

Chains of Cyclic Codes, Construction X and Incremental Redundancy

C. Tjhai, M. Tomlinson

Fixed and Mobile Communications Research
University of Plymouth
Plymouth, PL4 8AA, United Kingdom
{ctjhai,mtomlinson}@plymouth.ac.uk

M. Grassl

Institute for Quantum Optics and Quantum Information
Austrian Academy of Sciences
Technikerstraße 21a, 6020 Innsbruck, Austria
{markus.grassl}@oeaw.ac.at

*Accepted for publication at IEEE Information Theory
Workshop 2008 Porto, Portugal*

Abstract

It is shown that chains of cyclic codes in conjunction with Constructions X and XX can be used to efficiently construct sequences of linear codes for application in incremental redundancy communications. In addition to using a CRC for error detection, a novel CRC-less approach to error detection, which is based on the confidence level of the soft decision decoding output, is introduced. This novel approach provides an attractive trade-off between error rate performance and throughput for incremental redundancy communications.

1 Introduction

Incremental redundancy is a form of automatic-repeat-request (ARQ) which employs two levels of error protection. The first level is error correction, which uses error correcting codes to correct any error in both the user data and its checksum. The second level is error detection or a checksum, which checks for the presence of errors in user data and typically a cyclic-redundancy-check (CRC) code is employed for this purpose. The incremental redundancy ARQ system, abbreviated as IR-ARQ, initially attempts to correct errors in the user data and the checksum. It then verifies the checksum; if no error is detected, an acknowledgement (ACK) is fed back to the transmitter to indicate a successful transmission; otherwise, a negative acknowledgement (NACK) is returned to request for transmission

of some new parity check symbols, which will then be used for error correction. The process continues until no error is detected or the maximum number of transmissions is reached.

The idea of incremental redundancy dates back to the work of Davida and Reddy [1] and that of Mandelbaum [2]. A historical overview of the development of this type of retransmission scheme, which is also known as the type-II hybrid ARQ (HARQ), is given in [3]. Since the discovery of turbo codes and the rediscovery of low-density parity-check (LDPC) codes, there is a growing interest in IR-ARQ schemes using iteratively-decodable codes [4, 5, 6, 7]. These codes form a class of low-decoding complexity codes which, in general, have relatively poor minimum distance. The performance gain of this class of codes comes from their large block length and hence, they are not suitable for short packet applications. For many applications, wireless in particular, short packets are required and algebraic codes such as extended BCH and cyclic codes are attractive in this case.

It is known in the literature that cyclic codes are linear codes that, in general, have large minimum distance. It is possible to lengthen these cyclic codes to produce more good linear codes using Constructions X [8] and XX [9]. Many linear codes of the highest minimum distance for given length and dimension are cyclic codes or their lengthened codes and this is evident from [10]. In this paper, we apply cyclic codes and Constructions X and XX to produce sequences of codes ideally suited for IR-ARQ communications and also introduce a novel approach for IR-ARQ using error detection without using a CRC.

2 Incremental Redundancy Codes

Incremental redundancy codes have the property that all symbols of the higher-rate code are part of the lower-rate code. There are two approaches to construct codes with this property. The most commonly used approach is to use a good low-rate code, which is then successively punctured to produce higher-rate codes. Iteratively-decodable codes for incremental redundancy are constructed in this manner [4, 5, 7]. and so are the codes that appeared in [1, 2]. Using this approach, the minimum distance of the punctured code can collapse unless there is a proper selection of puncturing patterns and to determine good puncturing patterns is non-trivial. A second approach is to start with a good high-rate code and successively add parity check symbols to produce longer lower-rate codes with higher minimum distance. Some of the codes obtained from this approach include the codes introduced by Krishna and Morgera [11], the short codes of optimal weight structure from a computer search carried out by Cygan and Offer [12], and the $(u|u+v)$ construction of Reed-Muller codes [13]. In this paper, we show another method of constructing incremental redundancy codes based on the approach starting from high-rate codes. It is worth mentioning that the type-I HARQ described in this paper is different to that introduced in [14] where two codes, a half-rate invertible code and an error detecting code, were employed.

