DIXIEME COLLOQUE SUR LE TRAITEMENT DU
SIGNAL ET SES APPLICATIONS

NICE du 20 au 24 MAI 1985

PERFORMANCE EVALUATION OF BERLEKAMP-MASSEY DECODING ALGORITHM FOR AN AWGN CHANNEL

Hala ABDEL KADER Magdi EL-SOUDANI

Electronics and Electrical Communications Department
Faculty of Engineering - Cairo University - Egypt .

RESUME

Les codes correcteurs d'erreurs sont employés pour assurer la fiabilité de la transmission de données sur des voies bruyantes . A cet effet, les chercheurs dans ce domaine se sont efforcés de trouver des codes ayant de bonnes performances et de concevoir des techniques de décodage efficaces et pratiquement réalisibles . Certains procédés de décodage sont basés sur la structure algébrique des codes . Ceux-ci sont alors appelés les techniques du décodage algébrique . Ces procédés sont de complexité acceptable et sont utilisables pour de larges classes de codes linéaires .

En ce travail on considère une classe importante de codes, les codes BCH . Berlekamp a présenté une simple algorithme récursive pour décoder les codes BCH . Massey démontra que le procédure de décodage, est le même que celui du synthèse d'un registre a décalage rebouclé linéairement de longueur minimale, capable de générer une certaine séquence de symboles .

Les performances du décodage ont été effectuées sur un canal gaussien en utilisant des codes BCH binaires et non binaires . Dans le cas de codes BCH binaires, on utilise le code BCH(15,7,5). La performance du décodage de codes Reed-Solomon a été considérée comme un exemple de codes BCH non binaires . En ce domaine, on considère un système concaténé où un code de Reed-Solomon est utilisé comme un code extérieur . On utilise l'algorithme de Berlekamp -Massey pour le décodage extérieur seulement .

Enfin, on présente une simple modification de l'algorithme de Berlekamp-Massey donnant la possibilité de corriger des erreurs ainsi que des effacements . Les résultats obtenus par simulation quand on utilise l'algorithme modifiée, montrent l'amélioration de performance bien que la complexité du décodage soit à peu près la même .

SUMMARY

Error correcting codes are used to ensure reliable data transmission over noisy channels . To achieve this purpose, several works have been devoted to find high performance codes as well as practical cal decoding techniques . Some of the decoding approaches depend on the algebraic structures of the codes, therefore they are called algebraic decoding techniques . These techniques are of reasonable complexity and can be applied to a large class of linear codes .

In this paper we deal with an important family of codes which is the BCH codes . Berlekamp has introduced a simple iterative algorithm for decoding BCH codes . Massey has shown that the decoding procedure is the same as that of synthesizing the shortest linear feedback shift-register capable of generating a prescribed finite sequence of digits .

The decoding performance has been studied for an AWGN channel using binary and non binary BCH codes . The decoding performance of Reed-Solomon codes is studied as an example of non binary BCH codes . We consider a concatenated system where a RS code is used as an outer code. We apply the Berlekamp-Massey algorithm only for the outer decoding .

Finally, we present a simple modification of the Berlekamp-Massey algorithm to use it to correct erasures and errors. The decoding performance results -over an AWGN channel- show clearly the additional gain obtained by the modified algorithm . Moreover, the decoding complexity is nearly the same .

PERFORMANCE EVALUATION OF BERLEKAMP-MASSEY DECODING ALGORITHM FOR AN AWGN CHANNEL

I. INTRODUCTION

Spite of the different forms of decoding schemes and the mathematical rules that govern them, they all make use of redundancy . The redundant symbols are used to accentuate the uniqueness of each message hence they help to clear noise-introduced errors .

In this paper, we shall deal only with a class of linear cyclic block codes which is BCH codes .

The BCH codes form a subclass of cyclic block codes . For any positive integers t and m such that $(t < 2^{m-1})$, there exists a BCH code whose block length, $n = 2^m-1$, number of parity check digits, $n-k \leq mt$, and minimum distance, $d \geq 2t + 1$. Such a code is capable of correcting any combination of t or fewer errors .

