Lecture Notes in Computer Science 514

G. Cohen P. Charpin (Eds.)

EUROCODE '90

International Symposium on Coding Theory and Applications
Udine, Italy, November 1990
Proceedings

Springer-Verlag

Lecture Notes in Computer Science 514

G. Cohen P. Charpin (Eds.)

EUROCODE '90

International Symposium on Coding Theory and Applications
Udine, Italy, November 5-9, 1990
Proceedings

Springer-Verlag
Berlin Heidelberg New York
London Paris Tokyo
Hong Kong Barcelona
Budapest

Series Editors

Gerhard Goos
GMD Forschungsstelle
Universität Karlsruhe
Vincenz-Priessnitz-Straße 1
W-7500 Karlsruhe, FRG

Juris Hartmanis
Department of Computer Science
Cornell University
Upson Hall
Ithaca, NY 14853, USA

Volume Editors

Gérard Cohen
Ecole Nationale Supérieures des Télécommunications
46, rue Barrault, 75634 Paris Cedex 13, France

Pascale Charpin
INRIA, B.P. 105, 78153 Le Chesnay, France

CR Subject Classification (1991): E.4, E.3

ISBN 3-540-54303-1 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-54303-1 Springer-Verlag New York Berlin Heidelberg

Printing and binding: Druckhaus Beltz, Hemsbach/Bergstr.
2145/3140-543210 - Printed on acid-free paper

Preface

Eurocode 90, held in Udine, Italy, 5-9 November 1990, is a continuation as well as an extension of the previous colloquia "Trois Journées sur le codage". The previous ones took place in Cachan, France in 1986 and Toulon, France in 1988 ; their proceedings appeared as Lecture Notes in Computer Science, Volume 311 (G. Cohen, P. Godlewski, eds.) and Volume 388 (G. Cohen, J. Wolfmann, eds.) respectively. The Udine meeting gathered approximately one hundred scientists and engineers.

These colloquia are characterized by a very broad spectrum, ranging from algebraic geometry to implementation of coding algorithms. We would like to thank the referees (see enclosed list) with a special mention for P. Camion, J. Conan, A. Thiong Ly and J. Wolfmann, as well as C. Dubois, secretary of "projet code INRIA" and N. Le Ruyet for help in editing.

1 Algebraic Codes

The construction of spherical codes is now a classical problem related to important special cases, as showed by Delsarte et al. (1977). In their invited paper, Ericson and Zinoviev propose a new construction, improving the method of generalized concatenation. Following the work of A. Dür, two papers deal with the structure of Reed-Solomon codes. Elia and Taricco present new results on code automorphism groups which imply some properties on covering radius and coset weight distribution of RS-codes. Berger gives a new basis describing primitive cyclic codes of length q - 1 over F_q ; as an application he obtains directly the group of some automorphisms of the RS-codes. Beth, Lazić and Šenk present a very simple construction of an infinite sequence of self-dual codes ; properties of the first four codes imply a conjecture on the distance distribution.

The following two papers are devoted to open problems on Reed-Muller codes. Carlet shows that the weight of an RM-code of any order is related to the weight distribution of an RM-code of order 3 and greater length. Langevin studies the covering radius of the RM-code of order 1 and length 2^m, for small odd m ; he obtains a bound for m = 9.

In his paper, Rodier constructs codewords in the dual of binary BCH-codes of length $2^m - 1$, for an infinite number of m ; he can disprove a conjectured improvement of the Carlitz-Uchiyama bound. Augot, Charpin and Sendrier present an algebraic point of view in order to prove or disprove the existence of words of given weight in binary primitive cyclic codes of short length.

2 Combinatorial Codes

The next three papers are devoted to less classical coding problems. Burger, Chabanne and Girault deal with the construction of Gray codes with an additional constraint that 0-1 transitions should be evenly distributed, to provide, e.g., uniform wearing of memories. Mabogunje and Farell construct unequal error protection codes based on array codes and give simulation results for their bit error rates. Cohen, Gargano and Vaccaro propose t-unidirectional error detecting codes with high rates, for both systematic and nonsystematic cases, together with linear time encoding and decoding algorithms.

Two papers are devoted to graphs and finite fields. Montpetit presents some results in graphs which extend combinatorial results in coding theory. Astié-Vidal and Dugat propose a construction of homogeneous tournaments based on Galois fields.

