Hybrid-ARQ system for HF channels based on codeword partitioning

J.Serrat-Fernández
J.Dalmau-Royo

Indexing terms: Error correction, Codeword partitioning, Type 2 hybrid ARQ, HF communication

Abstract: A technique by which the codewords of an error-correcting code are partitioned to obtain an error-detecting code with half the original length is described. It is intended to be used in a hybrid-ARQ system for achieving high throughput on HF channels. Performance evaluations of examples based on BCH and RS codes are also provided.

1 Introduction

Owing to the nonstationary behaviour of the HF channel, conventional error control techniques such as forward error control (FEC) or automatic repeat request (ARQ) [1] are not suitable if the best use of the available channel capacity is required. For these channels some kind of adaptive procedure must be used in the sense that the amount of redundant information increases when more errors occur. Type-2 hybrid-ARQ schemes [1–3] are well known representatives of this general concept.

Krishna and Morgera [3] proposed a generalisation of the type-2 hybrid-ARQ schemes (GH-ARQ) based on KM codes. Since then, other error control strategies have been compared with GH-ARQ or with some of its members. For representative examples see [4, 5]. In this vein, the present paper describes an alternative to some members of the GH-ARQ family referred to as codeword partitioning. This technique can be used to implement a hybrid type-2 system with higher throughput than that of GH-ARQ when short codes are used like those often encountered in HF transmission. For these applications especially, the communication system is required to be inexpensive and robust and to have minimum size and power consumption. Hence the need to study simple codes with relatively short block or constraint lengths.

2 Codeword partitioning approach

Consider a particular (n, k, d) error correcting code with $k < n/2$. Once the k information bits have been encoded the n-bit codeword is partitioned into two equal blocks of m bits, where $m = n/2$, or $m = \text{int}[n/2] + 1$ if n is not a multiple of two, and int[x] is defined as the integer part of x. The first block, referred to as I, groups together the k information bits and $m–k$ parity bits selected from the whole $n–k$ in such a way that the minimum distance d_0 between these m-bit codewords is maximised. The procedure to fulfil this requirement is explained hereinafter. On the other hand, the second block, referred to as P, contains the remaining parity bits plus one possible stuffing bit.

IEE Proceedings online no. 19960341

Paper first received 18th April 1995 and in revised form 19th January 1996

J. Serrat-Fernández is with Universitat Politècnica de Catalunya, Department of Signal Theory and Communications, Campus Nord UPC Edifici D-4, Gran Capitán, s/n 08034 Barcelona, Spain

J. Dalmau-Royo is with ENHER, Department of Communications, Córcega 333, 08037 Barcelona, Spain

2.1 Transmitting procedure

The transmitter sends I and P blocks alternatively, i.e. I_1, P_2, I_3, P_4, ..., until it receives an ACK from the receiver.

2.2 Receiving procedure

Until the k information bits are accepted the receiver gets the sequence I_1, P_2, I_3, P_4, ..., referred to as the first transmission, the second transmission, and so on. Once the block I_1 is available, the receiver carries out an error detection process based on the (m, k, d_0) code. If no errors are detected the k information bits are delivered and the process is ended by sending an ACK to the transmitter. Otherwise, the receiver sends a NACK and the process continues.

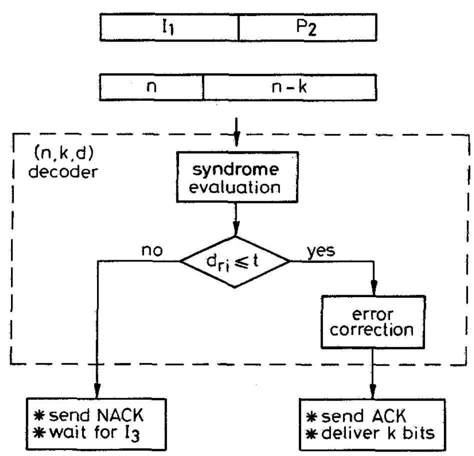

Fig. 1 *Process carried out by proposed ARQ scheme after reception of second transmission*
d_{ri} is Hamming distance between block and ith codeword

