1995

QPSK Block-Modulation Codes for Unequal Error Protection

Robert H. Morelos-Zaragoza
Osaka University, robert.morelos-zaragoza@sjsu.edu

Shu Lin
University of Hawaii at Manoa

Recommended Citation

Robert H. Morelos-Zaragoza and Shu Lin. "QPSK Block-Modulation Codes for Unequal Error Protection" *Faculty Publications* (1995): 576-581. doi:10.1109/18.370154

2) in the case where $i \neq j$

$$C_{i,j}(\tau) = \begin{cases} -1, & \text{when } \tau = (p^m + 1)l, \\ & \quad \text{for } 0 \leq l \leq p^m - 2 \\ p^m - 1, & \text{occurs } (p^{n-1} + p^m - 2p^{m-1}) \text{ times} \\ p^m \omega^k - 1, & \text{occurs } (p^{n-1} - 2p^{m-1}) \text{ times,} \\ & \quad \text{for } 1 \leq k \leq p - 1. \end{cases}$$

V. Conclusion

It was shown that the new family consisting of $p^{n/2}$ (where n is even) balanced nonbinary sequences with period $p^n - 1$ can be obtained from the modified Kumar–Moreno sequences of the same period, and the distribution of correlation values for the family was shown to have $p+2$ distinct correlation values and the same maximum nontrivial correlation value of $p^{n/2} + 1$ as that of Kumar–Moreno sequences. On the other hand, it was shown that the cost of making sequences balanced is a decrease of family size in addition to the condition that n is an even number. The family size of the new sequences is $p^{n/2}$ which is much smaller than p^n, that of Kumar–Moreno sequences.

VI. Acknowledgment

The authors wish to thank Prof. P. V. Kumar for sending the draft of their paper [3] to one of the authors (K.I.), and would like to thank the anonymous referees for helpful comments useful for improving the readability of the paper.

References

[1] D. V. Sarwate and M. B. Pursley, "Cross-correlation properties of pseudorandom and related sequences," *Proc. IEEE*, vol. 68, pp. 593–618, May 1980.
[2] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread-Spectrum Communications*, vol. 1. Computer Science Press, 1985, ch. 5.
[3] P. V. Kumar and O. Moreno, "Prime-phase sequences with periodic correlation properties better than binary sequences," *IEEE Trans. Inform. Theory*, vol. 37, no. 3, pp. 603–616, May 1991.
[4] L. R. Welch, "Lower bounds on the maximum correlation of signals," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 397–399, May 1974.
[5] R. Lidl and H. Niederreiter, "Finite fields," in Vol. 20 of *Encyclopedia of Mathematics and Its Applications*. Amsterdam, The Netherlands: Addison-Wesley, 1983.
[6] S. Matsufuji, K. Imamura, and S. Soejima, "Balanced binary pseudorandom sequences with low periodic correlation," presented at the 1990 IEEE Int. Symp. on Information Theory, Jan. 1990.

QPSK Block-Modulation Codes for Unequal Error Protection

Robert H. Morelos-Zaragoza, *Member, IEEE*, and Shu Lin, *Fellow, IEEE*

***Abstract*—Unequal error protection (UEP) codes find applications in broadcast channels, as well as in other digital communication systems, where messages have different degrees of importance. In this correspondence, binary linear UEP (LUEP) codes combined with a Gray mapped QPSK signal set are used to obtain new efficient QPSK block-modulation codes for unequal error protection. Several examples of QPSK modulation codes that have the same minimum squared Euclidean distance as the best QPSK modulation codes, of the same rate and length, are given. In the new constructions of QPSK block-modulation codes, even-length binary LUEP codes are used. Good even-length binary LUEP codes are obtained when shorter binary linear codes are combined using either the well-known $|\bar{u}|\bar{u}+\bar{v}|$-construction or the so-called construction X. Both constructions have the advantage of resulting in optimal or near-optimal binary LUEP codes of short to moderate lengths, using very simple linear codes, and may be used as constituent codes in the new constructions. LUEP codes lend themselves quite naturally to multistage decodings up to their minimum distance, using the decodings of component subcodes. A new suboptimal two-stage soft-decision decoding of LUEP codes is presented and its application to QPSK block-modulation codes for UEP illustrated.**

***Index Terms*—Unequal error protection, coded modulation, multistage decoding.**

I. Introduction

There are many practical applications in which it is required to design a code that protects messages against different levels of noise, or messages with different levels of importance over a noisy channel of the same noise power level. Examples of such situations are: broadcast channels, multiuser channels, computer networks, pulse-coded modulation (PCM) systems and source-coding systems, among others. Such a code is usually said to be an *unequal error protection* (UEP) code. In this correspondence, we propose to use binary linear UEP (LUEP) codes [1], combined with Gray mapped QPSK signal constellations, to obtain new efficient QPSK block-modulation codes with *unequal squared Euclidean distances*. That is, code sequences associated with the most important message bits are separated by a squared Euclidean distance (SED) larger than the SED between code sequences associated with less important message bits. Several examples of LUEP QPSK block-modulation codes, having the same minimum squared Euclidean distance (MSED) as that of optimal QPSK modulation codes of the same rate and length [2], [3], are given. The correspondence is organized as follows. In Section II, basic concepts and two constructions of LUEP codes based on specifying the generator matrix are presented. Section III deals with new constructions of QPSK block-modulation codes and introduces a new suboptimal *two-stage soft-decision* (TSD) decoding of LUEP

