[6] P. Swerling, "Recent developments in target models for radar detection analysis," in *AGARD Avionics Tech. Symp. Proc.*, Istanbul, Turkey, May 1970.
[7] R. L. Mitchell and J. F. Walker, "Recursive methods for computing detection probabilities," *IEEE Trans. Aerospace Electron. Syst.*, vol. AES-7, pp. 671–676, July 1971.
[8] M. Abramowitz and I. A. Stegun, Eds. *Handbook of Mathematical Functions* (NBS Applied Mathematical Series 55). Washington, D.C.: U.S. Government Printing Office, 1964.
[9] W. W. Weinstock, "Target cross section model for radar systems analysis," Ph.D. dissertation, Univ. Pennsylvania, State College, 1964.
[10] C. W. Helstrom, *Statistical Theory of Signal Detection*, 2nd ed. New York: Pergamon, 1968, p. 219.
[11] H. Chernoff, "A measure of asymptotic efficiency for tests of a hypothesis based on a sum of observations," *Ann. Math. Statist.*, vol. 25, pp. 493–507, 1952.
[12] J. M. Wozencraft and I. M. Jacobs, *Principles of Communication Engineering*. New York: Wiley, 1965.
[13] G. A. Campbell and R. M. Foster, *Fourier Integrals for Practical Applications*. New York: Van Nostrand, 1948.
[14] D. A. Shnidman, "Evaluation of probability of detection for several target fluctuation models," M.I.T. Lincoln Lab., Tech. Note TN-1975-35, July 1975.
[15] L. E. Brennan and I. S. Reed, "A recursive method of computing the Q-function," *IEEE Trans. Inform. Theory*, vol. IT-11, pp. 312–313, April 1965.
[16] S. O. Rice, "Uniformly asymptotic expansions for saddle point integrals—Application to a probability distribution occurring in noise theory," *Bell Syst. Tech. J.*, vol. 47, pp. 1971–2013, Nov. 1968.
[17] K. E. Iverson, *A Programming Language*. New York: Wiley, 1962.

Optimum Permutation Modulation Codes and Their Asymptotic Performance

EZIO M. BIGLIERI, MEMBER, IEEE, AND MICHELE ELIA

***Abstract*—Permutation modulation codes are a class of group codes for the Gaussian channel whose codewords are obtained by permuting the components of a given initial vector X in Euclidean n-dimensional space. In this paper, the problem of choosing the components of X in such a way that the minimum distance between any two codewords is maximized is solved. In particular, a closed-form expression is obtained for this minimum distance and is used to investigate the asymptotic behavior of some selected codes.**

I. Terminology and Statement of the Problem

Let $\{\mu_1,\mu_2,\cdots,\mu_s\}$ be a set of distinct real numbers, and $\{m_1,\cdots,m_s\}$ a set of positive integers with $m_1 + m_2 + \cdots + m_s = n$. Consider the n-vector

$$X = (\underbrace{\mu_1,\cdots,\mu_1}_{m_1},\underbrace{\mu_2,\cdots,\mu_2}_{m_2},\cdots,\underbrace{\mu_s,\cdots,\mu_s}_{m_s}). \tag{1}$$

Manuscript received January 29, 1975; revised November 19, 1975. This paper was presented at the Colloquium on Information Theory, Keszthely, Hungary, August 1975.

E. M. Biglieri was with the Istituto di Elettronica e Telecomunicazioni del Politecnico, Corso Duca degli Abruzzi 24, Torino, Italy. He is now with the Instituto Elettrotecnico, Universitá di Napoli, Italy.
M. Elia is with the Instituto Matematico del Politecnico, Corso Duca degli Abruzzi 24, Torino, Italy.

If $\{\delta\}$ denotes the group of operators that act on X by permuting its components, then the set $\{\delta\}X$ will include

$$M = \frac{n!}{\prod_{i=1}^{s} m_i!}$$

distinct n-vectors. The set $\{\delta\}X$ is called a *variant I permutation modulation (PM) code* [4]–[9]. Clearly, each vector of the set $\{\delta\}X$ has the same norm, which we choose to be 1, i.e.,

$$\|\delta X\|^2 = \sum_{i=1}^{s} m_i\mu_i^2 = 1.$$

In geometrical terms, the vectors of a PM code may be thought of as points on the surface of a unit-radius n-dimensional hypersphere centered at the origin.