3 Geometric Codes

In 1989, Pellikaan gave an algorithm which decodes geometric codes up to $\lfloor (d-1)/2 \rfloor$-errors, where d is the designed distance of the code. Le Brigand shows how this algorithm can be performed, using some results about the Jacobian of a hyperelliptic curve. Rotillon and Thiong Ly describe an effective decoding procedure for some geometric codes on the Klein quartic. Gallager proved, in 1963, that almost all binary linear codes meet the Gilbert-Varshamov bound. In her paper, Voss presents a generalisation of this result. Moreover she proves that almost all linear codes in the class of subfield subcodes of certain geometric Goppa codes meet the Gilbert-Varshamov bound. Perret constructs nonlinear geometric codes for which the distance is lowerbounded by use of multiplicative character sums.

4 Protection of Information

The invited paper by Girault is devoted to a survey of a large variety of recent identification schemes. Harari introduces a secret key coding scheme which relies on a subset of a particular set of random codes. Patarin presents some improvements to the work of Luby and Rackoff on pseudorandom permutations.

The paper by Fell deals with the effects of bit change errors on the linear complexity of finite sequences. Chassé considers the situation where the cells of a LFSR over F_q are disturbed by sequences of elements of F_q. Creutzburg obtains valuable results for the determination of convenient parameters for complex number-theoretic transforms.

Domingo-Ferrer and Huguet-Rotger describe a cryptographic scheme for program protection by means of a coding procedure, using a one-way function and a public-key signature.

5 Convolutional codes

The basic principles and limitations of decoding techniques for convolutional codes are presented by Haccoun. Visualizing the decoding process as being a search procedure through the tree or trellis representation of the code, he gives methods to circumvent the inherent shortcomings of Viterbi and sequential decoding. Sfez and Battail describe a weighted-output Viterbi algorithm used in a concatenated scheme where the inner code is convolutional, and simulate it over Gaussian and Rayleigh channels. Baldini Filho and Farrel present a multilevel convolutional coding method over rings, suitable for coded modulation, and show curves of performance for 4-PSK and 8-PSK.

6 Information Theory

This section starts with an invited paper by Sgarro offering a Shannon-theoretic coding theorem for authentication codes. Next paper, by the same author together with Fioretto, continues work on fractional entropy, a kind of measure of uncertainty for list coding. The section ends with two papers on source coding: Battail and Guazzo compare the respective merits of three algorithms (Huffman-Gallager, Lempel-Ziv and Guazzo) ; Capocelli and De Santis derive a tight upper bound on the redundancy of Huffman codes, in terms of the minimum codeword length, and use it to improve a bound due to Gallager.

7 Modulation

The invited paper by Calderbank describes how binary covering codes can be used to design non-equiprobable signaling schemes for use in high-speed modems, gaining in low-dimensional space as would shaping the boundaries of the signal constellation in higher dimensions. The next paper, by Battail, De Oliveira and Weidong, considers a combination of an MDS code over a large alphabet and a one-to-one mapping of the alphabet into a symmetric constellation, for combined coding and multilevel modulation. Two modulation-coding schemes are compared by Sfez, Belfiore, Leeuwin and Fihel for low-rate digital land mobile radio communication. Finally, Leeuwin, Belfiore and Kawas Kaleh derive a Chernoff upper bound for the pairwise error probability over a correlated Rayleigh channel.

8 Application of coding

Darmon and Sadot propose a hybrid ARQ+FEC system using a convolutional code with large constraint length and sequential decoding, combined with a modified Go-Back-N ARQ protocol, adapted to a two-way troposcatter (Rayleigh) channel. The last paper, by Politano and Deprey, describes a VLSI implementation of a Reed-Solomon coder-decoder.

List of Referees

D. Augot, G. Battail, F. Bayen, J.C. Belfiore, P. Camion, C. Carlet, G. Castagnoli, P. Charpin, G. Chassé, G. Cohen, J. Conan, B. Courteau, M. Darmon, J.L. Dornstetter, H. Fell, L. Gargano, M. Girault, C. Goutelard, S. Harari, D. Haccoun, S. Lebel, D. Le Brigand, A. Lobstein, G. Longo, H.F. Mattson, P. Langevin, A. Montpetit, F. Morain, G. Norton, J. Patarin, J.J. Quisquater, P. Sadot, N. Sendrier, P. Solé, H. Stichtenoth, A. Thiong Ly, U. Vaccaro, J. Wolfmann, G. Zémor.