Manuscript received February 18, 1993. This research was supported by the NSF under Grants NCR-8813480, NCR-9115400, by NASA under Grant NAG 5-931, and by the Japanese Society for the Promotion of Science, ID no. 93157. Part of this work was presented at the 1993 IEEE International Symposium on Information Theory, San Antonio, TX, January 19, 1993.

R. M. Morelos-Zaragoza is with the Department of Information and Computer Sciences, Faculty of Engineering Science, Osaka University, Toyonaka, Osaka 500, Japan.

S. Lin is with the Department of Electrical Engineering, University of Hawaii, Holmes 483 Honolulu, HI 96822 USA.

IEEE Log Number 9408068.

codes. An example is given which illustrates TSD decoding of QPSK block-modulation codes for UEP. Finally, in Section IV, conclusions on the results are presented.

II. Basic Concepts of LUEP Codes

When a code is used to provide multiple levels of error protection, the conventional definition of minimum distance must be generalized. Since different levels of error protection are possible with a UEP code, a vector of minimum distances, one for each level of error protection, needs to be defined. Let C be an (n,k) block code (not necessarily linear) over a finite alphabet A, $n \geq k$. That is, C is a one-to-one mapping from A^k to A^n, i.e.

$$\bar{m} \in A^k \quad \overset{C}{\mapsto} \quad \bar{c}(\bar{m}) \in A^n$$

where

$$A^k = \underbrace{A \times A \times \cdots \times A}_{k \text{ times}}.$$

As usual, an element $\bar{m}$ from A^k is called a *message*, and an element $\bar{c}(\bar{m})$ from C is called a *codeword*. A^k is known as the *message set*. Let A^k be decomposed into the direct product of two disjoint *message subsets*, A^{k_i}, $i = 1, 2$, such that

$$A^k = A^{k_1} \times A^{k_2}.$$

A message $\bar{m} \in A^k$ can then be expressed as

$$\bar{m} = (\bar{m}_1, \bar{m}_2), \quad \bar{m}_i \in A^{k_i}, \quad i = 1, 2$$

where each $\bar{m}_i$ is called the *ith message part*, $i = 1, 2$. The *separation vector* of C is defined as the two-tuple $\bar{s} = (s_1, s_2)$, where

$$s_i \overset{\triangle}{=} \min\{d(\bar{c}(\bar{m}), \bar{c}'(\bar{m}')) : \bar{m}_i \neq \bar{m}_i', \quad \bar{m}_i, \bar{m}_i' \in A^{k_i}\}, \quad i = 1, 2$$

and $d(\bar{x}, \bar{x}')$ denotes the Hamming distance between $\bar{x}$ and $\bar{x}'$ in A^n. Note that in the definition of s_i above, there is no restriction on $\bar{m}_j$, $\bar{m}_j'$, for $j \neq i$. Assume that C has both components of its separation vector distinct and arranged in decreasing order, i.e., $s_1 > s_2$, such that C is an (n,k) block code of minimum distance s_2. We call $\bar{m}_1$ the *most important* message part and $\bar{m}_2$ the *least important* message part.

Code C is said to be an (n,k) *two-level UEP code* of separation vector $\bar{s} = (s_1, s_2)$, for the message set $A^{k_1} \times A^{k_2}$. This correspondence concentrates on *binary linear* two-level error correcting codes. That is, $A = \{0, 1\}$. For a binary *linear* two-level error correcting code, or binary LUEP code C, each element of the separation vector is given by

$$s_i \overset{\triangle}{=} \min\{\text{wt}(\bar{c}(\bar{m})) : \bar{m}_i \neq \bar{0}, \quad \bar{m}_i \in \{0, 1\}^{k_i}\}, \quad i = 1, 2 \quad (1)$$

where $\text{wt}(\bar{x})$ denotes the Hamming weight of vector $\bar{x}$. C is called an (n,k) two-level LUEP code, of separation vector $\bar{s} = (s_1, s_2)$, for the *message space* $\{0, 1\}^{k_1} \times \{0, 1\}^{k_2}$.

A. LUEP Codes Specified by their Generator Matrix

In this subsection, constructions of LUEP codes by appending cosets of subcodes in binary linear codes are presented. These constructions may be used to obtain constituent binary LUEP codes which, in conjunction with Gray mapped QPSK signals, yield efficient QPSK block-modulation codes for unequal error protection (see Section III).

