NEUVIEME COLLOQUE SUR LE TRAITEMENT DU
SIGNAL ET SES APPLICATIONS

NICE du 16 au 20 MAI 1983

EFFICIENT BLOCK CODED DIGITAL COMMUNICATIONS

VIJAY K. BHARGAVA* AND JEAN CONAN

Département de Génie Electrique, Ecole Polytechnique de Montréal, Case Postale 6079, Succursale 'A' Montréal, Québec, Canada H3C 3A7

RESUME

Il est bien établi que le décodage de la grande majorité des codes en blocs nécessite une quantification à décisions fermes à la sortie du démodulateur du système de réception. En conséquence ces systèmes subissent une perte de 2 à 3 dB par rapport à des systèmes, tels que les codes convolutionnels, qui utilisent une quantification à décisions pondérées.

Cependant dans les systèmes où le protocole de communication requiert une transmission des données en blocs (comme, par exemple, les réseaux utilisant l'AMRT ou la commutation par paquets) l'usage de codes convolutionnels ne s'avère pas attrayant en raison de la réinitialisation requise après chaque transmission. Dans ces situations les codes en blocs semblent être plus intéressants.

Dans cet article, on présente une classe de codes en blocs qui sont décodables par quantification à décisions pondérées, permettant ainsi une communication efficace. Ces codes appartiennent à la classe des codes quasi-cycliques mais, utilisant la théorie développée par Solomon et Van Tilborg, sont encodables de façon convolutionnelle avec une faible longeur de contrainte. La classe des codes obtenus comprend les codes auto-duaux extrêmaux, certains codes cycliques de Mac Williams et ceux dérivés des codes résidus puissance. La performance de ces codes est calculée en applicant, en conjonction avec une quantification à décisions pondérées, la borne union à la distribution de leurs poids de Hamming. Pour des taux d'erreur part bit inférieurs à 10^{-3}, correspondant au domaine d'intérêt pour les applications du codage, les gains de codage obtenus s'échelonnent de modérés à sensationnels.

Enfin, il est bon de mentionner la découverte d'un nouveau code cyclique (151,136) d'une puissance de correction de 2 erreurs. Jusqu'à présent le meilleur code en bloc de même dimension était un code non linéaire découvert par Preparata.

SUMMARY

It is well known that to decode almost all block codes it is necessary to use binary quantization (hard-decisions) at the demodulator output of a block coded communications system. This limitation translates as a loss of 2 to 3 dB in comparison with the soft-decision decoded convolutionally coded communications system.

On the other hand, in situations where the system protocols require the transmission of blocks of data (such as TDMA and Packet Satellite Networks), all convolutional systems require flushouts and restarts, i.e., the CODEC must be set to the all zero state before processing the next block. For such systems block codes appear to be more attractive.

In this paper, we present a class of block codes which are soft-decision decodable and thus contribute to efficient block coded digital communications. The approach taken is to construct a large number quasi-cyclic codes. These are convolutionally encodable with small constraint lengths due to the theory developed by Solomon and Van Tilborg. Using the weight distribution of the codes considered (which include extremal self-dual codes, certain cyclic codes of MacWilliams and codes derived from power residue codes) we compute their performance using the union bound for soft decision decoding. For bit error rates below 10^{-3}, which is the region of interest for coding application, the coding gains obtained from these codes range from moderate to spectacular.

A final point worth noting is the discovery of a (151,136) double error correcting cyclic code. Earlier, the best known block code of similar dimension was a nonlinear code due to Preparata

* On sabbatical leave from the Department of Electrical Engineering, Concordia University, 1455 de Maisonneuve Boulevard West, Montréal, Québec, Canada, H3G 1M8.

EFFICIENT BLOCK CODED DIGITAL COMMUNICATION

VIJAY BHARGAVA and JEAN CONAN

1. INTRODUCTION

Probably the best known techniques for soft-decision decoding are correlation decoding of block codes and Viterbi decoding of convolutional codes. It can be shown that for a code with equiprobable code words the correlation receiver is optimum (ref. 1). Unfortunately a majority of block coded systems employ a hard-decision quantiser before decoding in order to extract the digital information. This hard-decision process gives a degradation in performance of $\pi/2$ (approximately 2 dB) compared to the optimum receiver in the Gaussian channel. It follows that for this channel, the maximum improvement to be expected by introducing soft-decision decoding into a block coded system is equivalent to this degradation.