II. ALGEBRAIC DECODING OF BCH CODES

The algebraic decoding is a decoding procedure of reasonable complexity which enables the correction of a fixed number of errors (in terms of the code characteristics) . It is used for a large class of codes . Studying it for cyclic codes and specially for BCH codes, we found that the decoding procedure consists of two major steps : syndrome calculation and the processing of the syndrome to determine the error pattern . The latter step is much more complicated and, necessitates, as we shall see later, the determination of an error-locator polynomial whose roots are the errors' positions .

III. BERLEKAMP-MASSEY DECODING ALGORITHM FOR BCH CODES

Berlekamp presented an iterative algorithm /5/ giving the error-locator polynomial . Massey showed the equivalence of the decoding problem for BCH codes to a shift-register syntesis problem /1/ . Thus, using the Berlekamp-Massey algorithm, the problem of evaluating the error-locator polynomial, is as simple as the problem of synthesizing the shortest linear feedback shift-register (LFSR) . Such a LFSR is capable of generating a prescribed finite sequence of digits (which is the syndrome sequence in our case as will be shown later) . For the above reason, we give the presentation of a decoding procedure for BCH codes using th Berlekamp-Massey algorithm .

III.1 Notation and Formulation of the Problem

Suppose the codeword $\underline{v} = (v_0, v_1, \ldots v_{n-1})$, $\underline{v} \in C$ is transmitted over a noisy channel and corrupted by the additive noise $\underline{e} = (e_0, e_1, \ldots e_{n-1})$. Then, the disturbed vector $\underline{r} = \underline{e} + \underline{v}$ is received . The decoding problem is to determine $\underline{e}$, given $\underline{r}$.

Let $u(x)$ be the polynomial representation of the vector $\underline{u}$ such that, $u(x) = u_0 + u_1 x + \ldots + u_{m-1}x^{m-1}$.

Associating polynomials with $\underline{r}$, $\underline{e}$ and $\underline{v}$, we have :

$$r(x) = e(x) + v(x) \qquad (1)$$

Assuming the Hamming weight of the error vector e is such that :

$$wt(\underline{e}) = \theta \leq t \qquad (2)$$

Let a_i indicate the positions of non-zero elements in $\underline{e}$, then we can write the error polynomial in the form :

$$e(x) = \sum_{i=1}^{\theta} e_{a_i} x^{a_i} \qquad (3)$$

$$\text{Let } X_i = \alpha^{a_i} \text{ and } Y_i = e_{a_i} \qquad (4)$$

hence

$$e(\alpha^j) = \sum_{i=1}^{\theta} Y_i X_i^j \qquad (5)$$

X_i is called the error locator and it is an element of $GF(q^m)$ while Y_i is called the error magnitude and is an element of $GF(q)$. For binary codes, $q = 2$, the error locators completely describe the error pattern since $Y_i = 1$. On the other hand for non binary codes (Reed-Solomon codes for example) both X_i and Y_i belong to $GF(q^m)$.

The decoding procedure can be divided into three steps :

1. Calculation of the syndrome .
2. Finding the error-locator polynomial and its roots .
3. Determining the value of the errors (in case of non binary BCH codes) .

These procedures are illustrated in Fig.1.

III.2 Syndrome Calculation

For decoding a BCH code, the syndrome is defined as a vector $\underline{S}$ with 2t components as follows /4/ :

$$S_i = r(\alpha^i) = e(\alpha^i) + v(\alpha^i) = e(\alpha^i) \qquad i \in (1, 2, \ldots 2t) \qquad (6)$$

and from equation (5) :

$$S_i = \sum_{j=1}^{\theta} Y_j X_j^i \qquad (7)$$

which are also called the power sums .

III.3 The Error-Locator Polynomial

We define the error-locator polynomial :

$$\sigma(Z) = \prod_{i \text{ errors}} (Z - X_i) \qquad (8)$$

The element α^{-1}, $\alpha^{-1} \in GF(q^m)$, is a root of $\sigma(Z)$ if and only if an error has occurred in position 1 (X_1) , (see equations (3) and (4)) .