1) The $|\bar{u}|\bar{u} + \bar{v}|$ Construction: For $i = 1, 2$, let C_i be an (n, k_i, d_i) binary linear code with generator matrix G_i. Define the *append* operation between two vectors,

$$\bar{u} = (u_0, u_1, \cdots, u_{n-1}) \text{ and } \bar{v} = (v_0, v_1, \cdots, v_{n-1})$$

as

$$\bar{u} \circ \bar{v} \overset{\triangle}{=} (u_0, u_1, \cdots, u_{n-1}, v_0, v_1, \cdots, v_{n-1}).$$

Based on C_1 and C_2, the following code:

$$\mu(C_1, C_2) = \{\bar{w} | \bar{w} = \bar{u} \circ (\bar{u} + \bar{v}), \bar{u} \in C_1, \bar{v} \in C_2\}$$

is a $(2n, k_1 + k_2)$ binary linear code with generator matrix

$$G = \begin{pmatrix} G_1 & G_1 \\ 0 & G_2 \end{pmatrix}$$

and minimum distance $d = \min\{2d_1, \max\{d_1, d_2\}\}$ [9].

Theorem 1: $\mu(C_1, C_2)$ is a two-level binary LUEP code of separation vector $\bar{s} = (s_1, s_2)$, for the message space $\{0, 1\}^{k_1} \times \{0, 1\}^{k_2}$, where

$$s_1 = \min\{2d_1, \max\{d_1, d_2\}\}$$

and

$$s_2 = \min\{\max\{d_1, d_2\}, d_2\} = d_2.$$

Proof: See [8]. ∎

2) Construction X: For $i = 1, 2, 3$, let C_i denote a linear (n_i, k_i, d_i) binary code. Assume $C_3 \subseteq C_2$, so that $k_3 \leq k_2$ and $d_3 \geq d_2$. Let C_X be the linear code whose generator matrix is

$$G_X = \begin{pmatrix} G_1 & G_2 \\ 0 & G_3 \end{pmatrix}$$

where G_1, $[G_2^\top G_3^\top]^\top$ and G_3 are the generator matrices of C_1, C_2, and C_3, respectively. (Note that it is required that $k_1 = k_2 - k_3$.) Then C_X is an $(n_1 + n_3, k_1 + k_3)$ linear code of minimum distance $d_X = \min\{d_3, d_1 + d_2\}$ [9]. This method of combining shorter linear codes to obtain a linear code of increased length and minimum distance is known as *Construction X* [4], and can be viewed as a generalization of the $|\bar{u}|\bar{u} + \bar{v}|$ construction. By an argument similar to that used to prove Theorem 1, we can prove the following Theorem 2.

Theorem 2: C_X is a two-level binary LUEP code of separation vector $\bar{s} = (s_1, s_2)$, for the message space $M = \{0, 1\}^{k_1} \times \{0, 1\}^{k_3}$, where

$$s_1 = d_1 + d_2$$

and

$$s_2 = \min\{d_3, d_1 + d_2\}.$$ ∎

III. LUEP QPSK Modulation Codes

In this section, a method is presented for combining binary two-level LUEP codes with a QPSK signal set to achieve coded modulation schemes that offer *two values of minimum squared Euclidean distance*, one for each message part to be protected. In other words, symbols of the most important message part are mapped onto code sequences with a larger squared Euclidean distance (SED) between them than the SED between code sequences corresponding to the less important message part. With data transmission over an additive white Gaussian noise (AWGN) channel, and a good modulation code (i.e., efficient soft-decision decoding and small number of nearest neighbors), a *smaller* probability of bit error is achieved for the most important message part than for the rest of the message. To approach the error performance given by a minimum

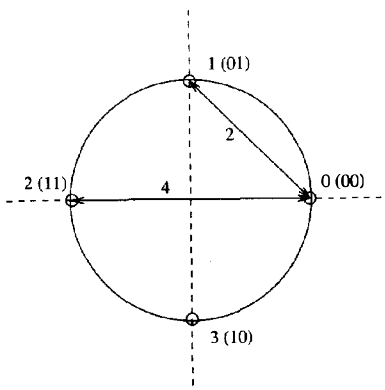

Fig. 1. A QPSK signal constellation with Gray mapping.

squared Euclidean distance (MSED), a new suboptimal *two-stage soft-decision decoding* of two-level LUEP codes, that employs their trellis structure, is introduced.