In this paper, we present a class of block codes which are soft-decision decodable and thus contribute to efficient block coded digital communication . The approach taken is to construct and compute the weight distribution of a large number of quasi-cyclic codes and then evaluate their performance using the union bound for soft-decision decoding. These codes are convolutionally encodable with small constraint length due to a theory developed by Solomon and van Tilborg (ref. 2).

This paper develops in the following way. Section 2 presents a model of block coded digital communication . In Section 3 we discuss the coding gain and the union bound for soft-decision decoding. In Section 4 we discuss the theory of the class of codes used. Section 5 is devoted to performance evaluation of several block codes. These include the rate 1/2 extremal self-dual codes (ref. 3), several codes with rates less than 1/2 and some high rate codes. Finally, Section 6 is devoted to discussion of the results presented in this paper.

2. BLOCK CODED DIGITAL COMMUNICATION

A block diagram which describes the digital communication process using forward error correction process is shown in Fig. 1. In block encoding, a block of k information bits is encoded into corresponding blocks of n symbols. Each block of n symbols from the encoder constitutes a code word contained in a set of 2^k possible code words. The code rate, defined as the ratio k/n and denoted r is a measure of the amount of redundancy in the (n,k) code. Thus if E_b denotes the energy per bit then E_s, the energy per coded bit, referred to as a symbol, is given by

$$E_s = rE_b = E_b - 10\log_{10}(\frac{1}{r})\text{dB}$$

Note that the introduction of error-control coding requires more capacity. This can be in the form of wider bandwidth, longer bursts in time division multiple access (TDMA) systems, or a higher "chip" rate (and hence a higher bandwidth) in spread spectrum systems, if the same processing gain is needed (ref. 4).

The Hamming weight of a code word $\underline{c}$, denoted $w(\underline{c})$, is defined to be the number of non-zero components of $\underline{c}$. For example, if $\underline{c} = (110101)$, then $w(\underline{c})=4$. The Hamming distance between two code words $\underline{c}_1$ and $\underline{c}_2$, denoted $d(\underline{c}_1,\underline{c}_2)$, is the number of positions in which they differ. For example, if $\underline{c}_1 = (110101)$ and $\underline{c}_2 = (111000)$ then $d(\underline{c}_1,\underline{c}_2) = 3$. Clearly $d(\underline{c}_1,\underline{c}_2) = w(\underline{c}_1 \oplus \underline{c}_2) = w(\underline{c}_3)$, where $\underline{c}_3$ for linear codes, is some other code word. Therefore, the distance between any two code words equals the weight of some other code word, and the minimum distance d for a linear block code equals the minimum weight of its non-zero code words.

A code can correct all patterns of t or fewer random errors and in addition detect all patterns having no more than s errors provided that $s+t+1 \leq d$. If the code is used for error correction only then the code can correct all patterns of t or fewer random errors provided that $2t+1 \leq d$.

The encoded sequence is suitably modulated and transmitted over the noisy channel. In systems where coherent demodulation is possible (i.e., a carrier reference can be obtained), phase shift keying (PSK) is often used. In binary PSK an encoded 1 is represented by the wave forms $s_1(t) = A\cos\omega_c t$, while an encoded 0 is represented by the antipodal signal $s_0(t) = -s_1(t) = A\cos(\omega_c t+\pi)$, the waveforms changing at discrete times T_s seconds (symbol duration) apart.

The demodulator estimates which of the possible symbols was transmitted based upon an observation of the received signal. For phase shift keying (PSK) with white Gaussian noise and perfect phase tracking, the optimum receiver is a correlator or matched filter receiver which is sampled each T_s seconds to determine its polarity. It is easily shown that the voltage z, at the matched filter output at the sample time is a Gaussian random variable with mean $\pm\sqrt{E_s}$, (depending upon whether a 1 or 0 was transmitted) and variance $\sigma^2 = N_o/2$. In the above, E_s is the energy per symbol. E_b denotes the received energy per bit (what we pay) and N_o denotes the one sided noise spectral density (what we must combat).

