GODDARD GRANT
IN-32-CR
111331
48P

Bandwidth Efficient Block Codes for M-ary PSK Modulation

(NASA-CR-181543) BANDWIDTH EFFICIENT BLOCK CODES FOR M-ary PSK MODULATION (Hawaii Univ.) 48 p CSCL 17B

N88-12712

Unclas
G3/32 0111331

Technical Report
to
NASA
Goddard Space Flight Center
Greenbelt, Maryland 20771

Grant Number NAG 5-931

Shu Lin
Principal Investigator
Department of Electrical Engineering
University of Hawaii at Manoa
Honolulu, Hawaii 96822

December 31, 1987

Bandwidth Efficient Block Codes for M-ary PSK Modulation

Tadao Kasami
Osaka University
Toyonaka, Osaka 560, Japan

Shu Lin
University of Hawaii
Honolulu, Hawaii 96822

ABSTRACT

In this report, a class of bandwidth efficient block codes for M-ary PSK modulation is presented. A soft-decision decoding for this class of codes is devised. Some specific short codes for QPSK, 8-PSK and 16-PSK modulations are constructed. These codes have good minimum squared Euclidean distances and provide 2 to 5.8 dB coding gains over uncoded QPSK modulation without (or with little) bandwidth expansion. The complete weight distributions of these specific codes are determined. Based on these weight distributions, their error probabilities are evaluated. Some of these codes have simple trellis structures and hence can be decoded by Viterbi decoding algorithm with relatively simple implementation. Moreover the codes are very suitable for use as inner codes for various cascaded coding schemes with Reed-Solomon codes as outer codes.

Bandwidth Efficient Block Codes for M-ary PSK Modulation

1. Introduction

Recently a great deal of research effort has been expended in bandwidth efficient coded modulations for achieving reliable communications on band-limited channels [1-27]. This new technique of coded modulation is achieved by coding onto an expanded set of channel signals (relative to that needed for uncoded transmission). Coded modulation can provide significant coding gain over an uncoded system with little or no bandwidth expansion. Most of the research works on coded modulation has been focused on trellis coded modulations (TCM), i.e., trellis (convolutional) coding with expanded signal sets. Not much has been done on block coded modulations.

In this report, we investigate block coding for M-ary PSK modulation. First we present a generalization of coset codes over binary lattices [20] to codes over additive groups. From this generalization, a method for constructing block coded M-ary PSK codes is devised. Then a soft-decision decoding algorithm for these M-ary codes is provided. Some specific QPSK, 8-PSK and 16-PSK codes with good minimum squared Euclidean distances and trellis structure are constructed. These codes provide 2 to 5.8 dB coding gains over uncoded QPSK modulation. Complete weight distributions of these codes are derived. Based on these weight distributions, we are able to analyze the error performance of these codes for an AWGN channel. Upper bounds on the error probabilities are obtained. Since these codes have simple trellis structure, they can be decoded with Viterbi decoding.

In our next report, we will investigate various cascaded coding schemes with bandwidth efficient M-ary PSK codes constructed in this report as the inner code. Preliminary results show that large coding gains can be achieved over the uncoded QPSK modulation.

2. Code Construction over Additive Groups

Let A be an additive group (finite or infinite) on which a distance between two elements s and s', denoted d(s,s'), is defined. The distance measure, d(s, s'), satisfies the following conditions:

$$1. \qquad d(s,s') = d(s-s',0), \tag{2.1}$$

where 0 denotes the zero element in A, and

$$2. \qquad d(s,s') = 0 \quad \text{if and only if } s = s'. \tag{2.2}$$

Let $B_1, B_2, \cdots, B_\ell$ be ℓ nonempty finite subsets of A for which the following unique decomposition property holds : for s_i and s_i' in B_i,

$$s_1 + s_2 + \cdots + s_\ell = s_1' + s_2' + \cdots + s_\ell', \tag{2.3}$$

if and only if $s_i = s_i'$ for $1 \leq i \leq \ell$. Let S be defined as

$$\begin{aligned} S &\triangleq B_1 + B_2 + \cdots + B_\ell \\ &= \{ s_1 + s_2 + \cdots + s_\ell : s_i \in B_i \text{ with } 1 \leq i \leq \ell \}. \end{aligned} \tag{2.4}$$

Clearly S is a subset of A.

For a nonempty finite subset B of A, let d[B] denote the minimum distance between elements of B. If B has only one element, let d[B] be defined as ∞. For $1 \leq i \leq \ell$, let d_i be defined as follows:

$$d_i = d[B_i + B_{i+1} + \cdots + B_\ell]. \tag{2.5}$$

For a positive integer n, let A^n denote the set of all n-tuples over A. Define the distance between two n-tuples $\bar{s} = (s_1, s_2, \cdots, s_n)$ and $\bar{s}' = (s_1', s_2', \cdots, s_n')$ over A, denoted $d^{(n)}(\bar{s},\bar{s}')$, as

$$d^{(n)}(\bar{s},\bar{s}') = \sum_{j=1}^{n} d(s_j,s_j'). \tag{2.6}$$

The sum of two n-tuples over A is defined as the component-wise sum of the two n-tuples. For $1 \le i \le \ell$, let C_i be a block code of length n over B_i with minimum Hamming distance δ_i. From $C_1, C_2, \cdots, C_\ell$, a block code C of length n over S is constructed as follows:

$$C = \{\bar{v}_1+\bar{v}_2+ \cdots + \bar{v}_\ell : \bar{v}_i \in C_i \text{ for } 1 \le i \le \ell\}. \tag{2.7}$$

We will use the following expression for C,

$$C = C_1 + C_2 + \cdots + C_\ell.$$

Let $|X|$ denote the number of elements in a finite set X. Then

$$|C| = \prod_{i=1}^{\ell} |C_i|. \tag{2.8}$$

Lemma 1 provides a lower bound on the minimum distance of the block code C.

Lemma 1: The minimum distance of C with respect to $d^{(n)}$, denoted D[C], is lower-bounded as follows:

$$D[C] \geq \min_{1 \leq i \leq \ell} \delta_i d_i \tag{2.9}$$

<u>Proof</u>: For different $\bar{v}$ and $\bar{v}'$ in C, let $\bar{v}$ and $\bar{v}'$ be expressed as

$$\begin{aligned} \bar{v} &= \bar{v}_1 + \bar{v}_2 + \cdots + \bar{v}_\ell, \quad \bar{v}_i \in C_i, \\ \bar{v}' &= \bar{v}'_1 + \bar{v}'_2 + \cdots + \bar{v}'_\ell, \quad \bar{v}'_i \in C_i, \end{aligned} \tag{2.10}$$

where

$$\begin{aligned} \bar{v}_i &= (s_{i1}, s_{i2}, \cdots, s_{in}), \quad s_{ij} \in B_i, \\ \bar{v}'_i &= (s'_{i1}, s'_{i2}, \cdots, s'_{in}), \quad s'_{ij} \in B_i, \end{aligned} \tag{2.11}$$

with $1 \leq i \leq \ell$ and $1 \leq j \leq n$. Let h denote the first suffix such that

$$\bar{v}_h \neq \bar{v}'_h. \tag{2.12}$$

Then, since the minimum Hamming distance of C_h is δ_h, there exist δ_h suffices $1 \leq j_1 < j_2 < \cdots < j_{\delta_h} \leq n$ such that

$$s_{hj_p} \neq s'_{hj_p}, \quad \text{for } 1 \leq p \leq \delta_h. \tag{2.13}$$

Since $s_{ij} = s'_{ij}$ for $1 \leq i < h$ and $1 \leq j \leq n$, we have that, for $1 \leq p \leq \delta_h$,

$$d(\sum_{i=1}^{\ell} s_{ij_p}, \sum_{i=1}^{\ell} s'_{ij_p}) \geq d[\sum_{i=1}^{h-1} s_{ij_p} + B_h + B_{h+1} + \cdots + B_\ell]. \tag{2.14}$$

It follows from (2.1), (2.5) and (2.14) that, for $1 \le p \le \delta_h$

$$d\left(\sum_{i=1}^{\ell} s_{ij_p}, \sum_{i=1}^{\ell} s'_{ij_p}\right) \ge d_h . \tag{2.15}$$

Since $d^{(n)}(\bar{v},\bar{v}') = \sum_{j=1}^{n} d\left(\sum_{i=1}^{\ell} s_{ij}, \sum_{i=1}^{\ell} s'_{ij}\right)$, we have that

$$d^{(n)}(\bar{v},\bar{v}') \ge \delta_h d_h \ge \min_{1\le i\le \ell} \delta_i d_i . \tag{2.16}$$

■■

3. Construction of Block Codes for M-ary PSK Modulation

In this section, we consider code construction for M-ary PSK modulation where

$$M = 2^{\ell} . \tag{3.1}$$

Let

$$A = \{ 0, 1, 2, \cdots , M\text{-}1\} \tag{3.2}$$

be the integer group under the modulo-M addition. Define a distance between two elements s and s' in A as follows:

$$d(s,s') = 4\sin^2(2^{-\ell}\pi(s-s')) . \tag{3.3}$$

It is clear that $d(s,s') = d(s\text{-}s',0)$ and $d(s,s) = 0$. For $1 \le i \le \ell$, let

$$B_i = \{ 0, 2^{i-1}\}. \tag{3.4}$$

Then, $B_1, B_2, \cdots, B_\ell$ have the unique decomposition property which is related to standard binary representation of an nonnegative integer. Note that

$$A = B_1 + B_2 + \cdots + B_\ell. \tag{3.5}$$

Then, it follows from (2.5), (3.3) and (3.4) that

$$d_i = 4\sin^2(2^{i-1-\ell}\pi), \text{ for } 1 \le i \le \ell. \tag{3.6}$$

Since $|B_i|=2$ for $1 \le i \le \ell$, a block code over B_i with minimum Hamming distance δ_i can be derived from a binary block code C_b of the same code length with the same minimum Hamming distance δ_i by substituting 2^{i-1} for 1 in each component of a codeword in C_b. The code over B_i will be denoted by $2^{i-1}C_b$.