A. Constructions via Gray Mapping

In a QPSK signal constellation with *Gray mapping* between labels and signal points, the squared Euclidean distance between signal points is *proportional to* the Hamming distance between their labels. This QPSK signal constellation is said to form a *second-order Hamming space* [7]. By mapping 2-bit symbols onto signal points in a QPSK signal set, via Gray mapping, $(2n, k_1 + k_2)$ two-level LUEP codes and QPSK signal sets are combined to achieve a block-coded modulation system that offers two values of minimum squared Euclidean distances, one for each message part. Some of the resulting QPSK block-modulation codes will be shown to have the same minimum squared Euclidean distance as that of *optimal* QPSK block-modulation codes of the same rate and length [2], [3], while offering in addition a larger minimum squared Euclidean distance between code sequences associated with the most important message symbols. The proposed construction is as follows:

Let C_b be a $(2n, k_1 + k_2)$ binary LUEP code of separation vector $\bar{s} = (s_1, s_2)$ for the message space $\{0,1\}^{k_1} \times \{0,1\}^{k_2}$. Let S denote the label set of the unit-energy QPSK signal constellation depicted in Fig. 1 and define the following Gray mapping $\boldsymbol{M}$ between two-bit symbols and $S = \{0, 1, 2, 3\}$:

$$\begin{aligned} 00, &\mapsto 0\\ 01 &\mapsto 1\\ 11 &\mapsto 2\\ 10 &\mapsto 3. \end{aligned}$$

The set

$$C = \boldsymbol{M}(C_b) = \{(\phi_0, \phi_1, \cdots, \phi_{n-1}) : \phi_i = \boldsymbol{M}(c_{2i}c_{2i+1}) \in S, \ (c_0, c_1, \cdots, c_{2n-1}) \in C_b\}$$

is said to be a two-level LUEP QPSK block-modulation code of length n, dimension k, rate $R = k/2n$ (bits per dimension), and *squared Euclidean separation vector* [6]

$$\bar{S}_{SED} = (2s_1, 2s_2)$$

where, for $i = 1, 2$, the ith component of $\bar{S}_{SED}$ is defined as the minimum squared Euclidean distance (MSED) between any two signal sequences in C whose corresponding ith *message bits* differ. (In [6], $\bar{S}_{SED}$ is defined as the MSED between signal sequences whose corresponding ith *code positions* differ.)

TABLE I
SOME LUEP QPSK BLOCK-MODULATION CODES

$2n$	k	k_1	k_2	s_1	s_2	R(bits/dim)	G_1(dB)	G_2(dB)	
4	2	1	1	3	2	1/2	1.76	0.00	
8	5	1	4	4	2	5/8	3.28	0.27	
8	5	4	1	3	2	5/8	2.03	0.27	
8	6	1	5	3	2	3/4	2.71	0.95	
10	5	1	4	5	4	1/2	3.98	3.01	⋆
10	7	1	6	4	2	7/10	3.65	0.64	
10	7	4	3	3	2	7/10	2.40	0.64	
10	8	1	7	3	2	4/5	3.06	1.30	
12	6	1	5	6	4	1/2	4.77	3.01	⋆
12	6	2	4	5	4	1/2	3.98	3.01	
12	9	1	8	4	2	3/4	3.96	0.95	
12	9	4	5	3	2	3/4	2.71	0.95	
12	10	1	9	3	2	5/6	3.32	1.56	
14	7	1	6	7	4	1/2	5.44	3.01	⋆
14	7	4	3	5	4	1/2	3.98	3.01	
14	8	1	7	5	4	4/7	4.07	3.10	
14	11	1	10	4	2	11/14	4.21	1.20	
14	11	4	7	3	2	11/14	2.96	1.20	
14	12	1	11	3	2	6/7	3.51	1.75	

⋆ = LUEP QPSK code based on the $|\bar{u}|\bar{u} + \bar{v}|$ construction.

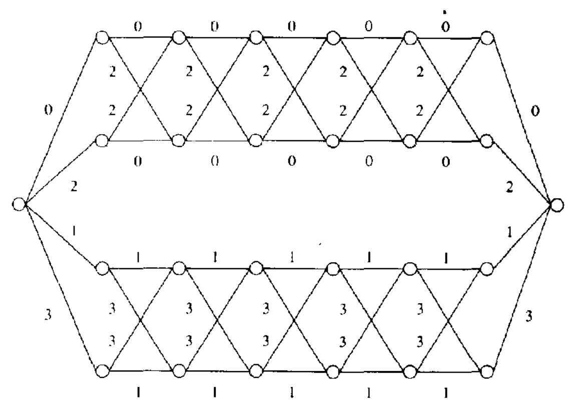

Fig. 2. Trellis diagram for an LUEP QPSK code of length 7.

For AWGN channels at very high signal-to-noise ratios, and given the MSED and rate of a modulation code, the *asymptotic coding gain* G is defined as the ratio of the MSED of the coded system to the MSED of an uncoded system transmitting at the same rate (or number of bits per signal) [8]. Although this coding gain is never realized in practical systems, it is used to provide a measure on the improvement in error performance of a coded system with respect to a comparable uncoded system. Accordingly, for each component of $\bar{S}_{\rm SED}$ an asymptotic coding gain is associated. In this correspondence, the *asymptotic coding gain vector* is defined as

$$\bar{G} = (G_1, G_2),$$

where, for $i = 1, 2$

$$G_i = 10\log_{10}\left[\frac{2s_i}{4\sin^2(\pi/2^R)}\right] \quad \text{(dB)}.$$