2.1 Hard Decisions, Soft Decisions

In practical communication systems, we rarely have the ability to process the actual analog voltages z_i (the values taken by the random variable z). The normal practice is to quantize these voltages. If a binary quantization is used, we say that a hard decision has been made on the correlator output as to which level was actually sent. In this case, we have the so called binary symmetric channel (BSC) with probability of error P_e. For example, in coherent PSK with equally likely transmitted symbols, the optimum threshold is at zero. Then the demodulator output is a zero if the voltage z at the matched filter output is negative. Otherwise, the output is a one. Without coding, matched filtering with hard decisions is an optimum receiver.

With coding, it is desirable to keep an indication of how reliable the decision was. A soft-decision demodulator first of all decides whether the output voltage is above or below the decision threshold, and then computes a "confidence" number which specifies how far from the decision threshold the demodulator output is. This number in theory could be an analogue quantity, but in most practical applications a three bit (eight level) quantization is used.

An example of three bit quantization is shown in Fig. 2. The input to the demodulator is binary, while the output is 8-ary, delineated by one decision threshold and three pairs of confidence thresholds. The information available to the decoder is increased considerably and translates as an additional gain of 2 dB in most instances (ref. 1). Furthermore, 8-ary quantization results in a loss of 0.25 dB compared to infinitly fine quantization, therefore, quantization to more than 8 levels can yield little performance improvement. Of course, the receiver complexity is increased as an AGC will probably be needed and three bits will have to be manipulated for every channel bit. The channel resulting from three bit quantization on a Gaussian. channel is called the binary input, 8-ary output, discrete memoryless channel (DMC), and is shown in Fig. 3.

3.0 CODING GAIN AND THE UNION BOUND FOR SOFT-DECISION DECODING

Before we start our study of codes, consider a Gaussian memoryless channel with one-sided noise spectral density N_o and under no bandwidth limitation. Let E_b denote the received energy per bit. Then it can be shown that for E_b/N_o greater than -1.6 dB, there exists

EFFICIENT BLOCK CODED DIGITAL COMMUNICATION

VIJAY BHARGAVA and JEAN CONAN

some coding scheme which allows us to communicate with zero error, while reliable communication is not generally possible at lower signal-to-noise ratios. On the other hand, it is well known that uncoded PSK over the same channel will require about 9.6 dB to achieve a bit error rate of 10^{-5}. Thus, a potential coding gain of 11.2 dB is theoretically possible. Coding gain is defined as the difference in values of E_b/N_o required to attain a particular error rate without coding and with coding.

Asymptotic coding gain, a figure of merit for a particular code, depends only on the code rate and the minimum distance. To define it, consider a t-error correcting code with rate r and minimum distance $d \geq 2t+1$. If we use the code with a hard decision PSK demodulator, it can be shown that the bit error rate P_b is

$$P_{b,h} \geq Q(\sqrt{2E_b r(t+1)/N_o}), \text{ where } Q(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} e^{-y^2/2} dy.$$

With a soft-quantized PSK demodulator, we have

$$P_{b,s} \geq Q(\sqrt{2E_b rd/N_o})$$

Recall that for uncoded PSK

$$P_b = Q(\sqrt{2E_b/N_o})$$

Thus the asymptotic coding gain G_a for the two cases is:

$$G_a \leq r(t+1) = 10 \log r(t+1), \quad \text{dB (Hard-decision)}$$

$$G_a \leq rd = 10 \log rd, \quad \text{dB (Soft-decision)}$$

The above indicates that soft decision decoding is about 3 dB more efficient than hard decision decoding at very high E_b/N_o. A figure of 2 dB is more likely at realistic values of E_b/N_o.

Let A_i denote the number of code words of weight i in an (n,k) code with minimum distance d. Then the soft-decision decoding bit error rate P_e, in the case of the Gaussian channel with CPSK modulation is bounded from above by

$$P_e \leq \frac{1}{n} \sum_{i=d}^{n} iA_i Q\left(\sqrt{\frac{2ki\,E_b}{n\,N_o}}\right) \qquad (1)$$

The computation of the probability of error for soft-decision decoding according to Eq. (1) requires the knowledge of the weight distribution of the code. Fortunately, the weight distribution of many codes have been tabulated in the literature.