Suppose that C_{bi} is a binary linear (n,k_{bi}) code with minimum Hamming distance δ_i for $1 \le i \le \ell$. Let C denote the sum code, $C_{b1} + 2C_{b2} + \cdots + 2^{\ell-1}C_{b\ell}$. C is linear code over A. C_{bi} is called a binary component code of C. It follows from (2.8) that

$$|C| = 2^{\sum_{i=1}^{\ell} k_{bi}}. \tag{3.7}$$

Let $\bar{s}$ and $\bar{s}'$ be two n-tuples over the group A. It follows from the definition of $d^{(n)}(\bar{s},\bar{s}')$ given by (2.6) and the definition of $d(\bar{s},\bar{s}')$ given by (3.3) that $d^{(n)}(\bar{s},\bar{s}')$ is simply a squared Euclidean distance between the two n-tuples $\bar{s}$ and $\bar{s}'$ over A. The minimum squared Euclidean distance (MSED) of code C is then given by

$$D[C] \triangleq \min\{d^{(n)}(\bar{v},\bar{v}') : \bar{v}, \bar{v}' \in C \text{ and } \bar{v} \neq \bar{v}'\}. \tag{3.8}$$

It follows from Lemma 1, (2.9), (3.6) and (3.8) that

$$D[C] \geq \min_{1 \leq i \leq \ell} 4\delta_i \sin^2(2^{i-1-\ell}\pi). \tag{3.9}$$

If each component of a code vector $\bar{v}$ in C is mapped into a point in the 2-dimensional 2^{ℓ}-PSK signal set, we obtain a block coded 2^{ℓ}-PSK code. The effective rate of this code is given by

$$R[C] = \frac{1}{2n} \sum_{i=1}^{\ell} k_{bi} \; . \tag{3.10}$$

which is the number of information bits transmitted by C per dimension. Let C_s denote a standard reference code. The asymptotic code gain of C, denoted $\gamma[C]$, over the reference code is given by [8,20]

$$\gamma[C] = 10\log_{10} \frac{R[C]D[C]}{R[C_s]D[C_s]} \; . \tag{3.11}$$

If the uncoded QPSK is used as the reference code C_s, then $R[C_s] = 1$, $D[C_s] = 2$ and

$$\gamma[C] = 10\log_{10} \frac{R[C]D[C]}{2} \; . \tag{3.12}$$

The asymptotic coding gain is used as a simple measure of the performance of a code. To analyze the performance of a code in details, we need to know the complete weight distribution of C.

Let $\bar{v} = (v_1, v_2, \cdots, v_n)$ be an n-tuple over the group A. The composition of $\bar{v}$, denoted comp($\bar{v}$), is a M-tuple

$$\bar{t} = (t_0, t_1, \cdots, t_{M-1})$$

where t_i is the number of components v_j in $\bar{v}$ equal to the integer i in A. Let $W(\bar{t})$ be the number of codewords $\bar{v}$ in C with $\text{comp}(\bar{v}) = \bar{t}$. Let T be the set

$$T = \{(t_0, t_1, \cdots, t_{M-1}) : 0 \leq t_i \leq n \text{ with } 0 \leq i < M\}. \tag{3.13}$$

Then

$$\{W(\bar{t}) : \bar{t} \in T\} \tag{3.14}$$

is the detail weight distribution of C. Once this weight distribution is known, the error performance of C can be analyzed and computed.

$W(\bar{t})$ can be enumerated from the joint weight distribution [28] of the binary component codes, $C_{b1}, C_{b2}, \cdots, C_{b\ell}$. For a binary ℓ-tuple $\bar{h} = (h_1, h_2, \cdots, h_\ell) \in \{0,1\}^\ell$ and binary vectors $\bar{v}_i = (v_{i1}, v_{i2}, \cdots, v_{in})$ with $1 \leq i \leq \ell$, let

$$\text{comp}(\bar{h}; \bar{v}_1, \bar{v}_2, \cdots, \bar{v}_\ell) \tag{3.15}$$

denote the number of j's such that $v_{ij} = h_i$ for $1 \leq i \leq \ell$. For nonnegative integers $t_0, t_1, \cdots, t_{M-1}$, let

$$W_J(t_0, t_1, \cdots, t_{M-1}) \tag{3.16}$$

denote the number of ℓ-tuples,

$$(\bar{v}_1, \bar{v}_2, \cdots, \bar{v}_\ell)$$

with $\bar{v}_i \in C_{bi}$ for $1 \leq i \leq \ell$ such that

$$\mathrm{comp}(\bar{h}; \bar{v}_1, \bar{v}_2, \cdots, \bar{v}_\ell) = t_h$$

for $0 \leq h < M$, where $\bar{h}$ is the standard binary representation of integer h. It follows from the construction of C that

$$W((t_0, t_1, \cdots, t_{M-1})) = W_J(t_0, t_1, \cdots, t_{M-1}). \tag{3.17}$$

The set,

$$\{ W_J(t_0, t_1, \cdots, t_{M-1}) \}$$

is the joint weight distribution of the binary component codes, $C_{b1}, C_{b2}, \cdots, C_{b\ell}$.

If a maximum likelihood decoding algorithm is used, it is desirable for a code to have a simple trellis structure [20]. A trellis diagram of C is a direct product of those of binary component codes $C_{b1}, C_{b2}, \cdots, C_{b\ell}$. The number of states of a trellis diagram of a binary (n,k) code is upper-bounded by [29]

$$2^{\min\{k, n-k\}}. \tag{3.18}$$

Some codes may have a trellis diagram with smaller number of states than the bound. For instance, the (16,11) Reed-Muller code has a 4-section trellis diagram with 8 states [20]. The number of states depends on the order of bit positions. It can be proved based on Appendix 1 in [20] that the number of states is equal to (3.18) for any n-section trellis diagram of a shortened cyclic code. The order of bit positions should be chosen in a clever way.

The code construction presented in this section is actually a generalization of Sayegh's [26].

4. Some Specific Block Codes for QPSK, 8-PSK and 16-PSK

In this section, we construct some block codes for QPSK, 8-PSK and 16-PSK modulations. These codes have good minimum squared Euclidean distances. Some of these codes have simple trellis structure and hence can be decoded by Viterbi decoding algorithm. The codes are constructed in such a way that they are suitable for being used as inner codes of various cascaded coding schemes with outer codes over GF(2^8). For QPSK, the signal set is shown in Figure 1. The construction of QPSK codes is based on the additive group, $A_4 = \{0, 1, 2, 3\}$, modulo-4 with $B_1 = \{0, 1\}$ and $B_2 = \{0, 2\}$. It follows from (3.6) that the distances between signal points are :

$$d_1 = 2, \quad d_2 = 4. \tag{4.1}$$

For 8-PSK, the signal set is shown in Figure 2. The symbols for 8-PSK codes are from the group, $A_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$, modulo-8 addition. $B_1 = \{0, 1\}$, $B_2 = \{0, 2\}$ and $B_3 = \{0, 4\}$ are chosen to be the symbol sets for the component codes. From (3.6), we find the distances between signal points are:

$$d_1 = 0.586, \quad d_2 = 2, \quad d_3 = 4. \tag{4.2}$$

For 16-PSK, the signal set is shown in Figure 3. The 16-PSK codes have symbols from the group, $A_{16} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15\}$, under modulo-16 addition. The four component codes have symbols from $B_1 = \{0, 1\}$, $B_2 = \{0, 2\}$ and $B_3 = \{0, 4\}$ and $B_4 = \{0, 8\}$ respectively. From (3.6) we find that the distances between signal points are $d_1 = 0.152$, $d_2 = 0.586$, $d_3 = 2$ and $d_4 = 4$.

Let P_n denote the (n,n–1) linear binary code which consists of all the even weight vectors. The minimum Hamming distance of P_n is 2. Let $P_n^{\perp}$ denote the dual code of P_n. Then $P_n^{\perp}$ is the (n,1) code which consists of the all-zero and all one vectors. The minimum Hamming distance of $P_n^{\perp}$ is n. Let H_{2^m-1} denote the even-weight subcode of the binary $(2^m-1, 2^m-m-1)$ Hamming code. Then the minimum distance of H_{2^m-1} is 4. In the following, we present a sequence of specific codes for QPSK, 8-PSK and 16-PSK.

Example 1: Let $\ell = 2$, $M = 2^2 = 4$ and $n = 5$. We choose $C_{b1} = P_2 \times P_3$ and $C_{b2} = \{0,1\}^5$ as the two binary component codes where $P_2 \times P_3$ is the cartesian product of P_2 and P_3. The binary component code C_{b1} is a (5, 3) code with minimum Hamming distance $\delta_1 = 2$. The second binary component code C_{b2} is simply the (5, 5) code. Let

$$C_{Q,1}^{(2)} \triangleq C_{b1} + 2C_{b2}.$$

Then $C_{Q,1}^{(2)}$ is a QPSK code over the additive group $A_4 = \{0, 1, 2, 3\}$ with the following parameters:

$$|C_{Q,1}^{(2)}| = 2^8, \tag{4.3}$$

$$D[C_{Q,1}^{(2)}] = 4, \tag{4.4}$$

$$R[C_{Q,1}^{(2)}] = \frac{4}{5}, \tag{4.5}$$

$$\gamma = 10\log_{10}\frac{8}{5} = 2.0(\text{dB}). \tag{4.6}$$

This QPSK code maps a 8-bit message into a sequence of 5 symbols over A_4. Each of these 5 symbols is then mapped into a two-dimensional signal point in the QPSK signal set shown in Figure 1. The QPSK code $C_{Q,1}^{(2)}$ can be shown to have a trellis diagram with two states.

Example 2: Let $\ell = 2$, $M = 2^2 = 4$ and $n = 15$. Chose $C_{b1} = H_{15}$ and $C_{b2} = P_{15}$ be the binary component codes. Then the minimum Hamming distances of C_{b1} and C_{b2} are $\delta_1 = 4$ and $\delta_2 = 2$ respectively. Let

$$C_{Q,3}^{(4)} \triangleq C_{b1} + 2C_{b2}.$$

Then $C_{Q,3}^{(4)}$ is a QPSK code with the following parameters:

$$|C_{Q,3}^{(4)}| = 2^{24}, \tag{4.7}$$

$$D[C_{Q,3}^{(4)}] = 8, \tag{4.8}$$

$$R[C_{Q,3}^{(4)}] = \frac{4}{5}, \tag{4.9}$$

$$\gamma = 10\log_{10}\frac{16}{5} = 5.0(\text{dB}). \tag{4.10}$$

Since H_{15} is obtained by truncating the (16,11) Reed-Muller code, the component code C_{b1} has a 4-section trellis diagram with 8 states[20]. The component code C_{b2} has a trellis of two states.

The detail weight distribution of the QPSK code $C_{Q,3}^{(4)}$ can be evaluated easily. For integers i, j and h such that i and j are even, $0 \le h \le i < 15$ and $0 \le h \le j \le 15-i+h$,

$$W((15-i-j+h,\ i-h,\ j-h,\ h)) = A_{H,i}\binom{i}{h}\binom{15-i}{j-h}, \tag{4.11}$$

where $A_{H,i}$ denotes the number of codewords in H_{15} with weight i. For other composition, $\bar{t} = (t_0, t_1, t_2, t_3)$,

$$W(\bar{t}) = 0. \tag{4.12}$$

In the next 5 examples, we present specific codes for 8-PSK modulation.

<u>**Example 3**</u>: Let $\ell = 3$, $M = 2^3 = 8$, $n = 8$. Choose $C_{b1} = P_8^{\perp}$, $C_{b2} = P_8$ and $C_{b3} = \{0, 1\}^8$ as the 3 binary component codes. The minimum Hamming distances of C_{b1}, C_{b2} and C_{b3} are $\delta_1 = 8$, $\delta_2 = 2$ and $\delta_3 = 1$ respectively. Let

$$C_{8,2}^{(2)} \triangleq C_{b1} + 2C_{b2} + 4C_{b3}.$$

Then $C_{8,2}^{(2)}$ is a 8-PSK code with symbols from $A_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$. $C_{8,2}^{(2)}$ has the following parameters:

$$|C_{8,2}^{(2)}| = 2^{16}, \tag{4.13}$$

$$D[C_{8,2}^{(2)}] = 4, \tag{4.14}$$

$$R[C_{8,2}^{(2)}] = 1, \tag{4.15}$$

$$\gamma = 10\log_{10} 2 = 3(\text{dB}). \tag{4.16}$$

Note that this code provides a 3 dB (asymptotic) coding gain over the uncoded QPSK modulation without bandwidth expansion. C_{b1} and C_{b2} both have trellis diagrams with two states. $C_{8,2}^{(2)}$ has an 8-section trellis diagram of 4 states as shown in Figure 4 (see Appendix A for construction).