To illustrate this construction method, in Table I some QPSK block-modulation codes with two levels of error protection are listed. Codes labeled with ⋆ in the rightmost column of Table I are LUEP QPSK modulation codes obtained from the $|\bar{u}|\bar{u} + \bar{v}|$ construction, have the same minimum squared Euclidean distance as that of *optimal* QPSK block-modulation codes of the same rate and length [2], [3], and provide additional coding gain (or, equivalently, smaller probability

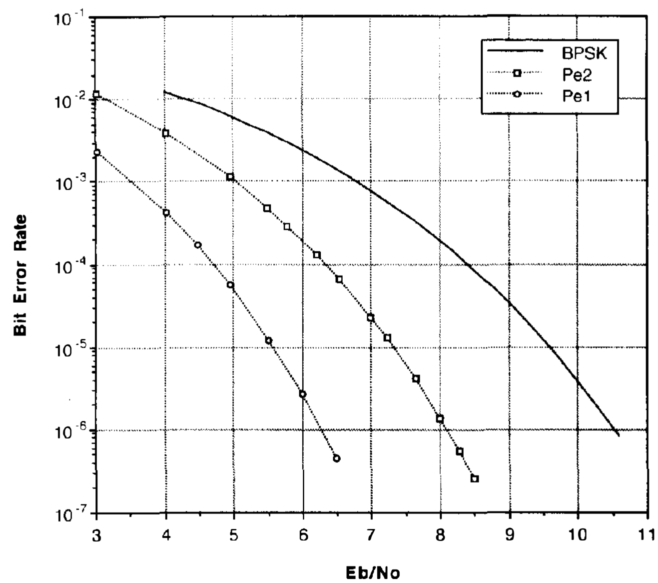

Fig. 3. Error performance of an LUEP QPSK modulation code of length 7.

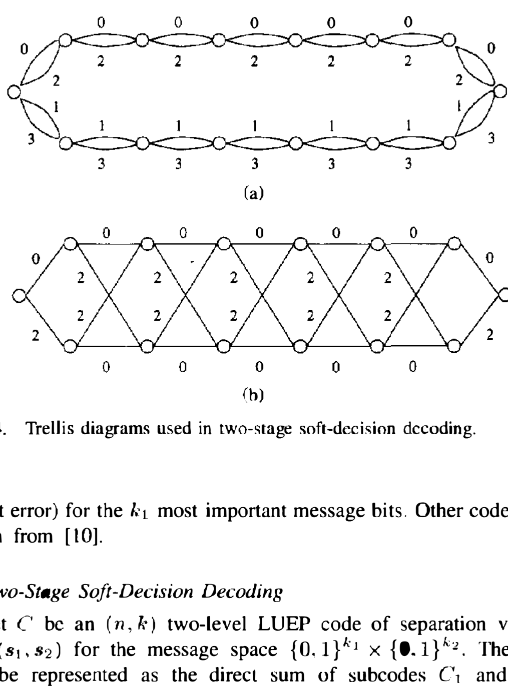

Fig. 4. Trellis diagrams used in two-stage soft-decision decoding.

of bit error) for the k_1 most important message bits. Other codes are taken from [10].

B. Two-Stage Soft-Decision Decoding

Let C be an (n, k) two-level LUEP code of separation vector $\bar{s} = (s_1, s_2)$ for the message space $\{0,1\}^{k_1} \times \{0,1\}^{k_2}$. Then C can be represented as the direct sum of subcodes C_1 and C_2, $C = C_1 \oplus C_2$, i.e

$$C = \{\bar{c} = \bar{c}_1 + \bar{c}_2 : \bar{c}_1 \in C_1 \quad \text{and} \quad \bar{c}_2 \in C_2\}$$

where C_2 is an (n, k_2, s_2) subcode which contains all codewords of minimum weight of C, and C_1 is an $(n, k_1, d_{min} \geq s_1)$ subcode spanned by a system of coset representatives of C_2 in C. Let T_i be a trellis diagram for subcode C_i of C, $i = 1, 2$. Then a trellis diagram of C can be expressed as the direct product of T_1 and T_2, $T = T_1 \otimes T_2$. That is, states in T are pairs (s_1, s_2), where s_i is a state in T_i, for $i = 1, 2$. The pair (s_1, s_2) is joined to all pairs (s_1', s_2'), in such a way that, for $i = 1, 2$, s_i is joined to s_i' in T_i [11]. The Viterbi maximum-likelihood decoding algorithm can then be applied to T to estimate the most likely codeword of C using soft decisions. To reduce the number of computations in soft-decision decoding of a modulation code, a technique called *multistage decoding* is usually employed. The proposed suboptimal two-stage soft-decision decoding for two-level LUEP codes is as follows:

1) Using soft decisions (squared Euclidean distance) and the Viterbi algorithm, determine the closest path $\hat{c}_1$ in T_1' to the received sequence, where T_1' is a trellis corresponding to $C_1 \oplus C_2'$, C_2' a supercode of C_2. At this decoding stage, the most important message part is decoded.
2) Using soft decisions and the Viterbi algorithm, determine the closest path $\hat{c}_2$ in $\hat{c}_1 + T_2$ to the received sequence, to estimate the least important message part. Here $\hat{c}_1 + T_2$ indicates that the value of $\hat{c}_1$, obtained in the first decoding stage, is used at each decoding step of the Viterbi algorithm operating on trellis T_2.