The key problem we want to solve is the following: given the set $\{m_1,m_2,\cdots,m_s\}$, and thus the number M of vectors in a PM code, choose the set $\{\mu_1,\cdots,\mu_s\}$ so that the minimum distance between any two points of $\{\delta\}X$ is a maximum. In Section II we give a solution to this problem by showing that the optimum X has components μ_i that satisfy the relation

$$\mu_i - \mu_{i+1} = \lambda$$

where λ is a suitable constant. The resultant codes have interesting geometric features: if we think of the codewords as points in Euclidean n-space [1]–[3], every code can be viewed geometrically as an n-dimensional polytope with vertices at those points. Now, in spaces with dimension more than four, there are only three regular polytopes [10]: the hypercube, the cross-polytope, and the regular simplex, giving rise to well-known "good" codes [3]. The codes to be described in the next section are the *semiregular polytopes*, first observed by Slepian, who analyzed them [4], [5]; a description of their geometrical properties can be found in [11], [12].

An existence theorem of coding theory shows that it is possible to find sequences of codes of M points in n-space such that, in the limit as n approaches ∞, both the minimum distance between codewords and the rate R are bounded below by positive quantities (see, for instance, [13]). It has been shown by Landau [14] that PM codes cannot achieve such strong asymptotic behavior; nevertheless, we shall see in Section IV that interesting asymptotic behavior can be obtained through a suitable choice of the parameters.

II. Optimum PM Codes

We wish now to find an n-vector X, satisfying the constraint $\|X\|^2 = 1$, such that

$$g(X) = \min_{\delta \neq I_n} \|X - \delta X\|^2 \tag{2}$$

is a maximum. Here, I_n is the identity permutation.

We first observe that the initial vector X is completely defined, for given $m_1,m_2,\cdots,m_s$, by a set of real numbers $\mu_1,\mu_2,\cdots,\mu_s$ and a correspondence between the m and μ. Thus, we can write

$$\max_X g(X) = \max_{\tau} \max_{\{\mu_1,\cdots,\mu_s\}} g(X)$$

where τ is a one-to-one mapping of the set of integers $\{1,2,\cdots,s\}$ onto itself. Thus, we may take X in this form

$$X = (\underbrace{\mu_1,\cdots,\mu_1}_{m_{\tau(1)}},\underbrace{\mu_2,\cdots,\mu_2}_{m_{\tau(2)}},\cdots,\underbrace{\mu_s,\cdots,\mu_s}_{m_{\tau(s)}}). \tag{3}$$

We shall approach the problem in two steps: i) find the optimum set $\{\mu_1,\cdots,\mu_s\}$ for a given τ; and ii) find the optimum τ.

Before proceeding further, we observe from (2), letting $X + h$ denote the vector obtained by adding an equal quantity h to

all the components of X (i.e., a translation of X), that

$$g(X + h) = g(X).$$

Moreover, the minimum value of $\|X + h\|$ is obtained when

$$h = -\sum_{i=1}^{s} m_{\tau(i)}\mu_i.$$

Thus, we shall henceforth impose on PM codes the condition

$$\sum_{i=1}^{s} m_{\tau(i)}\mu_i = 0. \tag{4}$$

We are now ready to solve our main problem of finding the maximum value of $g(X)$ under the constraints (4) and

$$\sum_{i=1}^{s} m_{\tau(i)}\mu_i^2 = 1 \tag{5}$$

where X has the form (3). Suppose that masses $m_{\tau(1)}, \cdots, m_{\tau(s)}$ are located at points $\mu_1, \mu_2, \cdots, \mu_s$ along the μ-axis. Because of (4), (5) gives the central moment of inertia. We seek to slide the points along the line (without passing each other) to maximize the nearest neighbor distance keeping a fixed central moment of inertia.