The upper bound of Eq. (1) is particularly tight at high signal-to-noise ratios. Usually, it gives an accurate performance estimate for bit-error rates below 10^{-3}, which is the region of interest for coding. The bound is also valid for QPSK modulation. Indeed the BPSK modulation of quadrature carriers is equivalent to quadraphase modulation of one carrier. Thus, QPSK need not be separately treated except for synchronization and phase error requirements.

4.0 THE CLASS OF CODES CONSIDERED

We are primarily concerned with (ms,m) rate 1/s and (m(s+1),ms) rate s/(s+1) quasi-cyclic codes and codes related to them. Example of the related codes include the power residue codes, extremal self-dual codes etc. (ref. 5,6).

The generator matrix of a (ms,m) rate 1/s quasi-cyclic code is of the form

$$G = [C_1, C_2, C_3, \ldots, C_s] \qquad (2)$$

where each C_i is a m×m square circulant matrix of the form

$$C = \begin{bmatrix} c_0 & c_1, \ldots, c_{m-1} \\ c_{m-1} & c_0, \ldots, c_{m-2} \\ \ldots & \ldots \ldots \ldots \\ c_1 & c_2 \ldots c_0 \end{bmatrix} \qquad (3)$$

with $c_i \in GF(2)$ for the binary codes.

In the systematic form Eq. (2) can be written as

$$G = [I_m, C_1, C_2, \ldots, C_{s-1}] \qquad (4)$$

Here I_m is an identity matrix of order m. Similarly, a (m(s+1),ms) rate s/(s+1) quasi-cyclic in the systematic form, has a generator matrix of the form

$$G = \begin{bmatrix} & C_1 \\ & C_2 \\ I_{ms} & \vdots \\ & C_s \end{bmatrix} \qquad (5)$$

Every code word of the code generator by the matrix of Eq. (4) is a linear combination of the rows of G. It is well known that the algebra of m×m circulant matrices over GF(p) is isomorphic to the algebra of all polynomials (mod x^m-1) over GF(p). Further, the matrix C of Eq. (3) is completely specified by associating with it the following polynomial formed on its leading row

$$c(x) = c_0 + c_1(x) + \cdots + c_{m-1}x^{m-1}.$$

Thus, if i(x) represents the information digits in the polynomial form, each code word in the rate 1/s code is of the form

$$v(x) = [i(x); i(x)c_1(x), \ldots, i(x)c_{s-1}(x)] \ (\text{mod } x^m-1).$$

In a similar fashion, each code word in the code generated by the matrix G of Eq. (5) is of the form

$$v(x) = [i_1(x), i_2(x), \ldots, i_s(x); p(x)] \ (\text{mod } x^m-1)$$

where $p(x) = \sum_{j=1}^{s} i_j(x)c_j(x) \ (\text{mod } x^m-1)$.

Note that the generator matrix of Eq. (4) or Eq. (5) is completely specified by the circulant matrices $C_1, C_2, \ldots$. Thus, we shall speak of the code as being generated by the circulants $C_1, C_2, \ldots$. Equivalently, we shall also speak of the code as being generated by the polynomials $c_1(x), c_2(x), \ldots$. Also, in the binary case we shall often use the octal representation of these polynomials. For instance, the octal number 64 has the binary form 110100 and represents the polynomial $1+x+x^3$.

The encoding of quasi-cyclic codes is quite straightforward and like cyclic codes can be accomplished by shift registers. More importantly, under certain conditions, these codes are soft-decision decodable and thus contribute to efficient block coded digital communications. Specifically, Solomon and van Tilborg have shown a large number of quasi-cyclic codes to be convolutionally encoded with small constraint length. Thus we have a simple maximum likelihood decoding algorithm for many quasi-cyclic and related codes. Further, the weight distribution of many quasi-cyclic codes has been tabulated in (ref. 7-13).

5.0 PERFORMANCE EVALUATION

In this section we first evaluate the performance of several rate 1/2 quasi-cyclic (or related) codes. We then examine codes with rates less than 1/2. Such codes buy improved performance at the expense of increased bandwidth expansion and more difficult symbol tracking due to decreased symbol energy-to-noise ratios. Some of these low rate codes are useful for spread

spectrum applications as well. Codes with rates above 1/2 conserve bandwidth but are not as efficient in energy.

