are good. It is our opinion that they are still better than currently believed and that, when combined with a proper multilevel modulation, they can behave very similarly to random coding, thus closely approaching the capacity of the channel. The key to their efficient use is weighted decoding since it can approach maximum likelihood decoding which chooses the signal point closest to the received one according to the Euclidean metric. Complexity can be kept reasonable only at the expense of strict optimality.

Although the principles of such weighted decoding has already been elaborated, some work remains to be done before truly usable algorithms can be designed. For instance, proper quantization of the received signal space should provide an acceptable compromise between complexity and performance degradation. We hope that the prediction of achievable performance presented in this paper will prompt research in this direction.

References