Let E(Z) be the infinite degree syndrome polynomial written as /2/ :

$$E(Z) = \sum_{j=1}^{\infty} E_j Z^{-j+1} \quad \text{where } E_j = S_j$$

$$= Z \sum_i Y_i \sum_j X_i^j Z^{-j}$$

$$= Z \sum_i Y_i (X_i Z^{-1})/(1 - X_i Z^{-1})$$

$$= \sum Y_i X_i /(1 - X_i Z^{-1}) \qquad (9)$$

We notice that E(Z) may be reduced to a fraction form where $\sigma(Z)$ is the denominator :

$$E(Z) = Z^{\theta} P(Z)/\sigma(Z) \qquad (10)$$

Only the first 2t coefficients of E(Z) series are known . This information is

quite enough to determine $\sigma(Z)$ since we have assumed that $(\theta \leq t)$. Equation (10) is called the key equation of the decoding process .

III.4 Solution of the Key Equation

Since the coefficients of the polynomial E(Z) are known only up to the coefficient of Z^{2t-1}, so in terms of these known coefficients and with the substitution of Z by D^{-1}, equation (10) can be written as :

$$S(D)\, C(D) = R(D) \bmod D^{2t} \qquad (11)$$

where $S(D) = \sum_{i}^{2t} S_i\, D^{i-1}$ (=E(Z) where $Z = D^{-1}$)

$C(D) = D^{\theta}\, \sigma(D^{-1})$ (reciprocal polynomial of $\sigma(D)$)

and $R(D) = P(D^{-1})$ (= P(Z) where $Z = D^{-1}$) .

The Berlekamp-Massey decoding algorithm used to obtain the reciprocal of the error-locator polynomial $\sigma(D)$; C(D) is given in /1/ .

III.5 Determination of the Error Values

This step is required only when decoding non binary BCH codes . To determine the value of the error in the i-th position , i.e. Y_i, we proceed as follows: referring to equations (9), (10) and (11) we nave :

$$S(D) = R(D)/C(D) =$$

$$= \Sigma_i\, Y_i\, X_i/(1-X_i\, D) \qquad (12)$$

From equation (12) :

$$R(D) = C(D)\ \Sigma_i\, Y_i\, X_i/(1-X_i\, D)$$

$$= \Sigma_i\, Y_i\, X_i\, \Pi_i\, (1-X_i\, D)/(1-X_i\, D)$$

$$= \Sigma_i\, Y_i\, X_i \prod_{j \neq i} (1-X_j\, D) \qquad (13)$$

Consider the derivative of the polynomial C(D) ; C'(D) :

$$C'(D) = -\Sigma_i\, X_i \prod_{j \neq i} (1-X_j\, D) \qquad (14)$$

Substituting (14) in (15), it becomes :

$$R(D) = -C'(D)\, \Sigma_i\, Y_i$$

and hence for a certain error in position i, (X_i), we have :

$$R(X_i^{-1}) = -Y_i\, C'(X_i^{-1})$$

from which the value of the error is :

$$Y_i = R(X_i^{-1})/C'(X_i^{-1}) \qquad (15)$$

III.6 Berlekamp-Massey Algorithm for a Concatenated System

As an example of a decoding scheme using the Berlekamp-Massey algorithm is the concatenated system /6/ .
We consider a two stage concatenated code where a non binary BCH code, the Reed-Solomon code, is used as an outer code . We apply the Berlekamp-Massey algorithm for the outer decoding, while maximum likelihood decoding is assumed for the inner decoder /7/ . The overall performance is studied over an additive white gaussian noise, (AWGN), channel .

IV. CORRECTION OF ERASURES AND ERRORS

It has been recognized that there are advantages in allowing the demodulator not to guess at all on certain transmissions when the evidence does not clearly indicate one signal as the most probable ; such events are called "erasures /3/ .

The decoder has as goal now, to correct all the errata which consist of two types : erasures, whose locations are known but whose values are unknown, and errors, whose locations and values are both unknown .

Algebraic decoding algorithms can be modified to handle erasures efficiently . In the next paragraph we explain how the Berlekamp-Massey algorithm can be modified to deal with this situation .