5.1 Extremal Self-dual Codes

A binary (2m,m) rate 1/2 code is generated by a matrix of the form

$$G = [I_m, P] \qquad (6)$$

where I_m is the m×m identity matrix and P is an m×m binary matrix. If P is a circulant, we have a quasi-cyclic code.

The code generated by Eq. (6) is said to be self-dual if

$$PP^T = I_m \text{ (modulo 2)}$$

Many good codes are self-dual, such as the extended Golay code and certain quadratic residue codes, etc.

The minimum distance d of a (2m,m) self-dual code is upper bounded by the relation

$$d \leq 4[m/12] + 4,$$

and if $d = 4[m/12] + 4$, the code is called an extremal self-dual code (ref. 14). The known codes in this family are summarized in Fig. 19.2 of ref. 6. However, it is not known if there is a (72,36) extremal self-dual code (ref. 15). The codes considered have been selected for the following reasons:

(i) Extremal self-dual codes are well understood (See Chapter 19 in ref. 6).
(ii) The union bound for soft decoding depends on the weight distribution of the code and thus it can be applied to codes with known weight distribution. Fortunately, the weight distributions of extremal self-dual codes are known (ref. 14).
(iii) When a transmission system is bandwidth-limited for BPSK the combination of QPSK and the codes considered can provide a solution (ref. 1).
(iv) These codes are "transparent" and are thus valuable for PSK modulated systems with its ensuing sign ambiguity. Decoding can be done prior to ambiguity removal and thus circumventing differential decoding at the decoder input which will double the decoder input rate (ref. 1).
(v) There are plenty of extremal self-dual codes of various lengths (ref. 14).

In Fig. 4, we present the performance of several extremal self-dual codes of length 8 to 72 using the bound of Eq. (1). These were first reported in (ref. 14). All codes except the (72,36) code are known to exist. As can be seen from Fig. 4, the coding gains obtained from these codes range from moderate to spectacular. Several observations may be made based on Fig. 4.

(i) At very low error rates, not much is to be gained by going to longer block lengths for a specified minimum distance.
(ii) At high error rates and for a specified minimum distance, there is a tradeoff between various codes. The tradeoff can be attributed to the weight distribution of the codes and in particular on the number of code words having the minimum weight.
(iii) The performance of the (48,24) code, for which a soft-decision decoding algorithm has been designed by several researchers at NASA's Jet Propulsion Laboratory, is only slightly inferior to a rate 1/2 constraint length 7 convolutional code with Viterbi decoding using soft quantization (ref. 16). However, it is also known that the (48,24) code can be modelled as a rate 1/2 constraint length 6 convolutional code and therefore will have a significantly less decoding complexity (ref. 2).

5.2 Low Rate Codes

We now determine the performance of several block codes whose generator matrix can be permuted in the form of Eq. (2) or Eq. (4). Two such families are the cyclic codes of MacWilliams (ref. 17) and the power residue codes (ref. 18).

MacWilliams' Codes

Mrs. MacWilliams has given the method for the decomposition of certain cyclic codes of block lengths 3p, 7p and 5p. Using her results, it is easy to compute the weight distribution of the (87,29), (85,17) and the (91,13) code with minimum distance 24, 21 and 36 respectively.

The (87,29) code is generated in the systematic form by $c_1(x) = 6364221362$ and $c_2(x) = 5413556414$.

The (85,17) code is generated in the systematic form by $c_1(x) = 42412$, $c_2(x) = 41144$, $c_3(x) = 540014$ and $c_4(x) = 602202$.

The (91,13) code is generated in the systematic form by $c_1(x) = 4264$, $c_2(x) = 61104$, $c_3(x) = 75134$, $c_4(x) = 5403$, $c_5(x) = 63744$ and $c_6(x) = 5667$.

The performance of all these codes is plotted in Fig. 5.

Codes Derived from Power Residue Codes

It is well known that the s-th power residue codes with first digit deleted are equivalent to rate 1/s quasi-cyclic codes (ref. 18). An s-th power residue code of length n is defined as a cyclic code over GF(2) with a check polynomial of the form

$$h(x) = \prod_{r \in R} (x - \beta^r)$$

where R is the set of s-th power residue mod n, and β is a primitive n-th root of unity in an extension field of GF(2). In Fig. 5 we plot the performance of the dual of quasi-cyclic codes obtained from power residue codes. These include the (72,9), (88,11) and (150,15) code derived from the octic and 10th power residue codes based on the primes 73, 89 and 151.