Once the block P_2 is available, the receiver combines I_1 and P_2 to carry out the decoding procedure based on the (n, k, d) parent code as follows. If the syndrome reveals that the distance between the received block and any of the 2^k codewords is smaller or equal to t, t being the error correction capability of the code, error correction process takes place, the information bits are delivered and the process is ended by sending an ACK to the transmitter. Otherwise (see Fig. 1) the third transmission is requested by sending the NACK. Note that for any t error correcting code, among the 2^n possible received blocks there will be $2^k \Sigma_0^t \binom{n}{i}$ blocks whose distance to any codeword is smaller than or equal to t.

If the third transmission is requested, the receiver first processes I_3 as I_1 from the first transmission. But at this point, if errors are detected I_3 is combined with P_2 to carry out the same process as that carried out with the second transmission. This is the procedure for all subsequent odd transmissions.

This algorithm has a very low complexity at both the transmitter and the receiver sites. In fact, besides the encoder and the decoder, which are simple owing to the fact that it is believed to use short-length codes, the control mechanisms required have the same complexity as in conventional selective-repeat ARQ systems.

2.3 Design of optimum partition

Consider an (n, k, d) linear block code defined by its $[k \times n]$ generating matrix G. The goal is to form an (m, k, d_0) code by selecting $m-k$ columns of G to constitute the parity part of its $[k \times m]$ generating matrix G'. The selected columns should be those which maximise d_0. Therefore a process to efficiently compute the minimum distance (d_0) of a given code is mandatory. With this goal in mind we propose using the property of the parity check matrix H' related to d_0 which states that no more than $d_0 - 1$ columns of H' will be linearly independent [1].

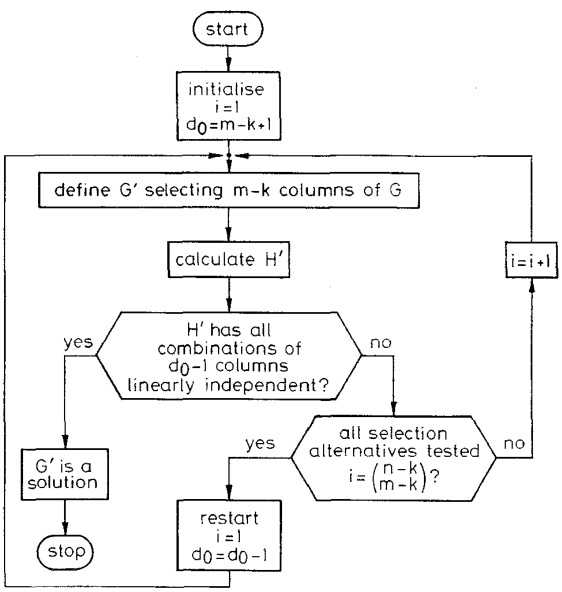

Fig. 2 *Program flowchart to derive the optimum partition with generating matrix G' from parent code with generating matrix G*

Fig. 2 shows the flowchart of a computer program designed to ascertain how many columns in H' are linearly independent. This is the proposed algorithm to achieve the optimum partition.

3 Application examples with BCH and RS codes

First consider the code BCH (31, 11), whose generating matrix is shown in Fig. 3. Suppose that blocks of 16 bits are chosen to make a consistent partition. Furthermore, since all 11 information bits must be included in the first transmission, there will only be place for five redundancy bits. In terms of the generator matrix, the five columns selected according to the principles stated in the previous Section are the 21st, 23th, 25th, 26th and 27th from left to right in Fig. 3. In this case the resulting (16, 11) code exhibits a minimum distance d_0 equal to three..