Hence it can be decoded with Viterbi decoding algorithm. The implementation should be rather simple. This block 8-PSK code may be considered to be equivalent to Ungerboeck's 4-state trellis code for 8-PSK modulation which has squared minimum free Euclidean Distance $d_f^2 = 4$ [8].

The complete weight distribution of the 8-PSK code $C_{8,2}^{(2)}$ can be evaluated from the joint weight distribution of its binary component code. For integers i, j and h such that i are even, $0 \le j \le i \le 8$ and $0 \le h \le 8-i$,

$$W((h, 0, j, 0, 8-i-h, 0, i-j, 0)) = W((0, h, 0, j, 0, 8-i-h, 0, i-j))$$

$$= \binom{8}{i}\binom{i}{j}\binom{8-i}{h}. \tag{4.17}$$

For other composition $\bar{t} = (t_0, t_1, t_2, t_3, t_4, t_5, t_6, t_7)$,

$$W(\bar{t}) = 0. \tag{4.18}$$

For its bandwidth efficiency, coding gain and simplicity in implementation, $C_{8,2}^{(2)}$ is extremely suitable for use as the inner code for a cascaded coding scheme with the NASA standard (255,223) RS code over $GF(2^8)$ as the outer code. Our preliminary results show that large coding gain can be achieved by such a cascaded coding scheme.

Example 4: Let $\ell = 3$, $M = 2^3 = 8$ and $n = 23$. Consider the 8-PSK code $C_{8,7}^{(2)}$ with binary component codes C_{b1}, C_{b2} and C_{b3} where C_{b1} is the (23,12) Golay code and $C_{b2}=C_{b3}=P_{23}$. The minimum Hamming distances of C_{b1}, C_{b2} and C_{b3} are $\delta_1 = 7$, $\delta_2 = \delta_3 = 2$ respectively. Then

$$C_{8,7}^{(2)} \triangleq C_{b1}+2C_{b2}+4C_{b3}$$

has the following parameters:

$$|C_{8,7}^{(2)}| = 2^{56}, \tag{4.19}$$

$$D[C_{8,7}^{(2)}] = 4, \tag{4.20}$$

$$R[C_{8,7}^{(2)}] = \frac{28}{23}, \tag{4.21}$$

$$\gamma = 10\log_{10}\frac{56}{23} = 3.8(\text{dB}). \tag{4.22}$$

C_{b1} has a 3-section trellis diagram with 2^6 states[20]. The complete weight enumerator of $C_{8,7}^{(2)}$ can be derived from the Hamming weight enumerator of the (23,12) Golay code.

Example 5: Let $\ell = 3$, $M = 2^3 = 8$, $n = 15$. Let C_{b1}, C_{b2} and C_{b3} be the shortened (15,4) Reed-Muller code, P_{15} and $\{0, 1\}^{15}$, respectively. Then, $\delta_1 = 8$, $\delta_2 = 2$ and $\delta_3 = 1$. Let

$$C_{8,4}^{(2)} \triangleq C_{b1}+2C_{b2}+4C_{b3}.$$

Then $C_{8,4}^{(2)}$ is an 8-PSK code with the following parameters:

$$|C_{8,4}^{(2)}| = 2^{33}, \tag{4.23}$$

$$D[C_{8,4}^{(2)}] = 4, \tag{4.24}$$

$$R[C_{8,4}^{(2)}] = \frac{11}{10}, \tag{4.25}$$

$$\gamma = 10\log_{10}\frac{11}{5} = 3.4(\text{dB}). \tag{4.26}$$

C_{b1} has a 4-section trellis diagram with 8 states[20]. The complete weight enumerator of $C_{8,4}^{(2)}$ can be derived from the Hamming weight enumerator of the shortened (15,4) Reed-Muller code.

Example 6: Let $\ell = 3$, $M = 2^3 = 8$ and $n = 4m+3$ where $4 \le m \le 7$. Let C_{b1}, C_{b2} and C_{b3} be $P_n^{\perp}$, the shortened $(n,n-6)$ code of H_{31} and P_n, respectively. Then, $\delta_1 = n$, $\delta_2 = 4$ and $\delta_3 = 2$. Let

$$C_{8,m}^{(4)} \triangleq C_{b1}+2C_{b2}+4C_{b3}.$$

Then $C_{8,m}^{(4)}$ is an 8-PSK code with the following parameters:

$$|C_{8,m}^{(4)}| = 2^{8m}, \tag{4.27}$$

$$D[C_{8,m}^{(4)}] = 8, \tag{4.28}$$

$$R[C_{8,m}^{(4)}] = \frac{4m}{4m+3}, \tag{4.29}$$

$$\gamma = 10\log_{10}\frac{16m}{4m+3}\ . \qquad (4.30)$$

The complete weight distribution of $C_{8,m}^{(4)}$ is known. For integers i, j and h such that i and j are even, $0 \le h \le i \le n$ and $0 \le h \le j \le n-i+h$,

$$W((n-i-j+h,\ 0,\ i-h,\ 0,\ j-h,\ 0,\ h,\ 0\ ))$$

$$= W((\ 0,\ n-i-j+h,\ 0,\ i-h,\ 0,\ j-h,\ 0,\ h\ ))$$

$$= A_{H,n,i}\binom{i}{h}\binom{n-i}{j-h}, \qquad (4.31)$$

where $A_{H,n,i}$ denotes the number of codewords in C_{b2} with weight i. For other composition $\bar{t} = (\ t_0, t_1, t_2, t_3, t_4, t_5, t_6, t_7\ )$,

$$W(\bar{t}) = 0. \qquad (4.32)$$

C_{b1} and C_{b3} have trellis-diagrams with two states. Since C_{b2} is derived by shortening the (32,26) Reed-Muller code, it has a 4-section trellis diagram with 16 states [20].

Example 7: Let $\ell = 3$, $M = 2^3 = 8$ and $n = 29$. Let C_{b1} is the linear (29,5) code which is obtained from the (32,6) Reed-Muller code of minimum weight 16 by first deleting two redundant bits and then truncating one information bit. The minimum weight of C_{b1} is at least 14. Let C_{b2} be the linear (29,23) code obtained from H_{31} by truncating two information bits, and C_{b3} be P_{29}. Then $\delta_2 \ge 4$ and $\delta_3 = 2$. Let

$$C_{8,7}^{(4)} \triangleq C_{b1}+2C_{b2}+4C_{b3}.$$

Then $C_{8,7}^{(4)}$ is an 8-PSK code with the following parameters:

$$|C_{8,7}^{(4)}| = 2^{56}, \tag{4.33}$$

$$D[C_{8,7}^{(4)}] = 8, \tag{4.34}$$

$$R[C_{8,7}^{(4)}] = \frac{28}{29}, \tag{4.35}$$

$$\gamma = 10\log_{10}\frac{112}{29} = 5.8(\mathrm{dB}). \tag{4.36}$$

Each of C_{b1} and C_{b2} has a trellis diagram with 16 states.

__Example 8__: In this example, we construct a code for 16-PSK modulation. The code has symbols from the group, $A_{16} = \{0, 1, 2, \cdots, 15\}$, modulo-16. The four binary component codes, C_{b1}, C_{b2}, C_{b3} and C_{b4}, used in the construction are $P_{32}^{\perp}$, the second-order (32,16) Reed-Muller code, P_{32} and $\{0,1\}^{32}$, respectively. Let

$$C_{16,10}^{(2)} \triangleq C_{b1}+2C_{b2}+4C_{b3}+8C_{b4}.$$

Then $C_{16,10}^{(2)}$ is a 16-PSK code which has the following parameters:

$$|C_{16,10}^{(2)}| = 2^{80}, \tag{4.38}$$

$$D[C_{16,10}^{(2)}] = 4, \tag{4.39}$$

$$R[C^{(2)}_{16,10}] = \frac{5}{4}, \tag{4.40}$$

$$\gamma = 10\log_{10}\frac{5}{2} = 3.9(\text{dB}). \tag{4.41}$$

Since the second-order (32,16) Reed-Muller code has a trellis diagram with 2^6 states [20], $C^{(2)}_{16,10}$ has a trellis diagram with 2^8 states, and is invariant to phase shifts of all multiplies of $\pi/8$.

5. Encoding and Decoding

In this section, we consider the encoding and decoding of the M-ary PSK codes constructed in Section 3 with $M = 2^{\ell}$. Let C denote a M-ary PSK code.

Encoding

In encoding, a k-bit message $\bar{u}$ is divided into ℓ submessages, $\bar{u}_1, \bar{u}_2, \cdots, \bar{u}_{\ell}$ such that the i-th submessage $\bar{u}_i$ consists of k_{bi} bits and $k = k_{b1} + k_{b2} + \cdots + k_{b\ell}$. For $1 \le i \le \ell$, the i-th submessage $\bar{u}_i$ is encoded by the binary component code C_{bi} encoder. Let $\bar{v}_i = (v_{i1}, v_{i2}, \cdots, v_{in})$ be the codeword for $\bar{u}_i$. Then the codeword for the entire message $\bar{u}$ is

$$\bar{v} = (s_1, s_2, \cdots, s_n) = \bar{v}_1 + 2\bar{v}_2 + \cdots + 2^{\ell-1}\bar{v}_{\ell}, \tag{5.1}$$

where

$$s_j = v_{1j} + 2v_{2j} + \cdots + 2^{\ell-1}v_{\ell j}, \tag{5.2}$$

for $1 \le j \le n$. Note that s_j is a symbol in the additive group, $A = \{0, 1, \cdots, 2^{\ell}-1\}$, modulo-$2^{\ell}$. The symbols, $s_1, s_2, \cdots, s_n$ are then modulated (mapped into points in the 2-dimensional 2^{ℓ}-PSK signal set) and transmitted. The overall encoder is shown in Figure 5.

Note that the correspondence between the message $\bar{u}$ and codeword $\bar{v}$ is one-to-one. Let f denote the mapping of $\bar{u}$ onto $\bar{v}$ and f^{-1} denote the inverse mapping of f. Then

$$\bar{v} = f(\bar{u}),$$

and (5.3)

$$\bar{u} = f^{-1}(\bar{v}).$$

The mapping f depends on how to divide the message $\bar{u}$ into ℓ submessages.

<u>Decoding</u>

In the following, we present a soft-decision decoding algorithm for the M-ary PSK code C.