Suppose the maximization problem is solved by an arrangement such that $\mu_{i+1} - \mu_i$ is not constant, and let Δ be the smallest separation between two adjacent masses in this configuration. Now slide all the masses along so that a configuration results with every adjacent pair of masses separated by distance Δ. The central moment of inertia, η^2, of this new configuration is smaller than 1 since we have packed the masses closer together. Now multiply the coordinates of all the masses in this new configuration by $1/\eta$; an equally spaced configuration of masses is obtained with central moment of inertia 1 and minimum distance between points $\Delta/\eta > \Delta$. Thus, the original configuration with unequal separation was not the best possible. We have proved that the optimum X must have components satisfying

$$\mu_\rho = \mu_1 + (\rho - 1)\omega. \tag{6}$$

The actual values of μ_1 and ω can be computed, using constraints (4) and (5), as

$$\mu_1 = -\frac{A_1}{\sqrt{n(A_2 - A_1^2)}}$$

$$\omega = -\mu_1/A_1$$

where

$$A_1 = \frac{1}{n}\sum_{j=1}^{s} m_{\tau(j)}(j-1)$$

$$A_2 = \frac{1}{n}\sum_{j=1}^{s} m_{\tau(j)}(j-1)^2.$$

The minimum distance can now be computed as

$$\max_{\{\mu_1,\cdots,\mu_s\}} g(X) = 2\omega^2 = \frac{2}{n(A_2 - A_1^2)}$$

and, after some algebra,

$$\max_{\{\mu_1,\cdots,\mu_s\}} g(X) = \frac{4n}{\sum_{i=1}^{s}\sum_{j=1}^{s} m_{\tau(i)}m_{\tau(j)}(i-j)^2}. \tag{7}$$

The second step is to find the optimum mapping τ. Since every one-to-one mapping of a finite set onto itself is equivalent to a permutation, our problem is to find the permutation τ such that

$$Q(\tau) = \sum_{i=1}^{s}\sum_{j=1}^{s} m_{\tau(i)}m_{\tau(j)}(i-j)^2$$

is a minimum. This problem was first solved by Slepian [4], who showed that $Q(\tau)$ attains its minimum value when τ is such that

$$m_{\tau(1)} \le m_{\tau(s)} \le m_{\tau(2)} \le m_{\tau(s-1)} \le \cdots. \tag{8}$$

Expressed in words, we must choose the pairing of m and μ in the initial vector in such a way that the least m is paired with the least μ, the second least m with the largest μ, the third least m with the second least μ, and so on.

III. Miscellaneous Comments and Additional Results

The optimized minimum distance d_{opt}^2 can also be written, with the aid of (7), as

$$d_{\text{opt}}^2 = \frac{2/n}{\frac{1}{n}\sum_{j=i}^{s} m_{\tau(j)}(j-1)^2 - \left(\frac{1}{n}\sum_{j=1}^{s} m_{\tau(j)}(j-1)\right)^2}. \tag{9}$$

The denominator of (9) can be interpreted as the variance of a random variable ξ that assumes the value $(j-1)$ with probability $m_{\tau(j)}/n$. Thus we can expect to get higher values of d_{opt}^2 when the probability distribution of ξ is somewhat concentrated around its mean value.

Suppose that the m were originally given in increasing order, i.e.,

$$m_1 \le m_2 \le m_3 \le \cdots \le m_s.$$

Then d_{opt}^2 can be computed from (8), (9), and the equality

$$\sum_{i=1}^{s} m_{\tau(i)}\psi(i) = \sum_{i=1}^{s/2}[m_i\psi(2i-1) + m_{s-i+1}\psi(2i)]$$

which holds for every function $\psi(i)$ and s even (for s odd, a similar formula holds) when τ is defined as in (8).