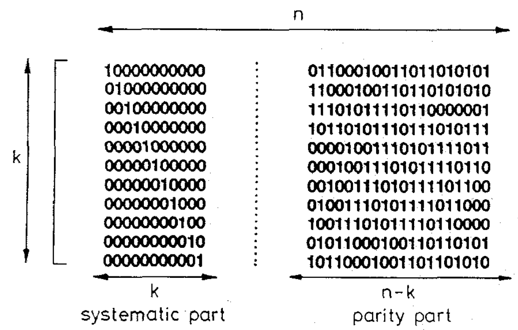

Fig. 3 *Generating matrix of BCH (31, 11) error correcting code used in examples*

At this point, a performance evaluation of the proposed strategy is to be carried out. In this context, two parameters are of interest, namely the system reliability and the system throughput, to compare our approach to a GH-ARQ using the BCH (15, 11) error detecting code and the (15, 5, 5) KM error correcting code, which is the closest approach in terms of the rate and length of the codes involved. Throughout this analysis and later simulations, an ideal backward channel is considered. Therefore both ACK and NACK messages reach the transmitter without being corrupted.

3.1 Reliability

In this context we restrict attention to evaluating the probability of having undetected errors when the information is delivered in the first or second transmission, P_{w1} and P_{w2}, respectively. In the case of the first transmission the undetectable error patterns are the codewords of the (16, 11) code. Therefore if $\{w_i\}$ is the weight distribution of this code,

$$P_{w1} = \sum_{i=1}^{16} w_i p^i (1-p)^{16-i} \qquad (1)$$

where p is the channel bit error rate (BER) and w_i is the number of codewords of weight i. The derivation of P_{w2} is carried out in the appendix. P_{w2} is the probability of the event B2, defined in the appendix.

Fig. 4 shows both reliability figures as functions of the BER. Note that the reliability of the GH-ARQ reference system is in practice the same as P_{w1} because it uses the BCH (15, 11) error detecting code instead of the (16, 11).

3.2 Throughput

The derivation of the system throughput is restricted so as to consider the effect of the first three transmissions only; in other words, any block of information bits will be delivered with no more than three transmissions.

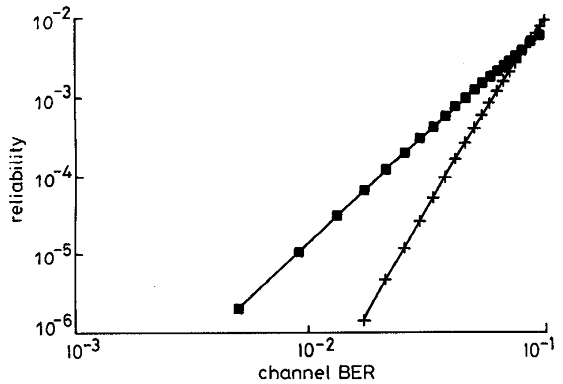

Fig. 4 *First and second transmission reliabilities for codeword partitioning using BCH (31, 11) error correcting code*
■——■ first transmission
+——+ second transmission

This simplifying assumption makes the analysis easier and it can be shown that it is a good approximation of the real system throughput even in high channel BER conditions. Thus, the throughput is expressed as

$$\eta = p_1 r_1 + p_2 r_2 + p_3 r_3 \tag{2}$$

where p_1, p_2 and p_3 are the probabilities of information delivery in the first, second and third transmissions, respectively. For their part, the r_i terms are the associated cumulative rates, 11/16, 11/32 and 11/48 in the example. Probability p_1 can be written as

$$p_1 = (1-p)^{16} + \sum_{i=1}^{16} w_i p^i (1-p)^{16-i} \tag{3}$$

In fact, the first term is the probability of having no errors and the second term is the probability of having undetectable error patterns as in eqn. 1. The derivation of p_2 and p_3 follows in the appendix.