For s in $\{ 0, 1, \cdots, 2^{\ell}-1 \}$, let X(s) and Y(s) be defined as

$$X(s) = \cos(2^{1-\ell}\pi s), \tag{5.4}$$

$$Y(s) = \sin(2^{1-\ell}\pi s). \tag{5.5}$$

For s and s' in $\{ 0, 1, \cdots, 2^{\ell}-1 \}$, it follows from (3.3), (5.4) and (5.5) that

$$d(s,s') = (X(s)-X(s'))^2 + (Y(s)-Y(s'))^2. \tag{5.6}$$

For $1 \leq j \leq n$, let (x_j,y_j) be the normalized output of the coherent demodulator [30] for the j-th symbol of a received vector. The received vector is then represented by the following 2n-tuple:

$$\bar{z} = (x_1, y_1, \cdots, x_n, y_n).$$

For the received vector $\bar{z}$ and a codeword $\bar{v} = (s_1, s_2, \cdots, s_n)$ in C, let $|\bar{z},\bar{v}|^2$ be defined as follows:

$$|\bar{z},\bar{v}|^2 = \sum_{j=1}^{n} (x_j - X(s_j))^2 + (y_j - Y(s_j))^2. \tag{5.7}$$

We assume that the channel is an AWGN channel. When symbol $s \in \{0, 1, \cdots, 2^{\ell}-1\}$ is transmitted, the normalized output (x, y) of a coherent demodulator for 2^{ℓ}-ary PSK is distributed with joint probability density function,

$$p(x,y) = \frac{1}{2\pi\sigma^2} e^{-[(x-X(s))^2 + (y-Y(s))^2]/2\sigma^2}, \tag{5.8}$$

where

$$\sigma^2 = \frac{1}{2\rho}, \tag{5.9}$$

and ρ is the SNR per symbol [30,p.167]. We also assume that every codeword of C is transmitted with the same probability.

Decoding rule: For a received vector $\bar{z}$, choose a codeword $\bar{v}$ in C with minimum $|\bar{z},\bar{v}|^2$. Then the decoded message $\bar{u}$ is given by $\bar{u} = f^{-1}(\bar{v})$.

This decoding rule achieves maximum likelihood decoding for C over an AWGN channel.

If C has a simple trellis structure (the number of states is moderate), the decoding of C can be implemented with Viterbi decoding algorithm.

6. Performance Analysis for Inner Codes

Assume that the channel is an AWGN channel and every codeword of C is transmitted with the same probability. Let P_c be the probability that a decoded vector is error-free and P_{ic} be the probability that a decoded vector is erroneous. Since C is linear over $\{0, 1, \cdots, 2^{\ell}-1\}$ under addition modulo-2^{ℓ} addition, we assume that the zero codeword $\bar{0}$ is transmitted without loss of generality. For a received vector $\bar{z}$, the decoded vector is error-free, if and only if

$$|\bar{z},\bar{v}|^2 > |\bar{z},\bar{0}|^2 \; , \qquad (6.1)^*$$

for every nonzero codeword $\bar{v}$ of C. It follows from (2.6), (3.3), (5.4), (5.5) and (5.7) that the inequality of (6.1) can be rewritten into the following inequality:

$$2\sum_{j=1}^{n} (X(s_j)-1)(x_j-1)+Y(s_j)y_j < \sum_{j=1}^{n} (X(s_j)-1)^2+Y(s_j)^2 = d^{(n)}(\bar{v},\bar{0}) \, . \qquad (6.2)$$

For an n-tuple $\bar{v} = (s_1, s_2, \cdots, s_n)$ over the group $\{0, 1, \cdots, 2^{\ell}-1\}$, let $Q(\bar{v})$ be the set of vectors, $(x_1, y_1, \cdots, x_n, y_n)$, which satisfy the inequality of (6.2). Define Q_c as follows:

$$Q_c \triangleq \bigcap_{\bar{v}\in C_1-\{\bar{0}\}} Q(\bar{v}). \qquad (6.3)$$

Then Q_c is a convex set of 2n dimensional Euclidean space. It follows from (5.8) that

---

* The probability that $|\bar{z},\bar{v}|^2 = |\bar{z},\bar{0}|^2$ is zero, and such a case can be neglected.

$$P_c^{(1)} = \frac{1}{(2\pi\sigma^2)^n} \int \underset{Q_c}{\cdots} \int e^{-\left(\sum_{j=1}^{n}(x_j-1)^2+y_j^2\right)/2\sigma^2} dx_1 dy_1 \cdots dx_n dy_n, \tag{6.4}$$

where the integration is taken over Q_c. Numerical computation of the integral is not feasible unless n is small or Q_c has a simple structure.

The following lemma holds on $Q(\bar{v})$.

<u>Lemma 2</u>: Let $\bar{v} = (s_1, s_2, \cdots, s_n)$, $\bar{v}' = (s_1', s_2', \cdots, s_n')$ and $\bar{v}'' = (s_1'', s_2'', \cdots, s_n'')$ be n-tuples over $\{0, 1, \cdots, 2^{\ell}-1\}$. Then

$$Q(\bar{v}) \cap Q(\bar{v}') \subseteq Q(\bar{v}''),$$

if the following condition (i) or (ii) holds:

(i) For each j, one of the following conditions holds.

(i.1) $s_j'' = s_j$ and $s_j' = 0$,

(i.2) $s_j'' = s_j'$ and $s_j = 0$,

(i.3) $s_j'' = 2^{\ell-1}$ and $s_j' = 2^{\ell-1} + s_j \pmod{2^{\ell}}$.

(ii) (ii.1) $s_j' = 0$ or $s_j' = 2^{\ell-1}$ for $1 \le j \le n$,

(ii.2) if $s_j' = 0$, then $s_j'' = s_j$, and

(ii.3) there is an s such that $X(s) \ge 0$ and $Y(s) \ge 0$, and if $s_j' = 2^{\ell-1}$, then either $s_j = s$ and $s_j'' = 2^{\ell-1} - s$ or $s_j = 2^{\ell} - s$ and $s_j'' = 2^{\ell-1} + s$.

<u>Proof</u>: (i) Suppose that condition (i) holds. Then we have that for $1 \le j \le n$

$$X(s_j) - 1 + X(s_j') - 1 = X(s_j'') - 1,$$

$$Y(s_j) + Y(s_j') = Y(s_j''),$$

$$(X(s_j) - 1)^2 + Y(s_j)^2 + (X(s_j') - 1)^2 + Y(s_j')^2 = (X(s_j'') - 1)^2 + Y(s_j'')^2.$$

Hence, inequalities (6.2) for $\bar{v}$ and $\bar{v}'$ imply inequality (6.2) for $\bar{v}''$.

(ii) Suppose that condition (ii) holds. Then we have that for $1 \leq j \leq n$,

$$X(s_j) - 1 + X(s)(X(s_j') - 1) = X(s_j'') - 1,$$

$$Y(s_j) + X(s)\, Y(s_j') = Y(s_j''),$$

$$(X(s_j) - 1)^2 + Y(s_j)^2 + X(s)\{(X(s_j') - 1)^2 + Y(s_j')^2\}$$
$$= (X(s_j'') - 1)^2 + Y(s_j'')^2.$$

Hence, inequalities (6.2) for $\bar{v}$ and $\bar{v}'$ imply inequality (6.2) for $\bar{v}''$. ■■

For a set T of n-tuples over $\{ 0, 1, \cdots, 2^{\ell}-1 \}$, a subset S of T is said to be T-representative, if

$$\bigcap_{\bar{v}\in T} Q(\bar{v}) = \bigcap_{\bar{v}\in S} Q(\bar{v}). \tag{6.5}$$

In the examples below, a relatively small subset S of nonzero codewords of C can be chosen as a $\{ C - \{\bar{0}\} \}$-representative set.

For nonzero codeword $\bar{v}$ of C, let $P_e(\bar{v})$ denote the probability that a received vector $\bar{z}$ satisfies the following condition:

$$|\bar{z},\bar{v}|^2 < |\bar{z},\bar{0}|^2,$$

that is,

$$2\sum_{j=1}^{n} (X(s_j)-1)(x_j-1)+Y(s_j)y_j \geq |\bar{v}|^2, \tag{6.6}$$

where $|\bar{v}|$ denotes $\sqrt{d^{(n)}(\bar{v},\bar{0})}$. Since the random variable,

$$2\sum_{j=1}^{n} (X(s_j)-1)(x_j-1)+Y(s_j)y_j\,,$$

has a Gaussian distribution with zero mean and variance $4\sigma^2|\bar{v}|^2$, we have

$$P_e(\bar{v}) = \int_{|\bar{v}|^2}^{\infty} \frac{1}{2\sqrt{2\pi}\sigma|\bar{v}|} e^{-\frac{x^2}{8\sigma^2|\bar{v}|^2}} dx$$

$$= \frac{1}{2}\,\mathrm{erfc}\left(\frac{|\bar{v}|}{2\sqrt{2}\sigma}\right)$$

$$= \frac{1}{2}\,\mathrm{erfc}\left(\frac{\sqrt{\rho}\,|\bar{v}|}{2}\right) \tag{6.7}$$

where

$$\mathrm{erfc}(x) = \frac{2}{\sqrt{\pi}} \int_{x}^{\infty} e^{-t^2} dt$$

and ρ is the SNR per symbol [30].

For a set Q of n-tuples over $\{ 0, 1, \cdots, 2^{\ell}-1 \}$, let $\bar{Q}$ denote the complementary set of Q. Suppose that S is $\{C-\{\bar{0}\}\}$-representative. Then it follows from (6.3) and (6.5) that

$$\bar{Q}_c = \bigcup_{\bar{v}\in S} \bar{Q}(\bar{v}).$$

Hence we have the following upper bound on P_{ic}.

$$P_{ic} = 1 - P_c \leq \sum_{\bar{v}\in S} P_e(\bar{v}). \tag{6.8}$$

Let Δ be the set of real numbers d such that there is a nonzero codeword $\bar{v}$ in C with squared Euclidean distance d from the zero codeword $\bar{0}$. For $d\in\Delta$ and a subset S of C, let $A_d[S]$ be the number of codewords of C in S with squared Euclidean distance d from the zero codeword. Then, it follows from (6.7) and (6.8) that

$$P_{ic} \leq \frac{1}{2} \sum_{d\in\Delta} A_d[S] \operatorname{erfc}\left(\frac{\sqrt{d\rho}}{2}\right). \tag{6.9}$$

$A_d[C-\{\bar{0}\}]$ can be computed from the complete weight distribution of C. If we can choose a small $\{C-\{\bar{0}\}\}$-representative set S, $A_d[S]$ may be much smaller than $A_d[C-\{\bar{0}\}]$ except for "dominant" d's close to D[C].

In the following, we evaluate the error performance of the specific codes constructed in Section 4.