This two-stage soft-decision decoding is well known, see [2], [5], [11]–[13]. However, this appears to be the first time, to the best of our knowledge, that *multistage soft-decision decoding* has been explicitly used for unequal error protection codes. Although at each stage the decoding is maximum-likelihood, the multistage soft-decision decoding method described above is suboptimal. At each decoding stage, the most likely path is estimated using only part (T_i) of the trellis T of C. This suboptimal multistage soft-decision decoding is known to increase the effective number of nearest neighbors, but this results in only a fraction of a decibel in overall coding gain reduction (see [2], [11], [12]).

C. An Illustrative Example

In this example we construct an LUEP QPSK block modulation code of length 7, and decode it using the suboptimal two-stage soft-decision decoding described above. Let C_1 be a $(7, 6, 2)$ parity-check code and C_2 be a $(7, 1, 7)$ repetition code. Then applying the $|\bar{u}|\bar{u} + \bar{v}|$ construction, we obtain a $(14, 7)$ binary LUEP

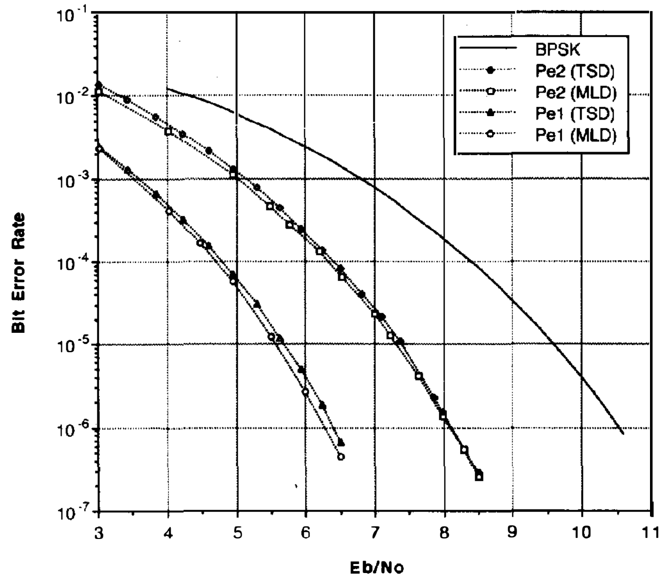

Fig. 5. Error performance of two-stage versus maximum-likelihood soft-decision decoding.

code C_b of separation vector $\bar{s} = (7, 4)$, for the message space $\{0,1\}^1 \times \{0,1\}^6$. With Gray mapping between 2-bit symbols and QPSK signals, we obtain an LUEP QPSK code C of length 7, rate $R = 1/2$ (bits per dimension), and squared Euclidean separation vector $\bar{S}_{\text{SED}} = (14, 8)$. The reference uncoded system is BPSK, which has an MSED of 4. It follows that the asymptotic coding gain vector for this LUEP QPSK block modulation code is $\bar{G} = (5.44, 3.01)$.

To obtain the trellis for code C, the following permuted version of C_b is considered: Repeat each branch of T_1, the trellis of code C_1, twice. This is the $|\bar{u}|\bar{u}|$ part of the construction, where $\bar{u} \in C_1$. This is equivalent to substituting in T_1 each branch label 0 by 00 and each branch label 1 by 11. Then modify trellis T_2 of code C_2 by appending a 0 to each branch label, thus constructing the $|0|\bar{v}|$ part of the code, where $\bar{v} \in C_2$. In this case, this is equivalent to replacing in T_2 each branch label 0 by 00 and each branch label 1 by 01. The trellis of the binary LUEP code C_b is then the direct product of T_1 and T_2, $T_1 \otimes T_2$, corresponding to $|\bar{u}|\bar{u}| + |0|\bar{v}|$, with $\bar{u} \in C_1$ and $\bar{v} \in C_2$. Replacing each 2-bit branch label by an element in $S = \{0, 1, 2, 3\}$, the labels for the QPSK signal set in Fig. 1, according to the Gray mapping $\boldsymbol{M}$ of Section III-A, results in the trellis T shown in Fig. 2.