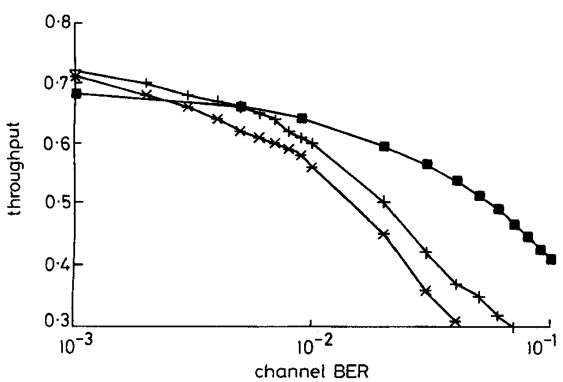

Fig. 5 *Throughput for codeword partitioning with BCH (31, 11) and two throughput lower bounds for GH-ARQ [BCH (15, 11); KM (15, 5)]*
■——■ proposed system
+——+ first lower bound
✳——✳ second lower bound

Fig. 5 shows the throughput η evaluated as a function of the channel BER. It also presents two throughput lower bounds for the reference GH-ARQ scheme calculated as in [3].

3.3 Some results for HF channel

The HF channel was modelled by means of data collected in field trials on short-range links, and also by means of a laboratory long-range HF channel simulator [6, 7]. Likewise, a protocol was developed to implement the encoding, decoding and control processes of two independent ARQ systems: one using the BCH (31, 11) [6], partitioned as previously described, and the other the RS (15, 5) partitioned into (8, 5) and (8, 0) subblocks. For practical purposes, the maximum number of transmissions for a given data block was limited to three in both cases. Interleaving was used in both protocols.

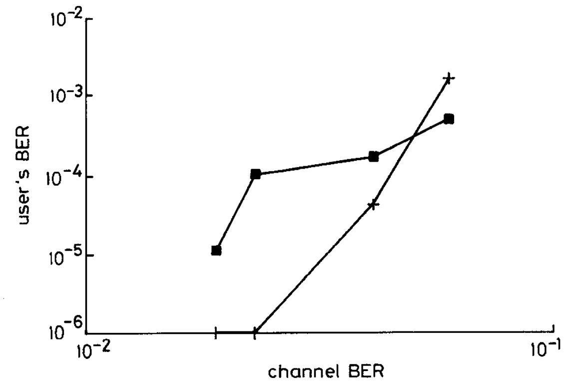

Fig. 6 *Residual bit error rate for cases analysed in HF channels*
■——■ BCH (31, 11)
+——+ RS (15, 5)

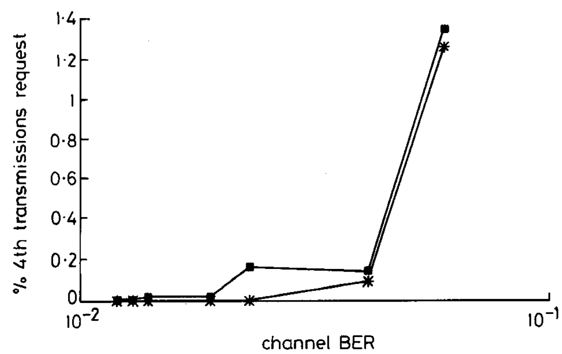

Fig. 7 *Relative number of four transmissions requests (percent) to total number of transmissions for cases analysed in HF channels*
■——■ BCH (31, 11)
✳——✳ RS (15, 5)

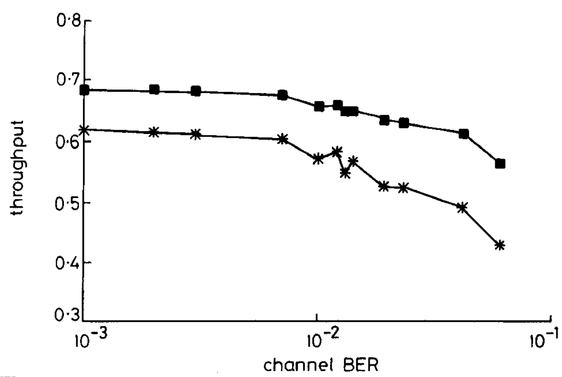

Fig. 8 *Systems throughput in HF channels*
■——■ BCH (31, 11)
✳——✳ RS (15, 5)