Example 1: Suppose C is the QPSK code $C^{(2)}_{Q,1}$. The following subset S of C can be easily shown to be $\{C-\{\bar{0}\}\}$-representative by using lemma 2.

$$S \triangleq \{ (s_1, s_2, \cdots, s_5) : \text{one component is 2 and the other components are zero.} \}$$

$$\cup \{ (s_1, s_2, 0, 0, 0) : s_1 \in \{1,3\}, s_2 \in \{1,3\} \}$$

$$\cup \{ (0, 0, s_3, s_4, s_5) : \text{two components of } \{ s_3, s_4, s_5 \} \text{ are in } \{1,3\} \text{ and the remaining one is zero.} \}.$$

It follows from (6.7) and (6.8) that

$$P_{ic} \leq \frac{21}{2} \operatorname{erfc}(\sqrt{\rho}). \tag{6.10}$$

__Example 2__: Let C be the QPSK code $C^{(4)}_{Q,3}$. Note that C_{b1} (= H_{15}) is a shortened code of the second-order (16,11) Reed-Muller code, denoted $RM_{4,2}$. A codeword $\bar{v}$ of a linear code is said to be decomposable if there are two nonzero codeword $\bar{v}_1$ and $\bar{v}_2$ in the code such that $\bar{v} = \bar{v}_1 + \bar{v}_2$ and the Hamming weight of $\bar{v}$ is the sum of those of $\bar{v}_1$ and $\bar{v}_2$. By using the canonical expressions of codewords of the second-order Reed-Muller code [28], it can be shown that any codeword of $RM_{4,2}$ with weight 8 or 12 is decomposable. It follows from this fact (Appendix B) and Lemma 2 that the following subset S of C is { C–{ $\bar{0}$ } }-representative. Let $|\bar{v}|_H$ denote the Hamming weight of $\bar{v}$.

$$S \triangleq \{ \bar{v}=(s_1, s_2, \cdots, s_{15}) : |\bar{v}|_H = 2 \text{ and } s_i \in \{0,2\} \text{ for } 1 \leq i \leq 15 \}$$

$$\cup \{ \bar{v}=(s_1, s_2, \cdots, s_{15}) : |\bar{v}|_H = 4, 6 \text{ or } 10, \text{ and } s_i \in \{0,1,3\} \text{ for } 1 \leq i \leq 15 \text{ and the number of occurrences of symbol 3 is even.} \}$$

$\cup \{ \bar{v}=(s_1, s_2, \cdots, s_{15}) : |\bar{v}|_H = 5, 7 \text{ or } 11$, and the number of occurrences of symbol 2 is one, and that of symbol 3 is odd. } .

It follows from (6.7) and (6.8) that

$$P_{ic}^{(1)} \le \frac{945}{2} \operatorname{erfc}(\sqrt{2\rho}) + 9100 \operatorname{erfc}(\sqrt{3\rho}) + 40320 \operatorname{erfc}(2\sqrt{\rho}) + 43008 \operatorname{erfc}(\sqrt{5\rho}) + 215040 \operatorname{erfc}(\sqrt{6\rho}) . \quad (6.11)$$

Example 3: Let C be the 8-PSK code $C_{8,2}^{(2)}$. Suppose that, for each message $(a_1, a_2, \cdots, a_{16})$, the bit a_1 is used as the input to the C_{b1} encoder, the bits $a_3, a_5, \cdots, a_{15}$ are used as the input to the C_{b2} encoder and the bits $a_2, a_4, \cdots, a_{16}$ are used as the input to the C_{b3} encoder. The following subset S is $\{C-\{\bar{0}\}\}$-representative,

$S \triangleq \{ (s_1, s_2, \cdots, s_8)$: one component is 4 and the others are zero. }

$\cup \{ (s_1, s_2, \cdots, s_8)$: the number of nonzero components is 2, and a nonzero component is 2 or 6. }

$\cup \{ (s_1, s_2, \cdots, s_8) : s_i$ is 1 or 7 for $1 \le i \le 8$ and the number of symbol 7 is even. }.

It follows from (6.7) and (6.8) that

$$P_{ic}^{(1)} \le 60 \operatorname{erfc}(\sqrt{\rho}) + 64 \operatorname{erfc}(\sqrt{2(2-\sqrt{2})\rho}) . \quad (6.12)$$

On the other hand, the probability $P_{Q,ic}$ that there occurs at least one bit error when 16 bits are transmitted by uncoded QPSK is given by [30],

$$P_{Q,ic} = 1 - [\, 1 - \tfrac{1}{2}\mathrm{erfc}(\sqrt{\tfrac{\rho}{2}}\,)\,]^{16}. \tag{6.13}$$

In Table 1 and Figure 6, we show the upper bounds on $P_{ic}^{(1)}$ given by (6.12) and $P_{Q,ic}$ given by (6.13) for various SNR per information bit, $\rho/2$. We see that the code $C_{8,2}^{(2)}$ achieves a 3dB real coding gain over the uncoded QPSK without bandwidth expansion at 10^{-6} block error rate. In Table 2 and Figure 7, we show the upper bounds on the decoded bit error probability for Example 3.

Let T be a subset of $\{\, 0, 1, \cdots, 2^{\ell}-1 \,\}$. For $\bar{v} \in C$, define

$$\mathrm{Occ}(\, T,\bar{v}\,) \triangleq \sum_{s \in T} (\text{the number of occurrences of symbol } s \text{ in } \bar{v}\,). \tag{6.14}$$

Example 4: Let C be the 8-PSK code $C_{8,7}^{(2)}$. Then the following subset S of $C-\{\bar{0}\}$ is easily shown to be $\{C-\{\bar{0}\}\}$-representative by using lemma 2.

$$S \triangleq \{\, \bar{v}=(\, s_1, s_2, \cdots, s_{23}\,) : |\bar{v}|_H = 2 \text{ and } s_i \in \{\, 0, 2, 6 \,\} \text{ for } 1 \le i \le 23 \,\}$$

$$\cup \{\, \bar{v}=(\, s_1, s_2, \cdots, s_{23}\,) : \mathrm{Occ}(\, \{\, j \,\},\bar{v}\,) \le 1 \text{ for each } j \in \{\, 2,3,4,5,6 \,\} \text{ and } \mathrm{Occ}(\{2,3,4,5,6\},\bar{v}) \le 2. \,\}.$$

Example 5: Let C be the 8-PSK code $C_{8,4}^{(2)}$. The following subset S of C can be easily shown to be $\{C-\{\bar{0}\}\}$-representative by using lemma 2.

$$S \triangleq \{\ \bar{v}=(s_1, s_2, \cdots, s_{15}) : |\bar{v}|_H = 1 \text{ and } s_i \in \{0, 4\} \text{ for } 1 \le i \le 15\ \}$$

$$\cup \{\ \bar{v}=(s_1, s_2, \cdots, s_{15}) : |\bar{v}|_H = 2 \text{ and } s_i \in \{0, 2, 6\} \text{ for } 1 \le i \le 15\ \}$$

$$\cup \{\ \bar{v}=(s_1, s_2, \cdots, s_{15}) : \mathrm{Occ}(\{j\},\bar{v}) \le 1 \text{ for each } j\in \{2,3,4,5,6\} \text{ and } \mathrm{Occ}(\{2,3,4,5,6\},\bar{v}) \le 2.\ \}.$$

Example 6: Let C be the 8-PSK code $C_{8,m}^{(2)}$. The following subset S of C can be easily shown to be $\{C-\{\bar{0}\}\}$-representative by using lemma 2.

$$S \triangleq \{\ \bar{v}=(s_1, s_2, \cdots, s_n) : |\bar{v}|_H = 2 \text{ and } s_i \in \{0, 4\} \text{ for } 1 \le i \le n\ \}$$

$$\cup \{\ \bar{v}=(s_1, s_2, \cdots, s_n) : s_i \in \{1, 3, 5, 7\} \text{ for } 1 \le i \le n \text{ and } \mathrm{Occ}(\{5,7\}, \bar{v}) \text{ is even.}\ \}$$

$$\cup \{\ \bar{v}=(s_1, s_2, \cdots, s_n) : |\bar{v}|_H = 4, 6 \text{ or } 10 \le |\bar{v}|_H \le n,\ s_i \in \{0, 2, 6\} \text{ for } 1 \le i \le n \text{ and } \mathrm{Occ}(\{6\}, \bar{v}) \text{ is even.}\ \}$$

$$\cup \{\ \bar{v}=(s_1, s_2, \cdots, s_n) : |\bar{v}|_H = 5, 7 \text{ or } 11 \le |\bar{v}|_H \le n,\ s_i \in \{0, 2, 4, 6\} \text{ for } 1 \le i \le n,\ \mathrm{Occ}(\{4\}, \bar{v}) = 1 \text{ and } \mathrm{Occ}(\{6\}, \bar{v}) \text{ is odd.}\ \}.$$

The error performance and coding gains of the codes given in the above examples are now being computed and will be included in our next report.

7. Conclusion

In this report, we have presented a class of bandwidth efficient block codes for M-ary PSK modulation. A soft-decision decoding for this class of codes is devised. Some specific codes with good squared minimum Euclidean distance are constructed. The complete weight distributions of these codes are determined. Their error probabilities are evaluated. Some specific codes have simple trellis structures and hence can be decoded by Viterbi algorithm. Some of these codes are suitable for use as the inner codes of cascaded coding scheme with Reed-Solomon codes over $GF(2^8)$ as outer codes. Our preliminary results show that such cascaded coding schemes provide extremely high reliability and large coding gains.

In our next report, we will present the coding gains of the codes presented in this report over the uncoded QPSK modulation.

Appendix A

Trellis Diagram for the 8-PSK Code $C_{8,2}^{(2)}$

The 8-PSK code $C_{8,2}^{(2)}$ consists of three binary component codes C_{b1}, C_{b2} and C_{b3} which are $P_8^{\perp}$, P_8 and $\{0,1\}^8$ respectively. Let $\bar{u}$ be a 16-bit message to be encoded. Divide $\bar{u}$ into three submessages $\bar{u}_1$, $\bar{u}_2$ and $\bar{u}_3$ where $\bar{u}_1$ consists of only one bit, $\bar{u}_2$ consists of seven bits and $\bar{u}_3$ consists of eight bits. Then $\bar{u}_1$, $\bar{u}_2$ and $\bar{u}_3$ are encoded based on C_{b1}, C_{b2} and C_{b3} respectively. Let

$$\bar{a} = (a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$$

$$\bar{b} = (b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8)$$

$$\bar{c} = (c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8)$$

be their corresponding binary codewords. Note that $\bar{a}$ is either the all-zero vector or the all-one vector. The codeword $\bar{b}$ has even weight.

For $1 \le \ell \le 8$, the input to the signal selector of the overall encoder-modulator at the ℓ-th time unit is the triplet (a_ℓ, b_ℓ, c_ℓ). If $a_\ell = 0$, then (b_ℓ, c_ℓ) selects a signal point from the QPSK signal set shown in Figure 2b. If $a_\ell = 1$, then (b_ℓ, c_ℓ) selects a point from the QPSK signal set shown in Figure 2c. Hence the system switches between two QPSK signal sets. To construct the trellis diagram for $C_{8,2}^{(2)}$, we need to define the states of the overall encoder-modulator. Let $(b_1, b_2, \cdots, b_\ell)$ denote the ℓ-bit prefix of codeword $\bar{b}$. Let $W(b_1, b_2, \cdots, b_\ell)$ denote the Hamming weight of $(b_1, b_2, \cdots, b_\ell)$. At the ℓ-th time unit, the state of the encoder-modulator depends on the bit a_ℓ and the number $W(b_1, b_2, \cdots, b_\ell)$. Define the following states:

(1) A_e represents the states that $a_\ell = 0$ and $W(b_1, b_2, \cdots, b_\ell)$ is even;

(2) A_0 represents the states that $a_\ell = 0$ and $W(b_1, b_2, \cdots, b_\ell)$ is odd;

(3) B_e represents the states that $a_\ell = 1$ and $W(b_1, b_2, \cdots, b_\ell)$ is even; and

(4) B_0 represents the states that $a_\ell = 1$ and $W(b_1, b_2, \cdots, b_\ell)$ is odd.