June 1991

Gérard Cohen
Pascale Charpin

Contents

1. Algebraic Codes

2. Combinatorial Codes

3. Geometric Codes

4. Protection of Information

5. Convolutional Codes

6. Information Theory

7. Modulation

8. Applications of Coding

CONSTRUCTION OF UNEQUAL ERROR PROTECTION CODES

A. O. Mabogunje and P. G. Farrell
Communications Research Group
Department of Electrical Engineering
University of Manchester
Manchester M13 9PL

Introduction

The study of unequal error protection(uep) codes has been prompted by an increase in the volume of digital data being transmitted across communication channels, where an increasing percentage of this data has reliability requirements that vary within a block of data. Classical error control codes, also referred to in this text as equal error protection (eep) codes, provide the same level of protection for all parts of an information block. This makes them non-optimal for protecting data with uep requirements. It is possible to optimize the redundancy in an error control code by giving different parts of an information block different levels of protection. This can be done by using uep codes. The concept of uep codes was first introduced by Masnick and Wolf (1967).

The objective in this paper is to draw attention to construction methods by which array codes can be modified to provide unequal error protection, and to highlight some of the advantages of using uep codes. Simulation results are shown for some array codes with unequal error protection.

Relative minimum distance

The minimum distance of a code relative to any information position is always the same in an eep code and is equal to the true minimum distance of the code. The error correction capability of such random error correction codes is based on the true minimum distance of the code. In a uep code, the situation is different because the relative minimum distance of the code differs from one information position to another and is not always the same as the true minimum distance of the code. In other words, information symbols in different positions see the code as having different minimum distances. The error correction capability of a uep code is therefore based on a more complicated distance parameter known as the separation vector, which was introduced by Dunning and Robbins (1978). Unlike the minimum distance of a code, which is independent of the generator matrix used in encoding, the separation vector is dependent on the generator matrix. It is therefore defined with respect to a particular generator matrix. The individual components of the separation vector refer to the minimum distance of a code relative to a particular position in the information stream being encoded.

Preliminary definitions.

Let the symbols in the information stream to be encoded be taken from GF(q) and let

$I = \{ I_j : j=0, 1,...,k-1 \}$ be the information stream with k positions per word,

$C = \{ C_j : j=0, 1,...,n-1 \}$ be an n-symbol codeword of a code V,

and $C^{(i,j)}$ be a codeword formed from an information stream with symbol 'i' in position I_j.

The *separation* of position I_j in the information stream I with respect to a code with generator matrix G and weight function w is the minimum distance of the code relative to position I_j and is defined as

$$s_w(G)_j = \min_i w\left(C^{(i,j)} - C^{(i',j)}\right) \qquad i \neq i'$$

The *separation vector* is defined along the same lines as

$$S_w(G) = \{ s_w(G)_i : i = 0,1,\ldots,k-1 \}$$

When no ambiguity will result, the separation $s_w(G)_i$ will be represented as s_i and the separation vector $S_w(G)$ as S. For large codes, the above form of the separation vector is cumbersome and it becomes convenient to use the polynomial form of the separation vector which is introduced below:

$$S = \sum_{b=0}^{z} a x^b$$

where a is the number of information bits that have a separation of b and z is the number of protection levels.

When reference needs to be made to a particular generator matrix and weight function, subscripts may be used in the usual manner.

The *protection level* t_j of an information position j with separation s_j is defined as

$$t_j = \lfloor (s_j - 1)/2 \rfloor$$

where $\lfloor x \rfloor$ is the integer part of x.

The protection spread of a code is defined as: $p = 1 + (s_{max} - s_{min})$ where s_{max} and s_{min} are the maximum and minimum components of the separation vector. By this definition, eep codes have a unit protection spread. Note that this is a slightly different from the protection bandwidth introduced by Pingzhi et al. (1988).

Construction of unequal error protection codes from array codes.