The number of nearest neighbors to each codeword (i.e., the number of codewords at the minimum distance from any given code vector) in the optimum code is given by

$$\nu = m_{\tau(1)}m_{\tau(2)} + m_{\tau(2)}m_{\tau(3)} + \cdots + m_{\tau(s-1)}m_{\tau(s)}. \tag{10}$$

Suppose that we want to maximize (10); it is easily seen that this is equivalent to maximizing the quadratic form

$$Q''(\tau) = \sum_{i=1}^{s}\sum_{j=1}^{s} m_{\tau(i)}m_{\tau(j)}c_{i-j}$$

with respect to τ, where

$$c_{i-j} = \begin{cases} 2, & i-j = 0 \\ 1, & |i-j| = 1 \\ 0, & |i-j| > 1. \end{cases}$$

We are now in position to use Theorem 371 of [17] to show that the arrangement (8) that maximizes the minimum distance also maximizes the number of nearest neighbors. (The authors conjecture that this property holds in general, i.e., that maximizing the number of nearest neighbors is equivalent to maximizing the minimum distance for every group code [20].)

Given an n-vector X of the form (1), where we now let

$$0 \le \mu_1 < \mu_2 < \cdots < \mu_s,$$

we define a *variant II PM code* as the set of vectors obtained by permuting the components of X in all possible ways and by making all possible assignments of sign to the components of the resulting vectors [5]. The same arguments leading to the optimum starting vector for variant I PM codes can be used to solve the same problem for variant II PM codes.

IV. Asymptotic Behavior of PM Codes

To analyze the communication capabilities of the optimum PM codes derived in Section III, we must consider, together with their distance properties, their information rate $R = \log M/n$. In particular, we shall consider the asymptotic behavior of R for sequences of PM codes with increasing n. In what follows, we stipulate that these sequences are constructed so that all the limits we shall consider exist as $n \to \infty$.

Using Stirling's formula, we can write the number M of distinct n-vectors in the set $\{\delta\}X$ as

$$\frac{\log M}{n} \sim H + \varphi$$

where H represents the entropy of a source that emits independent symbols with probabilities m_i/n, i.e.,

$$H = -\sum_{i=1}^{s} \frac{m_i}{n} \log \frac{m_i}{n}$$

and

$$\varphi = \frac{1}{2n} \sum_{i=1}^{s} \log 2\pi m_i.$$

Here it has been assumed that n and each m_i, $i = 1,2,\cdots,s$, is large. It can be seen that H is the relevant quantity in the computation of the rate.

Defining

$$\alpha = \lim_{n\to\infty} \frac{s}{n} \log n$$

one can show: i) If $\alpha = 0$, $\lim R = \lim H$; moreover, if $H \not\to 0$, $R \sim H$. ii) If $0 < \alpha \leq \infty$, $R \sim H$. In other words, the asymptotic behavior of R is the same as that of H, with the only possible exception being when $H \to 0$ as $n \to \infty$.

It is interesting to observe how some information on the limit behavior of the rate can be obtained by simply observing the behavior of s as $n \to \infty$. For instance, for $s > e$, we have $H \geq s/n$; moreover, $s/n \not\to 0$ implies $H \not\to 0$, $s \not\to \infty$ implies $H \not\to \infty$, and so on.

In the following we have collected some examples of the asymptotic behavior of both rate and distance for some selected PM codes.

Example 1: Let $s = 2$, $m_1 = n - h$, and $m_2 = h$, with h a finite, fixed constant. Then $R \to 0$ and

$$d_{\text{opt}}{}^2 = \frac{2/n}{(h/n) - (h/n)^2} \to \frac{2}{h}.$$

Example 2: Let $m_i = m$, a fixed constant independent of i, so that $s = n/m$. We find $R \to \infty$; moreover,

$$d_{\text{opt}}{}^2 = \frac{24m^2}{(n-m)\,n\,(n+m)} = 0(n^{-3}). \tag{11}$$

In the special case $m = 1$, (11) was first observed by Slepian [18] and independently rediscovered by Blake [19].

Example 3: Let $m_i = n/s$, with s a fixed constant. Then $R \to \log s$ and

$$d_{\text{opt}}{}^2 = \frac{24/n}{(s-1)\,(s+1)} = 0(n^{-1}).$$

Example 4: Let $m_i = i$; then $n = s(s+1)/2$ so that $s \sim \sqrt{2n}$. We get $R \sim \log n$, and $d_{\text{opt}}{}^2 = 0(n^{-2})$.