Note that the minimum squared Euclidean distance between any path in the upper subtrellis and any path in the lower subtrellis of Fig. 2 is $2 \times 7 = 14$, while the minimum squared Euclidean distance between paths within a subtrellis is $2 \times 4 = 8$. (By a path we mean a sequence of QPSK signals whose labels are a path in the trellis). In addition, the signal labels used in a subtrellis are from the same BPSK signal subconstellation, i.e., $\{0, 2\}$ for the upper subtrellis and $\{1, 3\}$ for the lower subtrellis. Soft-decision decoding can now be performed using the Viterbi algorithm with squared Euclidean distances as branch metrics.

Consider *maximum-likelihood soft-decision decoding*. At high signal-to-noise ratios on an AWGN channel, the probability of a block error P_e is dominated by the probability of taking a path in the trellis at minimum squared Euclidean distance, and can be approximated by

$$P_e^{(b)} \approx N(d_{\min})Q\left(\frac{a\sqrt{d_{\min}}}{2\sigma}\right)$$

where $N(d_{\min})$ is the number of paths in the trellis at MSED and a^2 is the average signal power. For this LUEP QPSK block-modulation code, the probability of a block error depends on what message part is being considered. For the least important message part (6 bits), we have

$$P_{e_2}^{(b)} = 21Q\left(a\sqrt{2}\right) + 35Q(2a) + 7Q\left(a\sqrt{8}\right)$$

while for the most important message part (1 bit),

$$P_{e_1}^{(b)} = 64Q\left(a\sqrt{3.5}\right).$$

In both of the above expressions, zero-mean unit-variance additive white Gaussian noise is assumed. Note that the above expressions are upper bounds on the probabilities of a bit error, P_{e_1} and P_{e_2}, in the most and least important message parts, respectively. In Fig. 3, we plot the probability of a bit error for uncoded BPSK and compare it with computer results on the bit error rate of the least important message part P_{e_2} and of the most important message part, P_{e_1}. The results of Fig. 3 were obtained using a one-step maximum-likelihood soft-decision decoding the Viterbi algorithm and the trellis diagram of Fig. 2. From Fig. 3, the simulated coding gains at probability of a bit error of 10^{-5} are approximately $G_1^s = 3.8$ (dB) and $G_2^s = 2.2$ (dB), for the most and least important bits, respectively. These numbers agree well with the expected coding gains $G_1^e = 4.2$ (dB) and $G_2^e = 2.1$ (dB), which are obtained from the asymptotic coding gain vector and taking into account the effects of the number of nearest neighbors (64 and 21, respectively), using the well-known rule of thumb [14] which states that, at probability of a bit error of 10^{-5}, doubling the number of nearest neighbors results in about 0.2-dB coding loss.

Attention is now turned to *two-stage soft-decision decoding*. In the first stage of decoding, trellis T_1', with branch labels as shown in Fig. 4(a), is used to decode the most important message bit. Note that, from the point of view of decoding the most important bit, the number of nearest neighbors has doubled, from 64 for one-step maximum-likelihood soft-decision decoding to 128 for two-stage soft-decision decoding. In the second decoding stage we use T_2, modified according to the decision in the previous step. If the decoded most important bit in the first decoding step is a 0, then we use the trellis T_2 shown in Fig. 4(b). If the decoded message bit in the first stage is a 1, then we modify T_2 replacing each branch label 0 by 1 and each branch label 2 by 3. The computer-simulated error performance of this two-stage soft-decision decoding (TSD) is presented in Fig. 5, and compared to one-stage maximum-likelihood soft-decision decoding (MLD). At a bit error rate of 10^{-5} for the most important message bit, TSD requires about 0.1 dB more E_b/N_0 than with single-stage MLD. This is caused by the twofold increase in the number of nearest neighbors in the first decoding stage, as mentioned before. It can be seen from Fig. 5 that the error performance of the second decoding stage, P_{e_2}(TSD), is very close to that of MLD. Once a correct decision on the most important message bit is made, the subtrellis used in TSD to decode the least important message bits is the same as in MLD. Therefore, at high E_b/N_0, about the same error performance is obtained. These results agree with the observation made in [12] that degradation of overall coding gain, with two-stage soft-decision decoding, is negligible if the MSED of trellis diagram T_1 of subcode C_1 is larger than the MSED of the trellis diagram T of the supercode.

IV. CONCLUSIONS

A new construction of QPSK block-modulation codes for unequal error protection of two types of messages was introduced. These codes offer two values of minimum squared Euclidean distance (MSED) between coded signal sequences associated with each message part. That is, coded signal sequences associated with the most important message part are separated by a squared Euclidean distance (SED) larger than the MSED for the code. When these signal sequences are transmitted over an AWGN channel, a larger SED results in a *smaller probability of error* for the most important message symbols. A Gray mapped QPSK signal set was used to obtain a second-order Hamming space in which $(2n, k)$ LUEP codes of separation vector $\bar{s} = (s_1, s_2)$ are mapped onto (n, k) LUEP QPSK modulation codes of squared Euclidean separation $\bar{S}_{SED} = (2s_1, 2s_2)$. For short lengths, some of the new QPSK block-modulation codes have the same coding gain as that of *optimal* QPSK modulation codes of the same rate and length [3]. A new suboptimal *two-stage soft-decision decoding* for LUEP codes was presented and an illustrative example showed its application in decoding QPSK block-modulation codes for unequal error protection. The results suggest that, with two-stage soft-decision decoding of QPSK block-modulation codes for UEP, *both coding gains* are reduced by only a fraction of a decibel, in the same way that overall coding gain degrades for conventional (equal error protection) modulation codes.