Assume that the encoder-modulator starts from the state A_0 at the time $\ell = 0$. Then the trellis diagram for $C_{8,2}^{(2)}$ can be constructed easily as shown in Figure 4. There are two parallel branches (or transitions) between the transition of two states; they correspond to $c_\ell = 0$ and $c_\ell = 1$ respectively.

The encoding of message $\bar{u}$ is equivalent to tracing a path in the trellis diagram. The codeword corresponding to $\bar{u}$ is a sequence of QPSK signal points either from the set shown in Figure 2b or from the set shown in Figure 2c.

■■

Appendix B

Consider the second-order (16,11) Reed-Muller code $RM_{4,2}$. We use a boolean function $b(\bar{v})$ for expressing a codeword $\bar{v}$ in $RM_{4,2}$.

By using an affine transformation, a codeword $\bar{v}$ in $RM_{4,2}$ with weight 8 or 12 can be represented as one of the following forms [28,p.438]:

1) If $|\bar{v}|_H = 8$, then $b(\bar{v}) = x_1x_2+x_3$ or $b(\bar{v}) = x_3$.

2) If $|\bar{v}|_H = 12$, then $b(\bar{v}) = x_1x_2+1$.

Let y be x_1, x_2 or $x_1 + x_2$. Then the degree of $yb(\bar{v})$ is at most 2. Let $\bar{v}_1$ and $\bar{v}_2$ denote the codewords represented by $yb(\bar{v})$ and $(y+1)b(\bar{v})$, respectively. Then, $\bar{v} = \bar{v}_1 + \bar{v}_2$, $\bar{v}_1 \neq \bar{0}$, $\bar{v}_2 \neq \bar{0}$, and $|\bar{v}|_H = |\bar{v}_1|_H + |\bar{v}_2|_H$. That is, $\bar{v}$ is decomposable.

Let $\bar{u}$ be a codeword of C_{b2} ($= P_{15}$) such that

$$|\bar{v}+2\bar{u}|_H = |\bar{v}|_H .$$

Let $|\bar{u}|_{H,y=a}$ denote the number of nonzero components of $\bar{u}$ in the bit-positions for which y=a. If $|\bar{u}|_{H,x_1=0}$ and $|\bar{u}|_{H,x_2=0}$ are odd, then $|\bar{u}|_{H,x_1=1}$ and $|\bar{u}|_{H,x_2=1}$ are odd. Then $|\bar{u}|_{H,x_1+x_2=0}$ and $|\bar{u}|_{H,x_1+x_2=1}$ are even. Therefore we can choose one of x_1, x_2 and $x_1 + x_2$ as y in such a way that $|\bar{u}|_{H,y=0}$ and $|\bar{u}|_{H,y=1}$ are even.

■■

REFERENCES

1. J.B. Anderson and R. de Buda, "Better Phase-Modulation Error Performance Using Trellis Phase Codes", Electron. Letters, Vol. 12, pp. 587-588, October 28, 1976.

2. A. Digeon, "On improving Bit Error Probability of QPSK and 4-Level Amplitude Modulation Systems by Convolutional Coding", IEEE Transactions on Communications, Vol. COM-25, pp. 1238-1239, October, 1977.

3. J.B. Anderson and D.P. Taylor, " A Bandwidth-Efficient Class of Signal Space codes", IEEE Transactions on Information Theory, Vol. IT-24, pp. 703-712, November, 1978.

4. J.B. Anderson, C.E. Sundberg, T. Aulin, and N. Rydbeck, " Power-Bandwidth Performance of Smoothed Phase Modulation Codes", IEEE Transactions on Communications, Vol. COM-29, pp. 187-195, March, 1981.

5. T. Aulin and C.E. Sundberg, "Continuous Phase Modulation (CPM) — Part—I: Full Response Signalling" , IEEE Transactions on Communications, Vol. COM-29, pp. 196-209, March, 1981.

6. T. Aulin, N. Rydbeck, and C.E. Sundberg, "Continuous Phase Modulation (CPM) — Part—II: Partial Response Signalling" , IEEE Transactions on Communications, Vol. COM-29, pp. 210-225, March, 1981.

7. T. Aulin and C.E. Sundberg, "On the Minimum Euclidean Distance for a Class of Signal Space Codes", IEEE Transactions on Information Theory, Vol. IT-28, pp. 43-55, January, 1982.

8. G. Ungerboeck, "Channel Coding with Multilevel / Phase Signals", IEEE Transactions on Information Theory, Vol. IT-28, pp. 55-67, January, 1982.

9. G.D. Forney, Jr., R.G. Gallager, G.R. Lang, F.M. Longstaff, and S.U. Qureshi, "Efficient Modulation for Band-Limited Channels", IEEE J. Select. Areas Communications, Vol. SAC-2, pp. 632-647, September, 1984.

10. L.F. Wei, "Trellis-Coded Modulation with Multidimensional Constellations", submitted to IEEE Transactions on Information Theory, 1986.

11. R. Fang, P. Chang, and F. Hemmati, "Coded 8-PSK Transmission over 72-MHz Nonlinear Transponders at 140-Mbit/s Information Rate for Trunking Applications", IEEE Globecom Conference Record, pp. 1013-1020, November 28-December 1, 1983, San Diego, CA.

12. T. Fujino et. al., "A 120 Mbit/s Coded 8-PSK Modem with Soft Decision Viterbi Decoder", IEEE International Conference on Communications Conference Record, June 22-25, 1986, Toronto, Canada.

13. E.Biglieri, "High-Level Modulation and Coding for Nonlinear Satellite Channels", IEEE Transactions on Communications, Vol. COM-32, pp. 616-626, May, 1984.

14. R. Padovani and J.K. Wolf, "Coded Phase / Frequency Modulation", IEEE Transactions on Communications, Vol. COM-34, pp. 446-453, May, 1986.

15. S.G. Wilson et. al., "Rate 3/4 Convolutional Coding of 16-PSK: Code Design and Performance Study", IEEE Transactions on Communications, Vol. COM-32, pp. 1308-1315, December, 1984.

16. S.G. Wilson, "Rate 5/6 Trellis-Coded 8-PSK", IEEE Transactions on Communications, Vol. COM-34, pp. 1045-1049, October, 1986.

17. G.D. Forney, Jr., "Coset Codes I : Geometry and Classification", submitted to IEEE Transactions on Information Theory, 1986.

18. R.H. Deng and D.J. Costello, Jr., "High Rate Concatenated Coding Systems with Bandwidth Efficient Inner Codes", submitted to IEEE Transactions on Communications, 1987.

19. A.R. Calderbank and N.J.A. Sloane, "New Trellis Codes", submitted to IEEE Transactions on Information Theory, 1986.

20. G.D. Forney, Jr., "Coset Codes II : Binary Lattices and Related Codes", submitted to IEEE Transactions on Information Theory, 1986.

21. A. LaFanechere, R.H. Deng, and D.J. Costello, Jr., "Multidimensional Trellis Coded Phase Modulation Using Unit-Memory and Partial Unit-Memory Convolutional Codes", submitted to IEEE Transactions on Information Theory, 1987.

22. A.R. Calderbank, J.E. Mazo, and V.K. Wei, "Asymptotic Upper Bounds on the Minimum Distance of Trellis Codes", IEEE Transactions on Communications, Vol. COM-33, pp. 305-309, April, 1985.

23. M. Rouanne and D.J. Costello, Jr., "A Gilbert Lower Bound on the Minimum Free Euclidean Distance of Trellis Coded Modulation", submitted to IEEE Transactions on Information Theory, 1987.

24. A.R. Calderbank and N.J.A. Sloane, "Four-Dimensional Modulation with an Eight-State Trellis Code", AT&T Tech. J., Vol. 64, pp. 1005-1018, 1985.

25. A.R. Calderbank and N.J.A. Sloane, "An Eight-Dimensional Trellis Code", Proc. IEEE, Vol. 74, pp. 757-759, 1986.

26. S.I. Sayegh, "A Class of Optimum Block Codes in Signal Space", IEEE Transactions on Communications, Vol. COM-34, pp. 1043-1045, October 1986.

27. H. Imai and S. Hirakawa, "A New Multilevel Coding Method Using Error-Correcting Codes", , IEEE Transactions on Information Theory, Vol. IT-23, pp. 371-377, March, 1977.

28. F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, 1977.

29. J.K. Wolf , "Efficient Maximum Likelihood Decoding of Linear Block Codes Using a Trellis", IEEE Transactions on Information Theory, Vol. IT-24, pp. 76-80, January, 1978.