Two information arrays (square or rectangular, say) are said to be orthogonal in the j^{th} order if and only if no more and no less than j positions are common to any of their rows and columns. There is a finite number of orthogonal arrays of the j^{th} order that can be formed on any particular array of information positions. In this study, orthogonal array codes of the first order are of primary interest because they are easy to understand and are easily decoded by one step majority logic decoding algorithms. Most of the arguments for the first order orthogonal arrays hold for higher order arrays. The three possible first order orthogonal 5x5 arrays that can be formed with twenty-five information positions are shown in figure 1. Let

each position hold a binary information symbol. Each row and column can be made a codeword of an even

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

1	10	14	18	22
7	11	20	24	3
13	17	21	5	9
19	23	2	6	15
25	4	8	12	16

1	8	15	17	24
9	11	18	25	2
12	19	21	3	10
20	22	4	6	13
23	5	7	14	16

Figure 1: Orthogonal arrays possible with 25 positions

parity check code by adding a 1 or a 0 to make the number of non-zeros in the row an even number. The result is a 6x6 array without the check on checks (figure 2). There are two sets of parity information on each array. One set corresponds to symbols a-e and the other to symbols f-k in figure 2. Due to the fact that the parity information is formed from orthogonal information arrays, each set of parity is orthogonal to the others and can be used independently to increase the minimum distance of the code by one. All six sets of parity information formed on the above arrays can be combined to give a triple error correcting (55,25,7) code. By combining different numbers of parity sets, the following eep (n,k,d) array codes can be formed:(30,25,2), (35,25,3), (40,25,4), (45,25,5), (50,25,6) and (55,25,7). The simulated bit error rates of the (55,25,7), (45,25,5) and (35,25,3) codes when used for random error correction are shown in figure 3, from which it is seen that there is little difference in performance below E_b/N_o values of 10dB. The decoding algorithm used in the simulation is a one step majority logic decoding algorithm. It should be noted from table 2 that the asymptotic coding gains of these codes differ.

Table 2

code	asymptotic coding gain (dB) 10log(rate x min. dist)
(55,25,7)	5.027
(45,25,5)	4.437
(35,25,3)	3.3099

1	2	3	4	5	a
6	7	8	9	10	b
11	12	13	14	15	c
16	17	18	19	20	d
21	22	23	24	25	e
f	g	h	j	k	

Figure 2: 6x6 array without check on checks.

If all the information in a parity set is not used simultaneously, a code with non-unity protection spread will result. For example, if only those parity symbols that check the information symbol in one particular position are included in the code, only one parity check is included from each of the parity sets and the separation vector of the resulting (31,25) code will be