Consider a code of minimum distance d, all combinations of v channel errors and e erasures are correctable providing that :

$$2v + e < d \qquad (16)$$

The Modified Algorithm

We define $\sigma_{\xi}(D) = \prod_{i \text{ erasures}} (1-\alpha^i\, D)$

to be the reciprocal erasure-locator polynomial, of degree = e
We have :

1) $\sigma_{\xi}(D) \longrightarrow C(D)$ $\quad 1 \longrightarrow B(D)$ $\quad 1 \longrightarrow x$
$\quad 0 \longrightarrow L$ $\quad\quad 1 \longrightarrow b$ $\quad\quad e \longrightarrow N$

2) If N = n, stop . Otherwise, compute
$L' = L + e$

$$d = S_N + \sum_{i=1}^{L'} c_i\, S_{N-i}$$

3) If d = 0, $x + 1 \longrightarrow x$ and go to 6) .

4) If $d \neq 0$, and $2L > N-e$, then

$C(D) - db^{-1}\, D^x\, B(D) \longrightarrow C(D)$
$x + 1 \longrightarrow x$
go to 6)

5) If $d \neq 0$ and $2L \leq N-e$, then
$C(D) \longrightarrow T(D)$ (temporary storage of C(D))

$C(D) - db^{-1}\, D^x\, B(D) \longrightarrow C(D)$
$N + 1 - L - e \longrightarrow L$
$T(D) \longrightarrow B(D)$
$d \longrightarrow b$
$1 \longrightarrow x$

6) $N + 1 \longrightarrow N$ and go to 2) .

Where n is the syndrome sequence length (2t), L' is the register length, S_i are the syndrome sequence terms and $C(D) = 1 + c_1\, D + c_2\, D^2 + \ldots + c_{L'}\, D^{L'}$, gives the reciprocal erasure and error locator polynomial . The syndrome terms are calculated using a modified received word obtained by replacing the erasures

with zeros .
In the original algorithm, C(D) is normalized by 1, and N (the iteration number) is normalized by 0 in step 1) . Also the register length is equal to L . The resulting C(D) using the original algorithm is clearly the reciprocal error-locator polynomial .

The roots of C(D) (obtained using the modified algorithm) give, the erasures and errors locations . Since the erasures' positions are already known, hence, the errors' positions can be determined . To find the value of an erasure we use equation (15) .

V. DECODING PERFORMANCE OF BCH CODES

Computer simulation has been carried out over an AWGN channel to study the decoding performance of the Berlekamp-Massey algorithm for binary and non binary BCH codes . The same channel has been chosen to study the decoding performance of the modified algorithm for binary BCH codes .

V.1 Decoding Binary BCH Codes

The simplest case to be considered is that of antipodal signalling over an AWGN channel .

Let X be the output of a matched filter . It has a gaussian distribution with mean equal to $S\sqrt{E}$ and variance equal to No/2, where E is the energy received per binary symbol, $S = (-1)^c$ (c represents the transmitted symbol) and No is the one side spectral density of the noise .

The demodulator guesses which symbol is transmitted according to its sign .

For a t-error correcting BCH code of length n, the word error probability is given by the probability that more than t errors occur in a codeword, i.e.

$$P_w = \sum_{i=t+1}^{n} \binom{n}{i} p^i (1-p)^{n-i} \qquad (17)$$

where p is the symbol error rate on the considered channel . For a gaussian channel, $p = Q(\sqrt{2E/No})$. Assuming that a pattern of i channel errors ($i > t$) will cause the decoded word to differ from the correct word in i + t positions and thus a fraction of (i + t)/n of the k information symbols to be decoded erroneously . Thus, an upper bound of the symbol error probability for BCH codes is given by :

$$P_s \leq \sum_{i=t+1}^{n} \frac{i+t}{n} \binom{n}{i} p^i (1-p)^{n-i} \qquad (18)$$

Considering the erasures and errors decoding, the channel outputs can be represented as shown in Fig.2 . We can say that the demodulator output has been quantized into three levels as shown in Fig.4 .
The decoding performance results over an AWGN channel of the BCH(15,7,5) code are given in figures 4 and 5 .