30. J.C. Proakis, Digital Communications, McGraw-Hill, 1983.

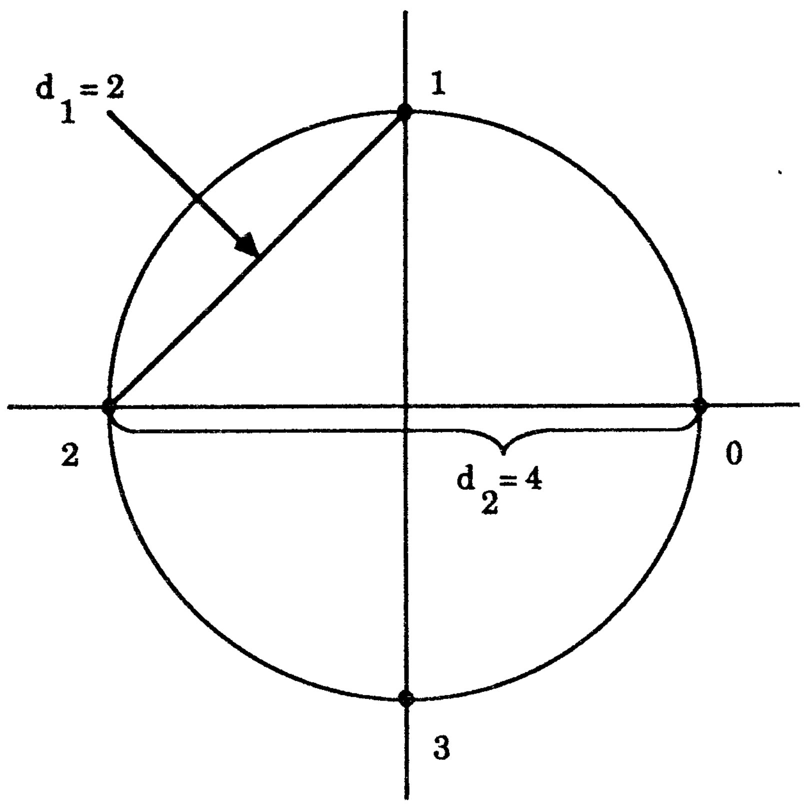
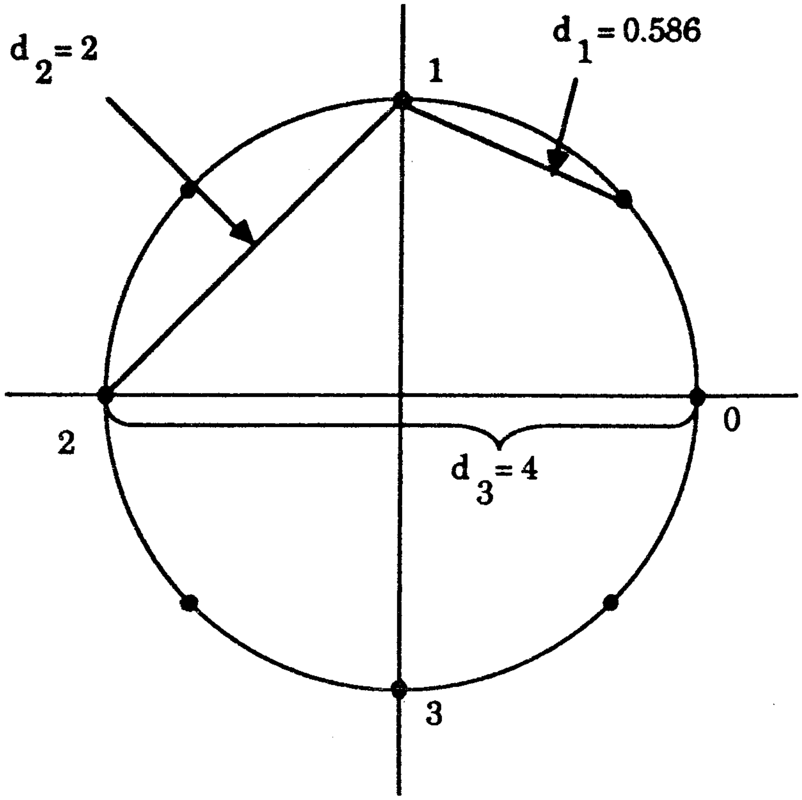
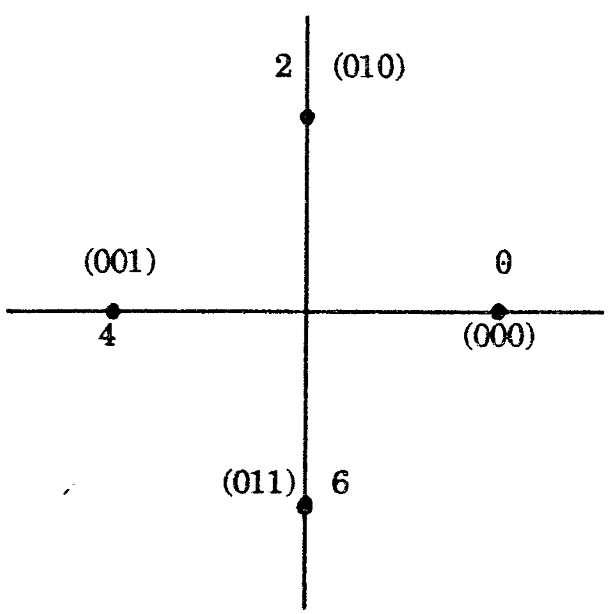


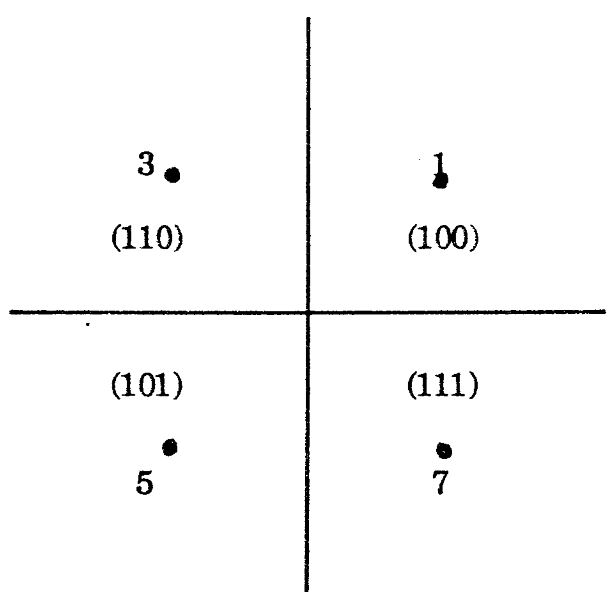
Figure 1 QPSK signal set and squared Euclidean distances between signal points.



(a) 8-PSK signal set and squared Euclidean distances between signal points



(b) QPSK signal set for a_ℓ=0 and signal mapping



(c) QPSK signal set for a_ℓ=1 and signal mapping

Figure 2

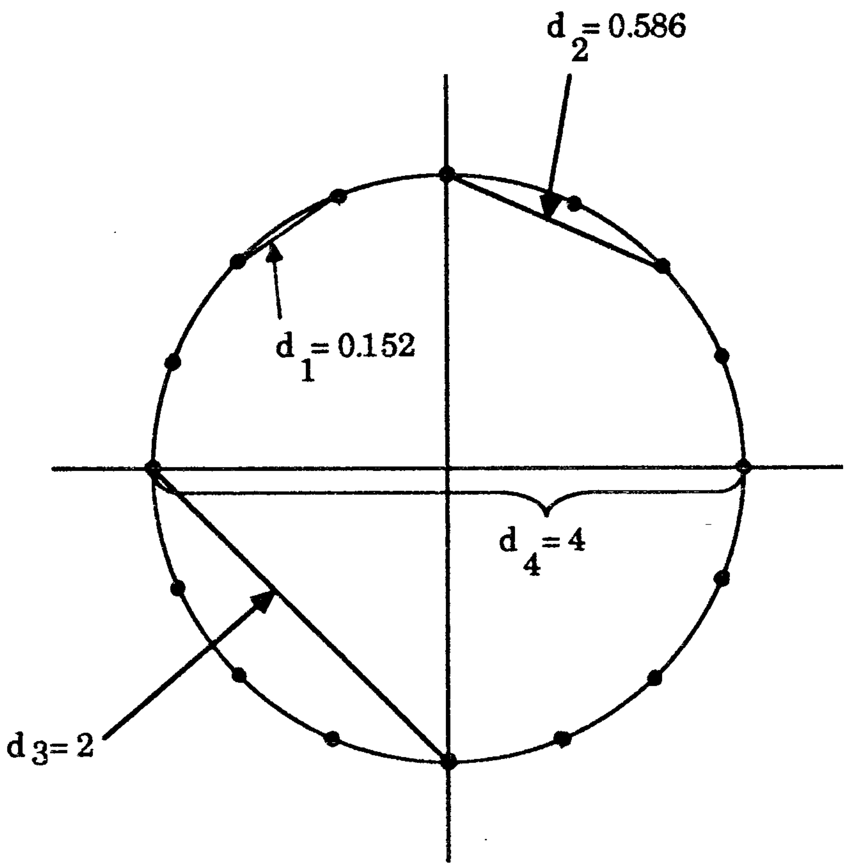


Figure 3 16-PSK signal set and squared Euclidean distances between signal points.