$$S = x^7 + 25x^2$$

Figure 3: Bit Error Rate curves for (55,25), (45,25) and (35,25) array codes

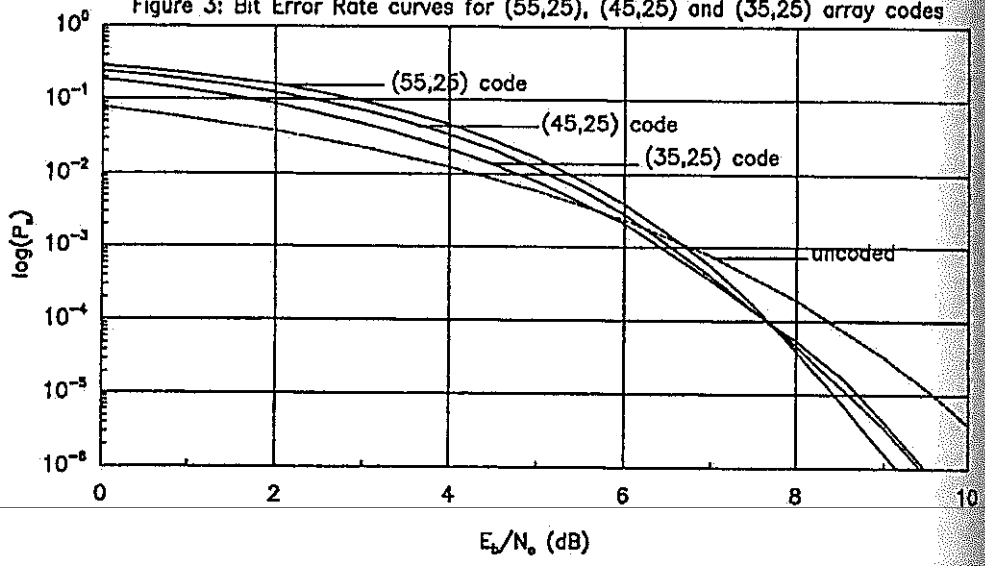


Figure 4: BER for (39,25,S_1)code

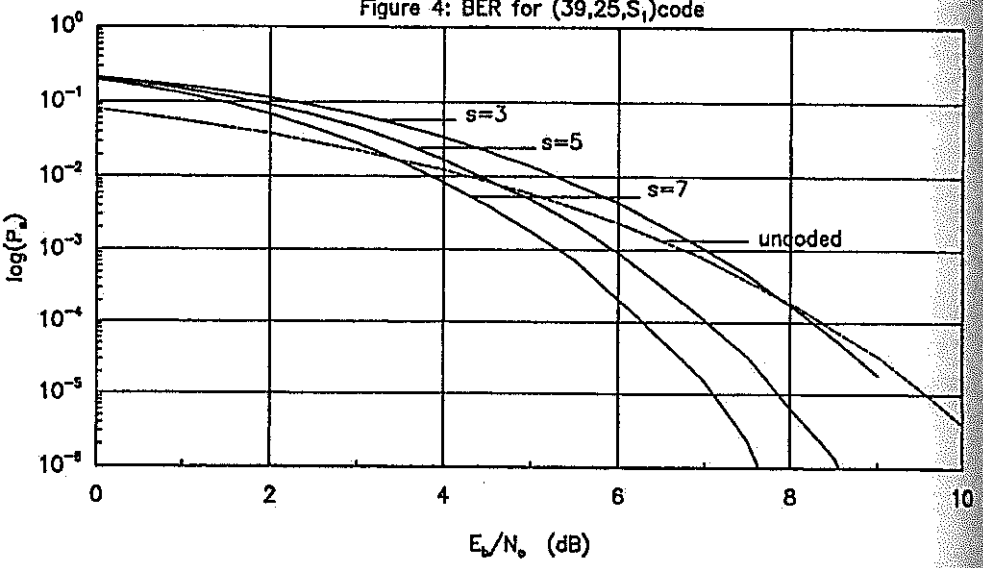


Figure 5: BER in positions with s=7 in $(39,25,S_1)$ and (55,25,7) codes