Let C be an $[n, k, d]$ linear code over \mathbb{F}_2 where n , k , and d denote the length, dimension, and minimum Hamming distance of the code respectively. In incremental redundancy with M transmissions, the prop-

erty of an $[n, k, d]$ incremental redundancy code \mathcal{C} implies that its codeword $c \in \mathcal{C}$ can be partitioned into M subblocks of codeword, i.e. $c = (u|p^{(1)}|p^{(2)}|\dots|p^{(M)})$, where $c^{(1)} = (u|p^{(1)}) \in \mathcal{C}^{(1)}$, $c^{(2)} = (c^{(1)}|p^{(2)}) \in \mathcal{C}^{(2)}$, \dots , $c = c^{(M)} = (c^{(M-1)}|p^{(M)}) \in \mathcal{C}^{(M)} = \mathcal{C}$. Here u denotes the information block of length k , $p^{(i)}$ denotes the i th parity block of length r_i and $\mathcal{C}^{(i)}$ denotes an $[n_i = k + \sum_{j=1}^i r_j, k, d_i]$ code. It is desirable to have $d_i > d_{i-1}$ for $2 \leq i \leq M$. However, it is not trivial to append parity symbols to increase the minimum distance while maintaining high code-rate of the overall code. Nonetheless, this can be neatly achieved, as shown in Section 3, by applying Constructions X and XX to a chain of cyclic codes.

3 Juxtaposition Codes: Chain of Cyclic Codes with Constructions X and XX

If \mathcal{C} is a cyclic code, there exists a generator polynomial $g(x) \in \mathbb{F}_2[x]$ and a check polynomial $h(x) \in \mathbb{F}_2[x]$ such that $g(x)h(x) = x^n - 1$. Two cyclic codes, \mathcal{C}_1 with $g_1(x)$ as the generator polynomial and \mathcal{C}_2 with $g_2(x)$ as the generator polynomial, are said to be chained or nested, if $g_1(x)|g_2(x)$, and we denote them by $\mathcal{C}_1 \supset \mathcal{C}_2$. With reference to this definition, it is clear that narrow-sense BCH codes of the same length form a chain of cyclic codes.

Let $G = [I | -R]$ be an $k \times n$ reduced-echelon generator matrix of a cyclic code with generator polynomial $g(x)$, the i th row of G is $[x^k(x^{n-k-i+1} - r_{n-k-i+1}(x))]$ where $r_j(x) = x^j \bmod g(x)$.

3.1 Lemma. Consider a chain of cyclic codes, $\mathcal{C}_1 \supset \mathcal{C}_2$, where $g_1(x) = f_1(x)$ and $g_2(x) = f_1(x)f_2(x)$, the reduced-echelon generator matrices of these cyclic codes can be written as

$$G_1 = \left(\begin{array}{c|c} I_{k_2} & \begin{array}{c} -r_{2,n-k_2}(x) \\ \vdots \\ -r_{2,n-1}(x) \end{array} \\ \hline 0 & \begin{array}{c} I_{k_1-k_2} \\ \vdots \\ -r_{1,n-1}(x) \end{array} \end{array} \right) \Bigg\} G_2$$

where G_i is the reduced-echelon generator matrix of \mathcal{C}_i , I_k is a $k \times k$ identity matrix and $r_{i,j}(x) = x^j \bmod g_i(x)$.