It is clear from Fig. 5 that significant coding gains can be realized by the use of low rate quasi-cyclic codes.

5.3 High Rate Codes

In Fig. 6 we provide the performance curves for some selected high rate codes. The (30,20) code is generated by $c_1(x) = 57$ and $c_2(x) = 726$ while the (54,36) code is generated by $c_1(x) = 400166$ and $c_2(x) = 475271$.

The (68,51) code is derived from the (85,68) cyclic code of MacWilliams and is generated by $c_1(x) = 42412$, $c_2(x) = 41144$ and $c_3(x) = 540014$.

The (150,135) code is derived from the (151,136) 10th power residue (ref. 20). A comparison with Fig. 2 in Appendix A of (ref. 6) reveals that this is the best known linear code to date. The best known nonlinear code, due to Preparata has the same minimum distance (ref. 21).

At present there is no soft-decision decoding algorithm for these high rate codes. However, using the results outlined in (refs. 2,22), it may be possible to devise a suitable soft-decision algorithm. In any event, Fig. 6 will serve as a bench mark for comparing the performance of any other code (block or convolutional) of similar dimensions and complexity.

6.0 DISCUSSION

In this paper we have presented a class of block codes. Many of these are soft-decision decodable. Useful coding gains are achievable on the Gaussian channel, and these are expected to be even greater for a burst-and-random channel.

Hardware implementation of the proposed codes should not prove difficult. Once the signal is quantized all data and reliability information can be manipulated using standard logic techniques. For more complex schemes involving finer quantization or more powerful codes, decoder complexity is likely to rise sharply. Assuming that data rate permits, currently available LSI microcomputers may provide a means of realizing such decoders, being well suited to the complex bit manipulations and decisions involved.

ACKNOWLEDGEMENTS

The support of the authors' research by the Natural Sciences and Engineering Research Council of Canada and by le Programme de Formation de Chercheurs et d'Action Concertée du Gouvernement du Québec is gratefully acknowledged.

The authors would like to thank Mr. Binh Nguyen for his computer work.

REFERENCES

1. V.K. Bhargava, D. Haccoun, R. Matyas and P.P. Nuspl, Digital Communications by Satellite. New York: Wiley, 1981.
2. G. Solomon and H.C.A. van Tilborg, "A connection between block and convolutional codes", SIAM J. Appl. Math., vol. 37, pp. 358-369, 1979.
3. V.K. Bhargava, "Soft decoding performance of extremal self-dual codes", Proc. IEEE, vol. 71, pp. 183-184, 1983.
4. V.K. Bhargava, "Forward error correction schemes for digital communications", IEEE Communications Magazine, vol. 21, pp. 11-19, 1983.
5. W.W. Peterson and E.J. Weldon, Jr., Error Correcting Codes, Second Edition, Cambridge, MA: MIT Press, 1972.
6. F.J. MacWilliams and N.J.A. Sloane, The Theory of Error Correcting Codes, Amsterdam, North Holland and New York: Elsevier/North Holland, 1977.
7. V.K. Bhargava, G. Young and A.K. Bhargava, "A characterization of the (56,28) extremal self-dual code", IEEE Trans. Inf. Theory, IT-27, pp. 258-260, 1981.
8. V.K. Bhargava and C. Nguyen, "Circulant codes based on the prime 29", IEEE Trans. Inf. Theory, IT-26, pp. 363-364, 1980.
9. V.K. Bhargava and C. Nguyen, "Weight distribution of some cyclic codes of MacWilliams", in D.G. Lainiotis and N.S. Tzannes (eds.), Advances in Communications, pp. 117-122, D. Reidel Publishing Company, Holland, 1980.
10. V.K. Bhargava, G.E. Séguin and J.M. Stein, "Some (mk,k) cyclic codes in quasi-cyclic form", IEEE Trans. Inf. Theory, IT-24, pp. 630-633, 1978.
11. J.M. Stein, V.K. Bhargava and S.E. Tavares, "Weight distribution of some best (3m,2m) binary quasi-cyclic codes", IEEE Trans. Inf. Theory, IT-21, pp. 708-711, 1975.
12. J.M. Stein and V.K. Bhargava, "Equivalent rate 1/2 quasi-cyclic codes", IEEE Trans. Inf. Theory, IT-21, pp. 588-589, 1975.
13. V.K. Bhargava, "Odd weight symmetry in some binary codes", IEEE Trans. Inf. Theory, IT-23, pp. 518-520, 1977.
14. C.L. Mallows and N.J.A. Sloane, "An upper bound for self-dual codes", Information and Control, vol. 22, pp. 188-200, 1973.
15. N.J.A. Sloane, "Is there a (72,36) d = 16 self-dual code?", IEEE Trans. Inf. Theory, IT-19, p. 251, 1973.
16. R.J. McEliece, "The Theory of Information and Coding", Reading, MA: Addison-Wesley, 1977.
17. F.J. MacWilliams, "Decomposition of cyclic codes of block lengths 3p,5p,7p", IEEE Trans. Inf. Theory, IT-25, pp. 112-118, 1979.
18. E.R. Berlekamp, Algebraic Coding Theory, New York: McGraw-Hill, 1968.
19. C.L. Chen, W.W. Peterson and E.J. Weldon, Jr., "Some results on quasi-cyclic codes", Information and Control, vol. 15, pp. 407-423, 1969.
20. V.K. Bhargava, "The (151,136) 10th power residue code and its performance", Proc. IEEE, vol. 71, 1983 (to appear).
21. F.P. Preparata, "A class of optimum nonlinear double-error correcting codes", Information and Control, vol. 13, pp. 378-400, 1968.
22. J.K. Wolf, "Efficient maximum likelihood decoding of linear block codes using a trellis", IEEE Trans. Inf. Theory, IT-24, pp. 76-80, 1978.