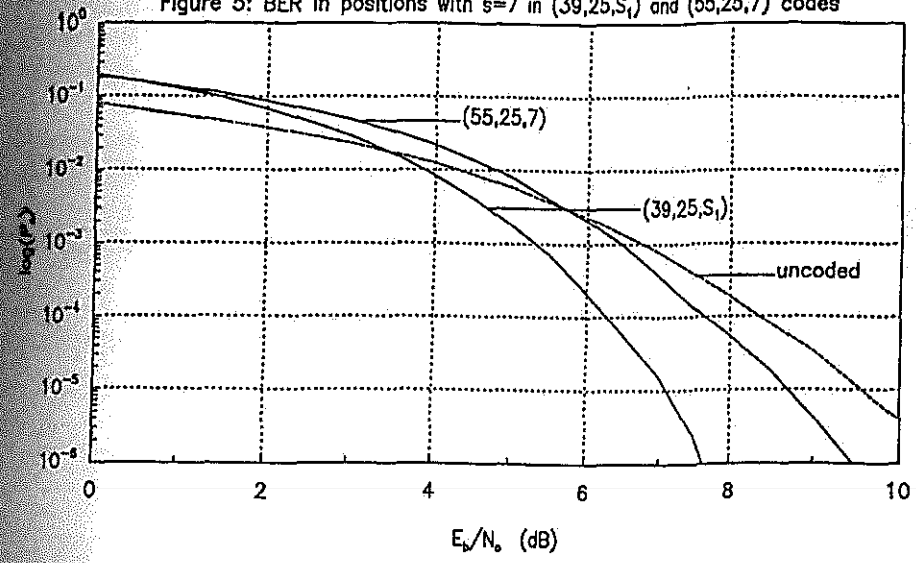


Figure 6: BER in positions with s=5 in $(39,25,S_1)$ and (45,25,5) codes

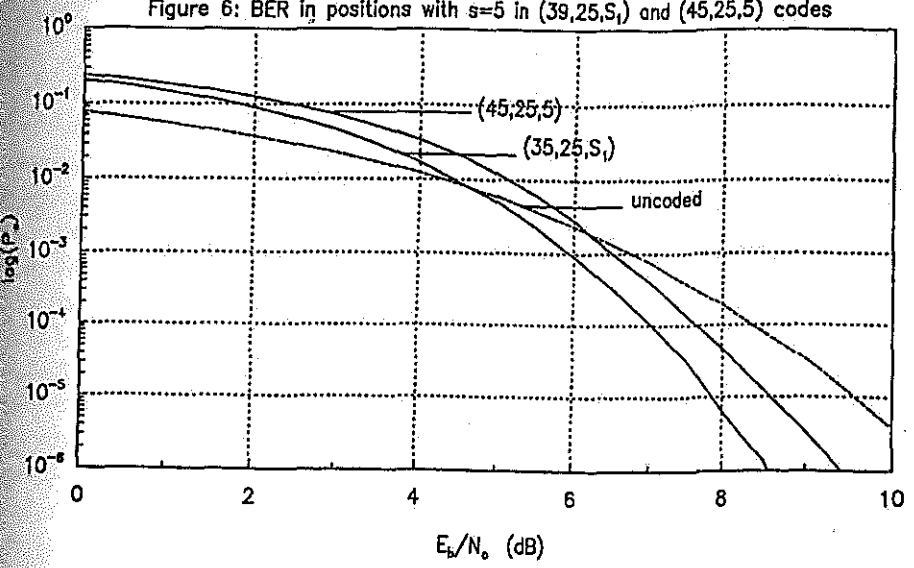


Figure 7: BER in positions with s=3 in (39,25,S_1) and (35,25,3) codes

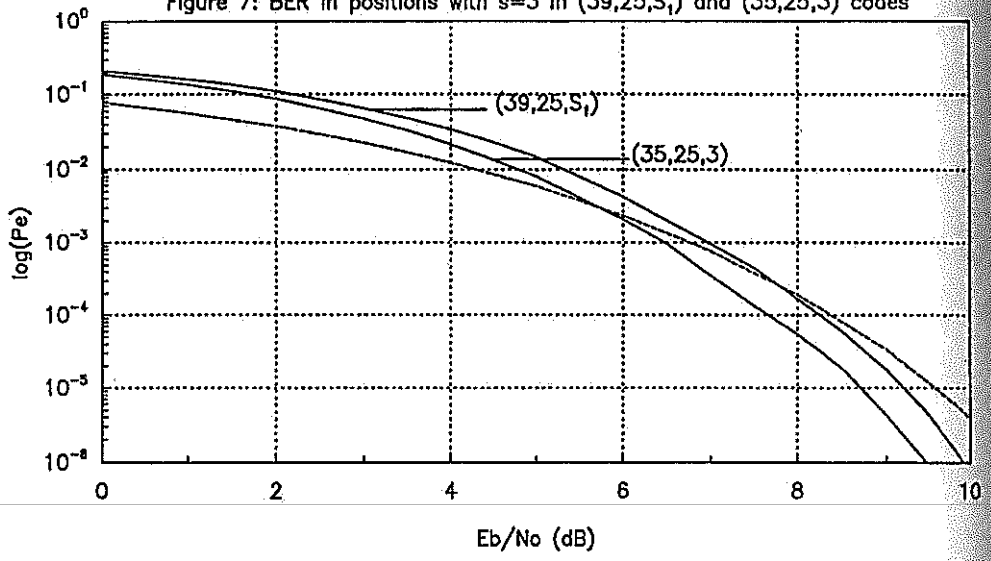
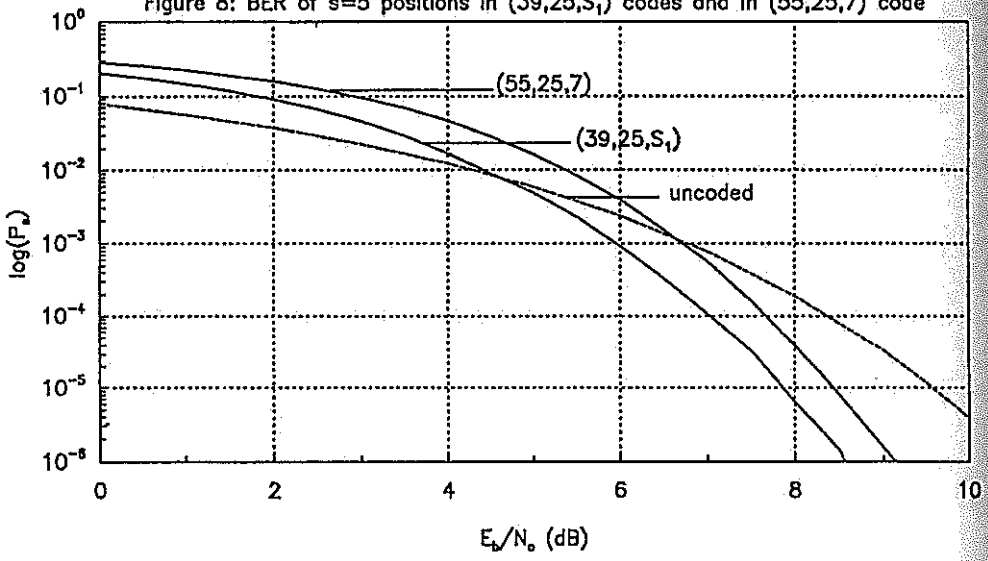