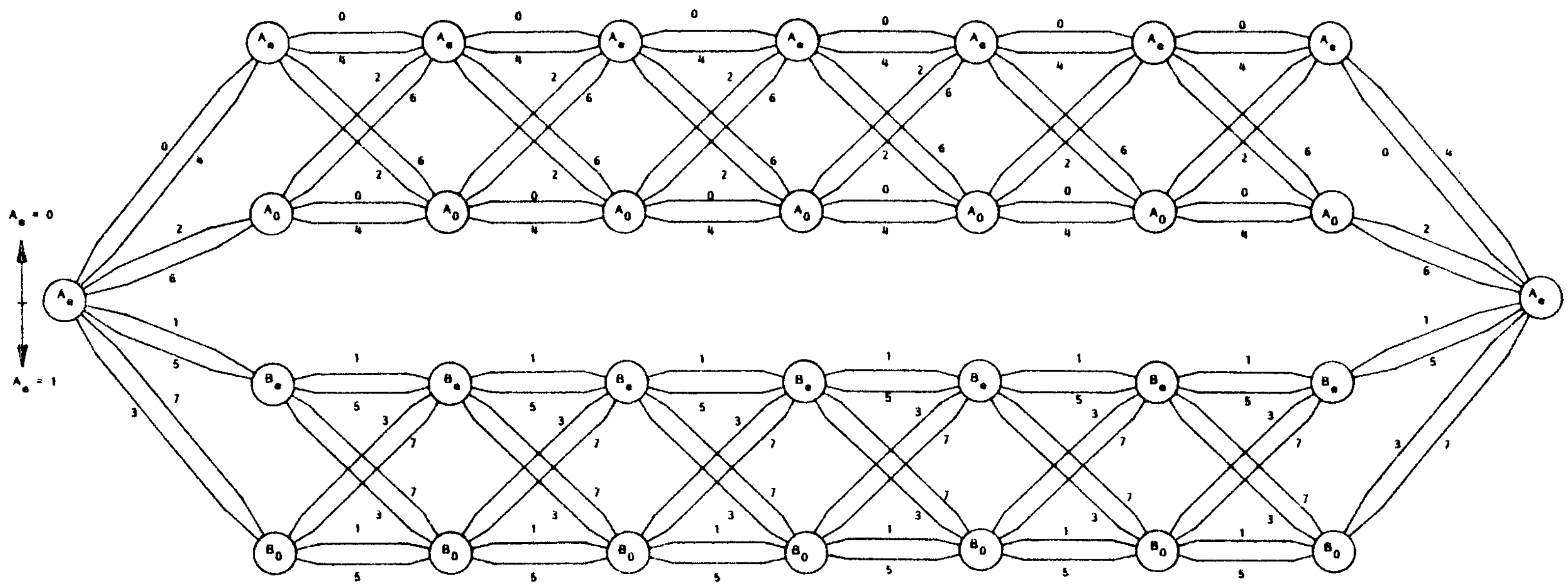


Figure 4   4-state trellis diagram for the 8-PSK code $C_{8,2}^{(2)}$

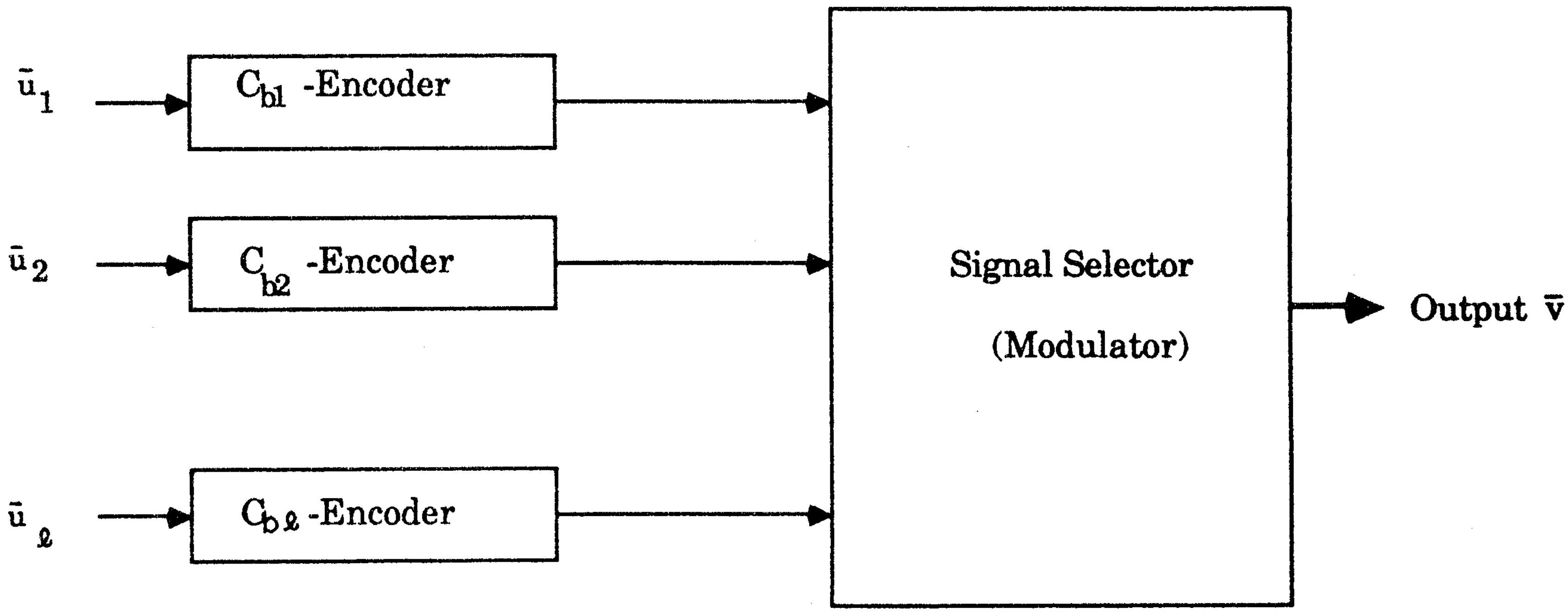


Figure 5 M-ary PSK code encoder

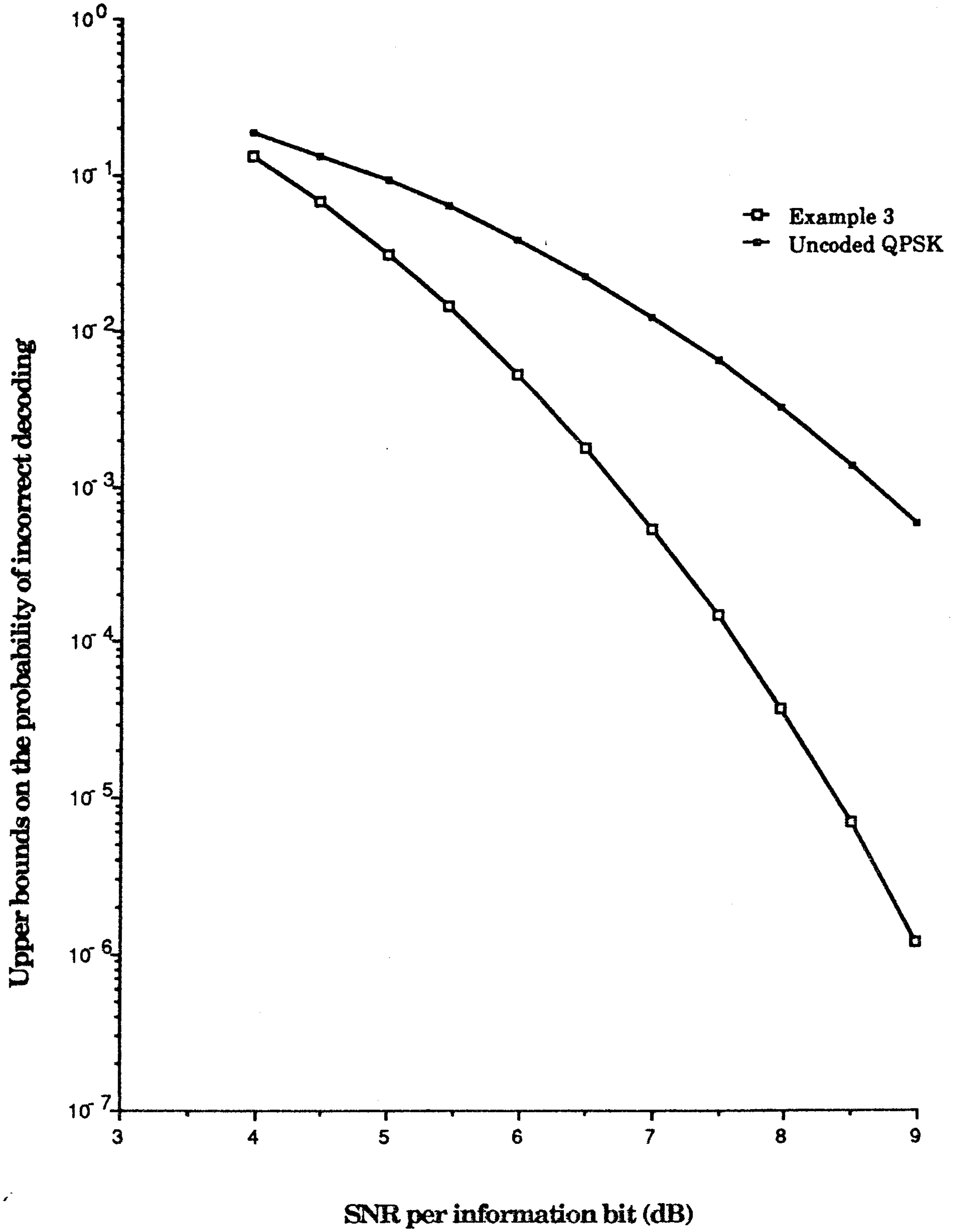


Figure 6 Upper bounds on the probability of incorrect decoding for a block with 16 information bits for Example 3 and uncoded QPSK

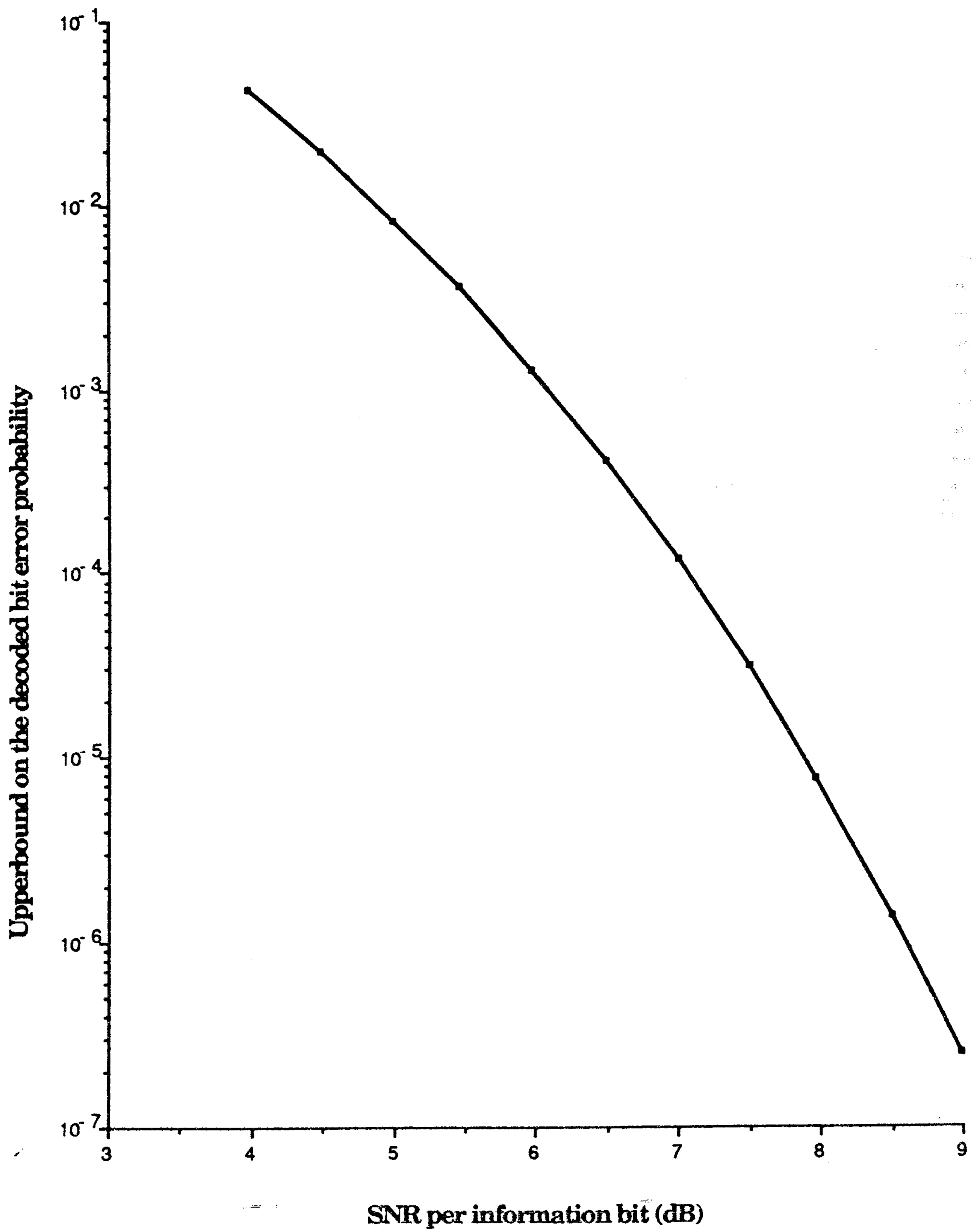


Figure 7 Upper bounds on the decoded bit error probability for Example 3

Table 1. Upper bounds on the probability of incorrect decoding for a block with 16 information bits for Example 3 and uncoded QPSK

SNR per symbol (dB)	SNR per information bit (dB)	Upper bounds on Pic for Example 3	$P_{Q,ic}$
7.0	3.98	1.34E-01	1.85E-01
7.5	4.48	6.78E-02	1.34E-01
8.0	4.99	3.10E-02	9.23E-02
8.5	5.45	1.43E-02	6.33E-02
9.0	5.97	5.31E-03	3.88E-02
9.5	6.49	1.79E-03	2.26E-02
10.0	6.99	5.48E-04	1.24E-02
10.5	7.49	1.53E-04	6.52E-03
11.0	7.96	3.84E-05	3.24E-03
11.5	8.49	7.15E-06	1.39E-03
12.0	8.98	1.22E-06	5.93E-04

Table 2 Upper bounds on the decoded bit error probability for Example 3

SNR per symbol (dB)	SNR per information bit (dB)	Upper bounds on the decoded bit error probability
7.0	3.98	4.31E-02
7.5	4.48	1.99E-02
8.0	4.99	8.42E-03
8.5	5.45	3.66E-03
9.0	5.97	1.29E-03
9.5	6.49	4.14E-04
10.0	6.99	1.21E-04
10.5	7.49	3.21E-05
11.0	7.96	7.78E-06
11.5	8.49	1.39E-06
12.0	8.98	2.52E-07