We have considered the cases where single, double and three erased symbols are allowed . Also we consider the case where the number of erased symbols is arbitrary . If the number of erased symbols exceeds d-1, the decoder passes the received word as it is with an indication that it failed to decode it . We have chosen two threshold values, $T = 0.05\sqrt{\frac{No}{2}}$ and $0.1\sqrt{\frac{No}{2}}$.

V2. Decoding Non Binary BCH Codes

As we pointed earlier, in section III.6, we study the decoding performance of Reed-Solomon codes, as an example of non binary BCH codes, in a concatenated system . The simulation results of the concatenated code(105,44,15) consisting of the Hamming code(7,4,3) as an inner code, and the Reed-Solomon code(15,11,5), as an outer code, are given in figures 6 and 7 .
The Reed-Solomon error probabilities are bounded by equations (17) and (18) . In this case, p is the Reed-Solomon symbol error probability at the outer decoder input and can be determined by simulation.

VI. REMARKS

From the simulation results, we found that a coding gain of about 0.4 db, at a bit error probability of 10^{-4}, can be obtained in the case of erasures and errors decoding . This gain depends upon the choice of the quantization levels . When a single erased symbol is considered, the gain is around 0.3 db at a bit error probability of 10^{-4} . When two erased symbols are allowed, we get a gain of about 0.8 db at a bit error probability of 10^{-4} .
It is evident that with the modified algorithm we can get an additional gain of 0.4 db compared with the original algorithm . The additional gain obtained with the modified algorithm, is due to the fact that more information is passed to the decoder (by the demodulator), thus improving its performance .

It is clear that the threshold choice affects the decoding performance . By a proper threshold choice, better results could be obtained . Also the number of allowed erased symbols greatly affects the performance .

We have only considered the decoding performance over an AWGN channel ; however the applied modified algorithm will be of more benefit on certain interference channels, where the interference may be treated as erasures .

Finally, for non binary BCH codes. a coding gain of about 3.9 dbs at a bit error probability of 10^{-4}, can be obtained. On the other hand, on observing the output of the outer decoder, we get an improvement of about 3.5 dbs as compared with its input at a symbol error probability of 10^{-4} .

ACKNOWLEDGMENT

Thanks are due to P. GODLEWSKI, ENST, Paris, for his help in this paper .

REFERENCES

1) JAMES L. MASSEY, "Shift-Register Synthesis and BCH Decoding", IEEE Trans. on Information Theory, IT-15, pp. 122-127, January 1969 .

2) P. GODLEWSKI, "Codes Correcteurs d'Erreurs", notes de cours, Ecole Nationale Suppérieure des Télécommunications (ENST). Paris, 1981 .

3) G. DAVID FORNEY, "Generalized Minimum Distance Decoding", IEEE Trans. on Information Theory, IT-12, pp. 125-131, April 1966 .

4) S. LIN, "An Introduction to Error-Correcting Codes", N-J : Prentice-Hall, Inc. 1976 .

5) E.R. BERLEKAMP, "Algebraic Coding Theory", Mc Graw-Hill, 1968 .

6) G. DAVID FORNEY, "Concatenated Codes", MIT Press, Cambridge, Mass., 1966 .

7) M. EL-SOUDANI and G. BATTAIL, "Soft Decoding Using a Trellis for a Concatenated System", neuvième colloque GRETSI sur le traitement du signal et ses applications , Nice, France, 1983 .