Figure 8: BER of s=5 positions in (39,25,S_1) codes and in (55,25,7) code



Many uep array codes can be formed in this way. As an example of the uep codes that can be achieved, the focus here will be mainly on the array codes introduced above, i.e. the (35,25), (45,25) and (55,25) codes and the (39,25,S_1) code, where

$$S_1 = 2x^7 + 2x^5 + 8x^4 + 13x^3$$

The parity symbols in this code are formed as illustrated in table 3, and the BER performance is shown in figure 4. The first row of table 3 means the parity symbol in position 1 checks the information in positions 1, 2, 3, 4 and 5 of the information word. Column 1 tells us that the information in position 1 is checked by parity symbols in parity positions 1, 5, 6 and 7.

Table 3

position	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
parity no. 1	*	*	*	*	*																				
2						*	*	*	*	*															
3											*	*	*	*	*										
4																*	*	*	*	*					
5	*					*					*					*					*				
6	*						*						*						*						*
7	*								*			*								*			*		
8		*								*			*			*								*	
9		*							*		*							*							*
10			*					*					*					*					*		
11			*						*						*	*						*			
12				*		*							*							*		*			
13				*					*					*					*					*	
14					*				*				*				*				*				

Concluding Remarks

A comparison of the error rates in positions with the same separation in the different codes confirms the theory that the error rate of a code depends on both its distance structure and its rate. Figure 5, 6 and 7 shows the BER in those information positions with a separation of 7, 5 and 3 respectively. The advantage of uep can be seen in figures 5 and 6, which shows that the protection received by the information in the s=5 and s=7 positions of the (39,25,S_1) code is greater than that received by information with an identical separation in the (45,25,5) and (55,25,7) codes respectively. This improvement in performance is easily explained by the higher rate of the (39,25,S_1) code. A similar explanation can be given for the lower protection received by the s=3 positions of the (39,25,S_1) code when compared to positions with identical separations in the (35,25,3) code as shown in figure 7. Finally, a situation where the advantages of a high rate out-weighs that of a slightly increased separation is illustrated in figure 8, where it is shown that below 10dB, the BER in the s=7 positions of the (55,25) code is higher than that in the s=5 positions of the (39,25) code.

References

1. B. Masnick and J. Wolf, " On Linear Unequal Error Protection Codes," IEEE *Trans. Inform. Theory*, vol. IT-3 no. 4, pp 600 - 607, Oct. 1967.

2. L. A. Dunning and W. E. Robbins, "Optimal encodings of linear block codes for unequal error protection" *Information and control*, vol 37, pp 150 - 177, 1978.

3. F. Pingzhi, C. Zhi and J. Fan, "One Step Completely Orthogonalisable UEP Codes and Their Soft Decision Decoding," *Electronic Letters*, vol. 24, no. 17, pp 1095 - 1096, 18 Aug. 1988.