REFERENCES

[1] B. Masnick and J. Wolf, "On linear unequal error protection codes," *IEEE Trans. Inform. Theory*, vol. IT-13, no. 4, pp. 600–607, July 1967.

[2] S. L. Sayegh, "A class of optimum block codes in signal space," *IEEE Trans. Commun.*, vol. COM-34, no. 10, pp. 1043–1045, Oct. 1986.

[3] ——, private communication (tables of codes from reference above), 1992.

[4] N. J. A. Sloane, S. M. Reddy, and C. L. Chen, "New binary codes," *IEEE Trans. Inform. Theory*, vol. IT-18, no. 4, pp. 503–510, July 1972.

[5] H. Imai and S. Hirakawa, "A new multilevel coding method using error-correcting codes," *IEEE Trans. Inform. Theory*, vol. IT-23, no. 3, pp. 371–377, May 1977.

[6] K. Yamaguchi and H. Imai, "A new block coded modulation scheme and its soft decision decoding," in *Proc. 1993 IEEE Int. Symp. on Information Theory* (San Antonio, TX, Jan. 17–22, 1993), p. 64.

[7] F. R. Kschischang, P. G. de Buda, and S. Pasupathy, "Block coset codes for M-ary phase shift keying," *IEEE J. Selected Areas Commun.*, vol. 7, no. 6, pp. 900–912, Aug. 1989.

[8] W. J. Van Gils, "Linear unequal error protection codes from shorter codes" *IEEE Trans. Inform. Theory*, vol. IT-30, no. 3, pp. 544–546, May 1984.

[9] J. F. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1978.

[10] W. J. Van Gils, "Two topics on linear unequal error protection codes: Bounds on their length and cyclic code classes," *IEEE Trans. Inform. Theory*, vol. IT-29, no. 6, pp. 866–876, Nov. 1983.

[11] A. R. Calderbank, "Multilevel codes and multistage decoding," *IEEE Trans. Commun.*, vol. 37, no. 3, pp. 222–229, Mar. 1989.

[12] F. Hemmati, "Closest coset decoding of $|\mathbf{u}|\mathbf{u}+\mathbf{v}|$ codes," *IEEE J. Selected Areas Commun.*, vol. 7, no. 6, pp. 982–988, Aug. 1989.

[13] T. Takata, Y. Yamashita, T. Fujiwara, T. Kasami, and S. Lin, "On a suboptimum decoding of decomposable block codes," in *Coded Modulation and Bandwidth-Efficient Transmission*, E. Biglieri and M. Luise, Eds. Amsterdam, The Netherlands: Elsevier, 1992, pp. 201–212.

[14] G. Ungerboek, "Trellis-coded modulation with redundant signal sets, Part II: State of the art," *IEEE Commun. Mag.*, vol. 25, no. 2, pp. 12–21, Feb. 1987.

The Nonexistence of Some Five-Dimensional Quaternary Linear Codes

R. Daskalov and E. Metodieva

***Abstract*—Let $n_4(k, d)$ be the smallest integer n, such that a quaternary linear $[n, k, d; 4]$-code exists. It is proved that n_4(5, 20) = 30, n_4(5, 42) ≥ 59, n_4(5, 45) ≥ 63, n_4(5, 64) ≥ 88, n_4(5, 80) = 109, n_4(5, 140) ≥ 189, n_4(5, 143) ≥ 193, n_4(5, 168) ≥ 226, n_4(5, 180) ≥ 242, n_4 (5, 183) ≥ 246, n_4 (5, 187) = 251.**

***Index Terms*—Quaternary linear codes, bounds on minimum length.**

I. INTRODUCTION

Let GF(q) denote the Galois field of q elements, and let $V(n, q)$ denote the vector space of all ordered n-tuples over GF(q). A linear code C of length n and dimension k over GF(q) is a k-dimensional subspace of $V(n, q)$. Such a code is called an $[n, k, d; q]$-code if its minimum Hamming distance is d.

A central problem in coding theory is that of optimizing one of the parameters n, k, and d for given values of the other two. Two equivalent version are:

Problem 1: Find $d_q(n, k)$, the largest value of d for which there exists an $[n, k, d; q]$-code.

Problem 2: Find $n_q(k, d)$, the smallest value of n for which there exists an $[n, k, d; q]$-code.

A code which achieves one of these two values is called optimal.

Manuscript received September 9, 1993; revised May 3, 1994.

The authors are with the Department of Mathematics, Technical University, 5300 Gabrovo, Bulgaria.

IEEE Log Number 9408293.