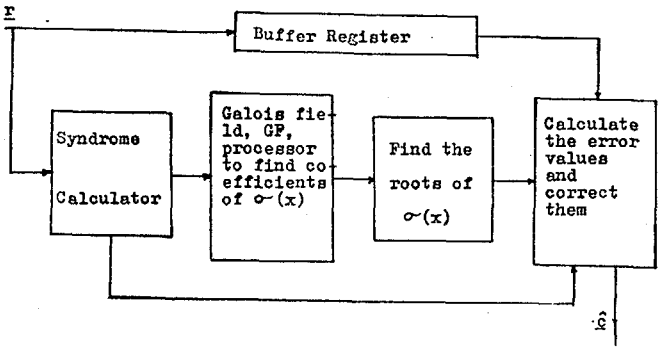


Fig.1 Algebraic decoder for BCH codes

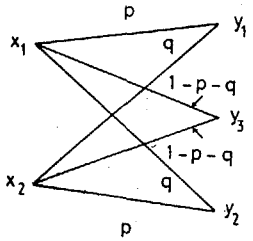


Fig.2 Quantized channel model

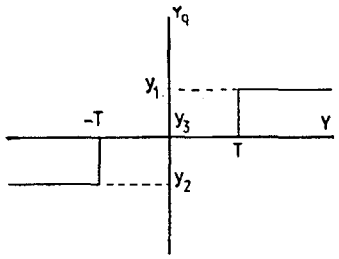


Fig.3 Quantization levels

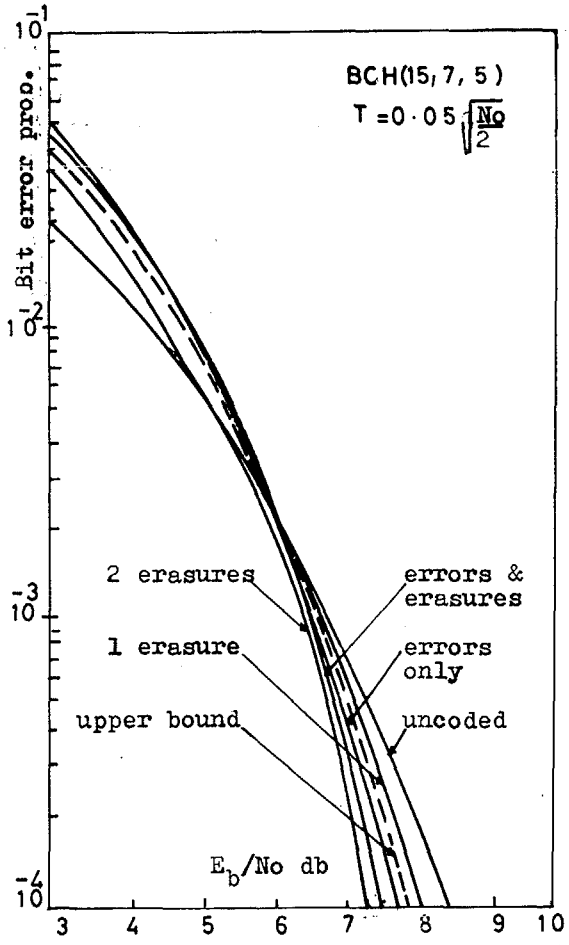
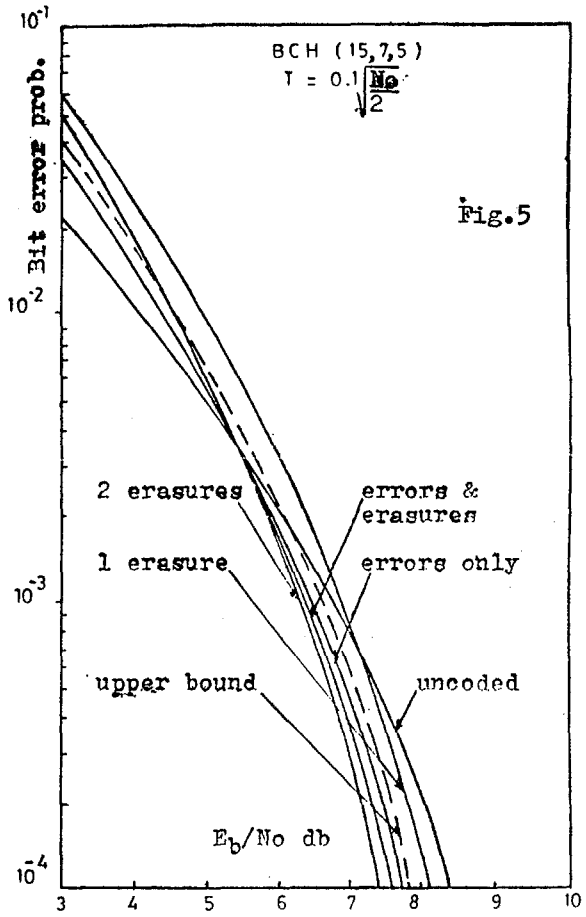
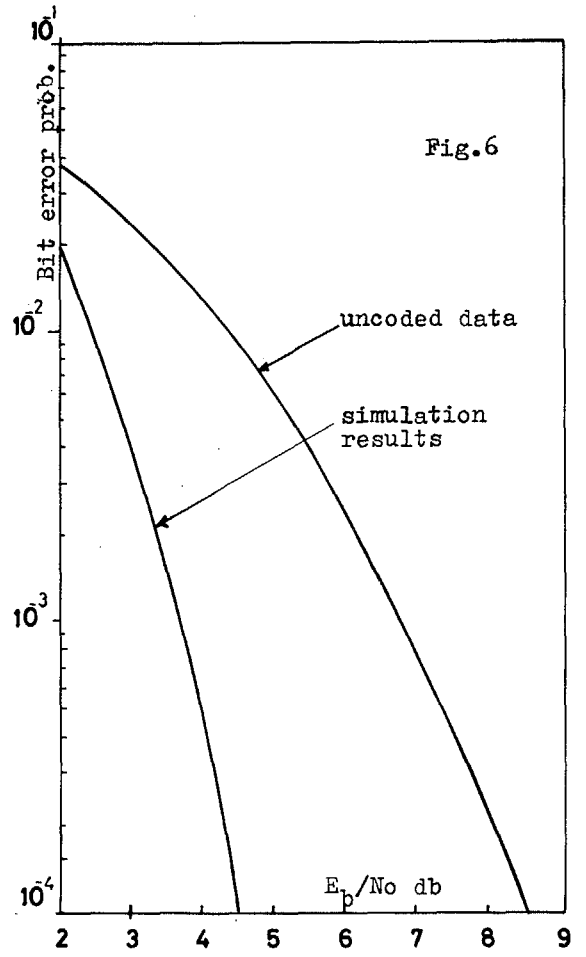