Example 5: Let $m_i = a^i$, with a an integer exceeding 1; in this case $n \sim a^{s+1}/(a-1)$ and

$$R \to \frac{a \log a + (a-1)\log(a-1)}{a-1}$$

with $d_{\text{opt}}{}^2 = 0(n^{-1})$.

Acknowledgment

The authors wish to thank D. Slepian, who contributed a proof of (6) which greatly shortened the original one.

References

[1] A. D. Wyner, "On coding and information theory," *SIAM Rev.*, vol. 11, pp. 317–346, July 1969.

[2] A. D. Wyner, "Capacity of the band-limited Gaussian channel," *Bell Syst. Tech. J.*, vol. 25, March 1966

[3] J. M. Wozencraft and I. M. Jacobs, *Principles of Communication Engineering.* New York: Wiley, 1965.

[4] D. Slepian, "Several new families of alphabets for signalling," Bell Telephone Labs., Unpublished Memorandum, 1951.

[5] ——, "Permutation modulation," *IEEE Proc.*, vol. 53, pp. 228–236, March 1965.

[6] T. Berger, F. Jelinek, and J. K. Wolf, "Permutation codes for sources," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 160–169, Jan. 1972.

[7] T. Berger, "Optimum quantizers and permutation codes," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 759–765, Nov. 1972.

[8] J. G. Dunn, "Coding for continuous sources and channels," Ph.D. Dissertation, Dep. Elec. Eng., Columbia Univ., New York, N.Y., 1965.

[9] ——, "The performance of a class of n-dimensional quantizers for a Gaussian source," in *Proc. Symp. Signal Transmission and Processing*, Columbia Univ., New York, N.Y., May 1965, pp. 76–81.

[10] H. S. M. Coxeter, *Regular Polytopes.* New York: MacMillan, 1963.

[11] A. B. Stott, "Geometrical deduction of semiregular from regular polytopes," *Ver. Koninklijke Akad. Wetensch. Amsterdam.* (eerste sectie), vol. 11.1, 1910.

[12] P. H. Schoute, "Analytical treatment of the polytopes regularly derived from the regular polytopes," *Ver. Koninklijke Akad. Wetensch. Amsterdam* (eerste sectie), vol. 11.5, 1913.

[13] A. D. Wyner, "Capabilities of bounded discrepancy decoding," *Bell Syst. Tech. J.*, vol. 44, pp. 1061–1122, Jul. Aug. 1965.

[14] H. J. Landau, "How does a porcupine separate its quills?" *IEEE Trans. Inform. Theory*, vol. IT-17, pp. 157–161, March 1971.

[15] A. V. Balakrishnan, "A contribution to the sphere-packing problem of communication theory," *J. Math. Anal. Appl.*, vol. 3, pp. 485–506, Dec. 1961.

[16] ——, "Signal selection theory for space communication channels," in *Advances in Communication Systems*, A. V. Balakrishnan, Ed. New York: Academic, 1965.

[17] G. H. Hardy, J. E. Littlewood, and G. Pòlya, *Inequalities*, 2nd ed. Cambridge: University Press, 1964.

[18] D. Slepian, "Large signalling alphabets generated by groups," Bell Telephone Labs., Unpublished Memorandum, 1951.

[19] I. F. Blake, "Distance properties of group codes for the Gaussian channel," *SIAM J. Appl. Math.*, vol. 23, pp. 312–324, Nov. 1972.

[20] D. Slepian, "Group codes for the Gaussian channel," *Bell Syst. Tech. J.*, vol. 47, pp. 575–602, April 1968.

Cooperative Bridge Bidding

ELWYN R. BERLEKAMP, FELLOW, IEEE

***Abstract*—A strategy is given for cooperative bidding by the players which results in the location of all 52 cards being encoded into a valid bridge auction which always terminates with a contract of six diamonds. Strategies are also given for encoding the card locations into auctions in which "double" and/or "redouble" are prohibited bids.**

Manuscript received December 12, 1975; revised April 26, 1976.

The author is with the Computer Science Division, Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, CA. 94720.