Fig. 6 shows the user's BER when our ARQ system uses the BCH (31, 11) or the RS (15, 5) error correcting codes. Errors only appeared for channel BER greater than about 2×10^{-2} and 4×10^{-2}, respectively, which in turn can be considered as poor or very poor channel propagation conditions. Fig. 6 also shows a sharp increase in the user's BER, or threshold effect. This effect was attributed to the fact that the maximum number of transmissions for a given data block was limited to three in our tests. This is confirmed by the results shown in Fig. 7, plotting the relative number of fourth transmissions requested. Around the threshold point a sudden increase in fourth transmission requests is observed. This suggests that having allowed the fourth transmission, the user's BER curves shown in Fig. 6 would be smoother, although with a very low penalty in the throughput of the protocol. Fig. 8 shows the throughput evolution for the two coding schemes considered in this example.

4 Conclusions

In spite of its limitations the analysis shows that the codeword partitioning technique performs better than a GH-ARQ based on similar rate and length codes. Furthermore, the proposed system does not introduce any extra complexity to the transmitter or to the receiver and it allows a transmission of equal block lengths.

Our approach is not as flexible as the GH-ARQ system concerning the selection of the error detecting code. In fact, if a rate k/n error correcting code is going to be used it is necessary to work with a rate $2k/n$ error detecting code. But although this $2k/n$ error detecting code would be wasteful in the event of relatively long codewords, this is not the case in the intended application to HF channels where short-length blocks are required.

5 References

1 LIN, S., and COSTELLO, D.J.: 'Error control coding: fundamentals and applications' (Prentice-Hall, Englewood Cliffs, NJ, USA, 1983)

2 LIN, S., and YU, P.S.: 'A hybrid ARQ scheme with parity retransmissions for error control of satellite channels', *IEEE Trans.*, 1982, **COM-30**, pp. 1701–1719.

3 KRISHNA, H., and MORGERA, S.D.: 'A new error control scheme for hybrid ARQ systems', *IEEE Trans.*, 1987, **COM-35**, pp. 981–990

4 BATE, S.D., HONARY, B., and FARRELL, P.G.: 'Error control techniques applicable to HF channels', *IEE Proc. I*, 1989, **136**, (1), pp. 57–63

5 KOUSA, M.A., and RAHMAN, M.: 'An adaptive error control system using hybrid ARQ schemes', *IEEE Trans.*, 1991, **COM-39**, (7), pp. 1049–1057

6 DALMAU, J., and SERRAT, J.: 'Performance analysis of a hybrid ARQ system in half duplex transmission at 2400 bps', Fifth international conference on *HF radio systems and techniques*, Edinburgh, UK, July 1991, pp. 248–252

7 DALMAU, J.: 'Contribution to the study and design of channel coding schemes for data mobile radiocommunications in the HF band', Doctorate thesis, Universitat Politècnica de Catalunya, Barcelona, 1991, (in Spanish)

6 Appendix: Basis for reliability and throughput evaluation of protocol based on partition of BCH(31, 11)

Assume the protocol state in the second transmission. Consider the following mutually exclusive events to characterise this transmission:

event A: The total number of errors in the 31 bit block has been between 1–5; i.e. the maximum error correction capability of the BCH (31, 11).

event B1: The total number of errors is greater than five and the 31 bit block is outside any of the spheres of radius five (Hamming distance) centred at each codeword of the BCH (31, 11).

event B2: The total number of errors is greater than five and the 31 bit block is inside one of the above mentioned spheres.