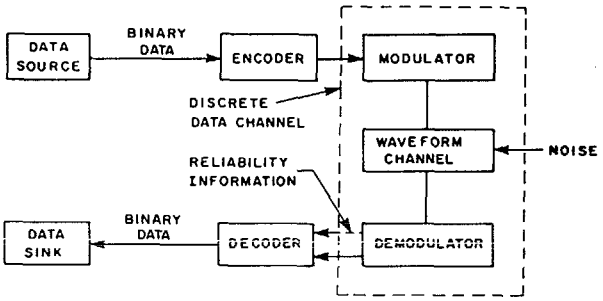

Fig. 1. Digital communication process using forward error correction.

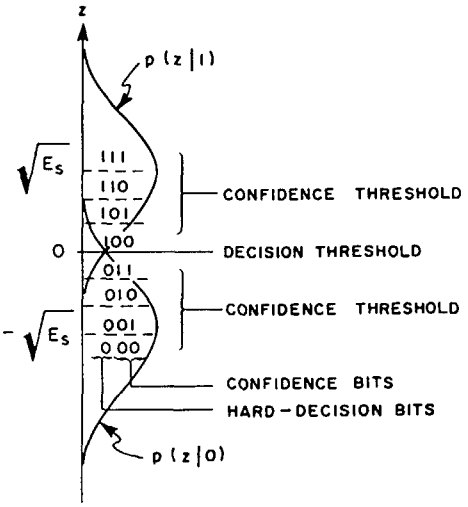

Fig. 2. Three bit (8-level) soft-decision quantization. $p(z|1)$ and $p(z|0)$ are conditional probability density functions of the matched filter output for CPSK.

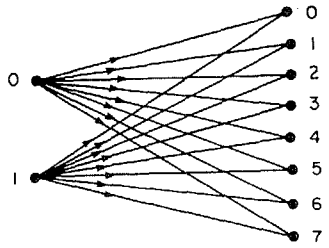

Fig. 3. Eight level soft quantized DMC produced by a three bit quantizer on a Gaussian channel.