Fig.4 Decoding performance for a gaussian channel using BCH(15,7,5) with $T=0.05\sqrt{\frac{No}{2}}$





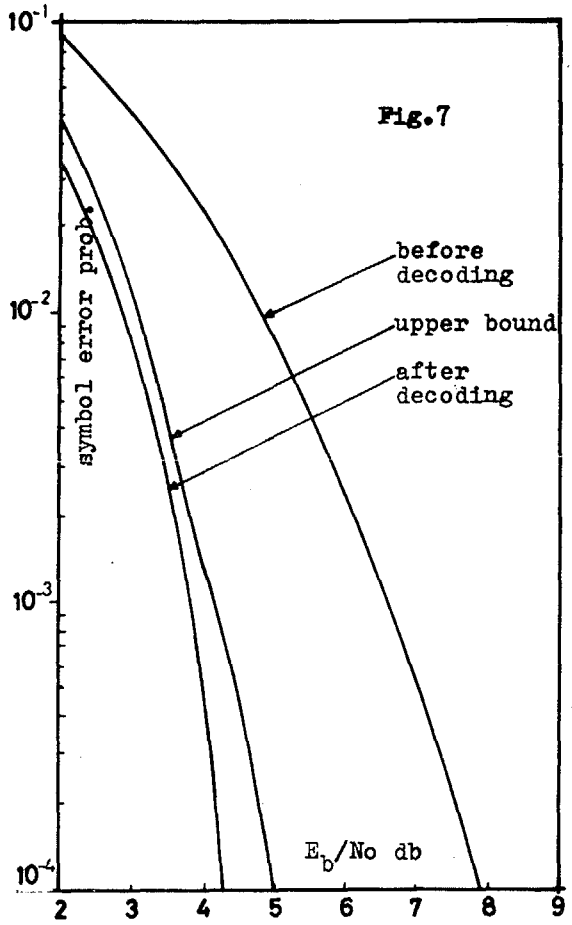


Fig.5 Decoding performance for a gaussian channel using BCH(15,7,5) with $T=0.1\sqrt{\frac{No}{2}}$

Fig.6 Decoding performance for a gaussian channel using the concatenated code(105,44,15) (having an inner code, the Hamming code(7,4,3), and an outer code, the Reed-Solomon (15,11,5)) .

Fig.7 Decoding performance for a gaussian channel of the outer decoder .