The knowledge of the probabilities of these events is necessary to determine the second transmission reliability and the mean throughput rate as well. In fact, P_{w2} being the probability of not detecting errors after the second transmission, we write

$$P_{w2} = P\{B2\} \tag{4}$$

On the other hand, the throughput evaluation requires the probabilities of information delivery in the first, second and third transmissions, p_1, p_2 and p_3, respectively. Clearly,

$$\begin{aligned} p_2 &= P\{A\} + P\{B2\} \\ p_3 &= P\{B1\} \end{aligned} \tag{5}$$

Evaluation of $P\{A\}$

The total number of errors between the two transmissions being e, we write

$$P\{A\} = \sum_{n=1}^{5} P\{e = n\} \tag{6}$$

$$P\{e = n\} = \sum_{i=1}^{n} P\{e_1 = i\} P\{e_2 = n - i\} \tag{7}$$

where e_1 is the number of detectable errors in the first transmission and e_2 is the number of errors in the second. Then

$$\begin{aligned} P\{e_1 = i\} &= \left[\binom{16}{i} - W_i\right] p^i (1-p)^{16-i} \\ P\{e_2 = n - i\} &= \binom{15}{n-i} p^{n-i} (1-p)^{15-(n-i)} \end{aligned} \tag{8}$$

where W_i is the number of codewords of weight i in the (16, 11) error detecting code and p is the channel BER. Substituting eqn. 8 into eqn. 7 we have

$$P\{e = n\} = p^n (1-p)^{31-n} \sum_{i=1}^{n} \left[\binom{16}{i} - W_i\right] \binom{15}{n-i} \tag{9}$$

and finally

$$P\{A\} = \sum_{n=1}^{5} \left(p^n (1-p)^{31-n} \sum_{i=1}^{n} \left[\binom{16}{i} - W_i\right] \binom{15}{n-i} \right) \tag{10}$$

Evaluation of $P\{B2\}$

We call attention to the fact that here the total number of errors is greater than five. Then

$$P\{B2\} = \sum_{n=6}^{31} \alpha_n P\{e = n\} \tag{11}$$

where α_n is the conditional probability of having the 31 bit block inside one sphere, provided that the total number of errors is n, and $P\{e = n\}$ is, as before, the probability of having n errors. The expression for $P\{e = n\}$ is as in eqn. 9 except when $n > 16$, where the limits 1 and n in the summation should be replaced by $(n - 15)$ and 16, respectively.

Evaluation of $P\{B1\}$

$P\{B1\}$ is formally the same as $P\{B2\}$ but using $(1 - \alpha_n)$ instead of α_n

Evaluation of α_n

The nonzero terms of the weight distribution of the BCH (31, 11) are as follows: $A_0 = 1$; $A_{11} = 186$; $A_{12} = 310$; $A_{15} = 527$: $A_{16} = 527$; $A_{19} = 310$; $A_{20} = 186$; $A_{31} = 1$. Assume that $n = 6$ and a codeword C is transmitted throughout the two transmissions. From the weight distribution we conclude that C is at a Hamming distance of 11 from 186 codewords, at 12 from 310 codewords, and so on. Therefore the six errors we have assumed can send C only outside any sphere or inside one sphere of radius five centred at one of the 186 codewords distant 11 from C. The number of ways in which C can fall inside a given sphere are

$$\binom{11}{6}$$

Therefore the total number of cases where six errors can send C inside one of any of the 186 spheres is

$$186\binom{11}{6}$$

As there are

$$\binom{31}{6}$$

error patterns, we conclude that

$$\alpha_6 = \frac{186\binom{11}{6}}{\binom{31}{6}} = 0.1167$$

Similarly, the other α_n can be found. The procedure is repetitive and is therefore omitted; the numerical results are summarised in Table 1.

Table 1: Values calculated for the coefficients α_n

α_6, α_7, α_{24}, α_{25}	0.1167
α_8, α_9, α_{22}, α_{23}	0.1789
α_{10}, α_{11}, α_{20}, α_{21}	0.2014
α_{12}, α_{13}, α_{18}, α_{19}	0.2007
α_{14}, α_{15}, α_{16}, α_{17}	0.1943
α_{26}, α_{27}, α_{28}, α_{29}, α_{30}, α_{31}	1.