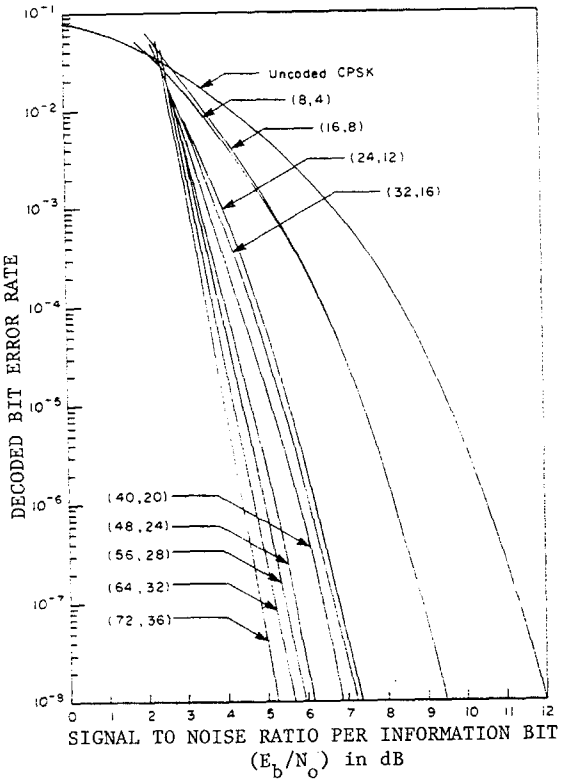

Fig. 4. Performance of several extremal self-dual codes over the Gaussian channel (CPSK modulation).

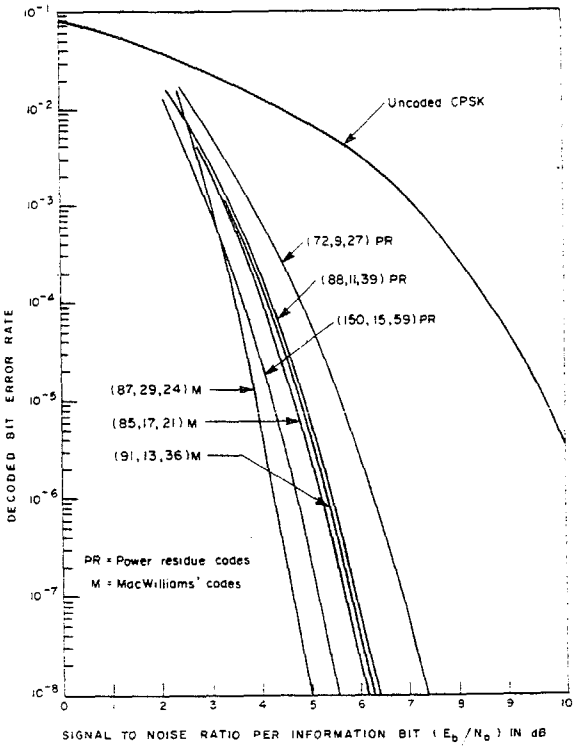

Fig. 5. Performance of several low rate quasi-cyclic codes over the Gaussian channel (CPSK modulation).

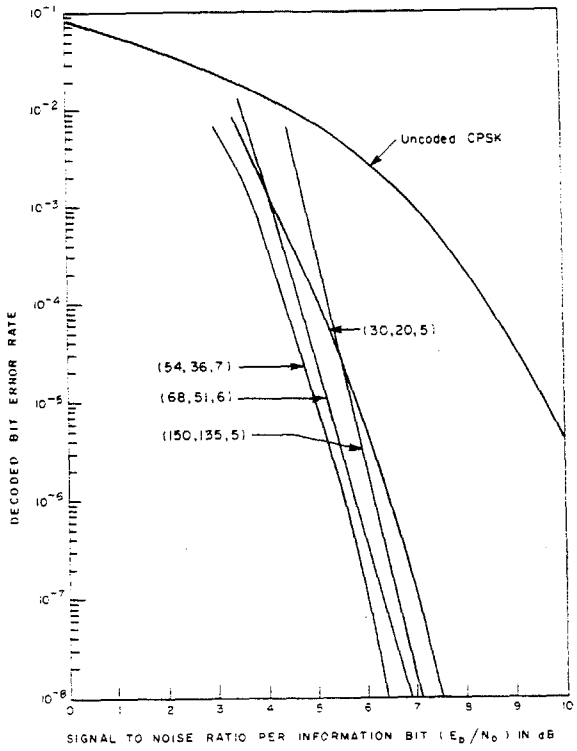

Fig. 6. Performance of some high rate quasi-cyclic codes over the Gaussian channel (CPSK modulation).