Proof. It is obvious that the first k_2 rows of G_1 is G_2 . We need to prove that the polynomials formed by the last $k_1 - k_2$ rows of G_1 do not contain $f_2(x)$, where $\deg(f_2(x)) = k_1 - k_2$, as a factor. From the $(k_2 + i + 1)$ th row of G_1 , for $0 \leq i \leq k_1 - k_2 - 1$, we have $u_i(x) = (x^{k_2+i} - x^{k_1}r_{1,n-k_1+k_2+i}(x))/f_1(x)$. For $0 \leq i \leq k_1 - k_2 - 1$, the numerator has degree at most $n - k_2 - 1$ and $\deg(f_1(x)) = n - k_1$, so the maximum degree of $u_i(x)$ is $k_1 - k_2 - 1$ and therefore, $f_2(x) \nmid u_i(x)$ since $\deg(f_2(x)) = k_1 - k_2$. ■

Given a chain of two codes, using Construction X [8], the code with larger dimension can be lengthened to produce a code with increased length

and minimum distance. We give a generalised Construction X which involves more than two codes in the following theorem, see also [15].

3.1 Theorem. Let \mathcal{B}_i be an $[n, k_i, d_i]$ code, given a chain of M codes, $\mathcal{B}_1 \supset \mathcal{B}_2 \supset \dots \supset \mathcal{B}_M$, and a set of auxiliary codes $\mathcal{A}_i = [n'_i, k'_i, d'_i]$, for $1 \leq i \leq M-1$, where $k'_i = k_1 - k_i$, a code $\mathcal{C}_X = [n + \sum_{i=1}^{M-1} n'_i, k_1, d]$ code can be constructed, where $d = \min\{d_M, d_{M-1} + d'_{M-1}, d_{M-2} + d'_{M-2} + d'_{M-1}, \dots, d_1 + \sum_{i=1}^{M-1} d'_i\}$.

From Theorem 3.1, we have the following corollary.

3.1 Corollary. Let v be a vector of length n formed by the first n coordinates of a codeword of \mathcal{C}_X . A codeword of \mathcal{C}_X is a juxtaposition of codewords of \mathcal{B}_i and \mathcal{A}_i , where

$$\begin{array}{l} \left(\begin{array}{c|c|c|c|c|c} b_M & 0 & 0 & \dots & 0 & 0 \end{array} \right) & \text{if } v \in \mathcal{B}_M, \\ \left(\begin{array}{c|c|c|c|c|c} b_{M-1} & 0 & 0 & \dots & 0 & a_{M-1} \end{array} \right) & \text{if } v \in \mathcal{B}_{M-1}, \\ & \vdots & & & & \vdots \\ \left(\begin{array}{c|c|c|c|c|c} b_2 & 0 & a_2 & \dots & a_{M-2} & a_{M-1} \end{array} \right) & \text{if } v \in \mathcal{B}_2, \\ \left(\begin{array}{c|c|c|c|c|c} b_1 & a_1 & a_2 & \dots & a_{M-2} & a_{M-1} \end{array} \right) & \text{if } v \in \mathcal{B}_1. \end{array}$$

Here, we denote $b_i \in \mathcal{B}_i$ and $a_i \in \mathcal{A}_i$.

Another lengthening method is Construction XX, which uses a lattice of four codes and makes use of Construction X twice. This construction was introduced in [9] and is restated in the following theorem.

3.2 Theorem. Consider three linear codes of the same length, $\mathcal{B}_1 = [n, k_1, d_1]$, $\mathcal{B}_2 = [n, k_2, d_2]$ and $\mathcal{B}_3 = [n, k_3, d_3]$ where $\mathcal{B}_2 \subset \mathcal{B}_1$ and $\mathcal{B}_3 \subset \mathcal{B}_1$. Let \mathcal{B}_4 be an $[n, k_4, d_4]$ linear code which is the intersection code of \mathcal{B}_2 and \mathcal{B}_3 , i.e. $\mathcal{B}_4 = \mathcal{B}_2 \cap \mathcal{B}_3$. Using auxiliary codes $\mathcal{A}_1 = [n_1, k_1 - k_2, d'_1]$ and $\mathcal{A}_2 = [n_2, k_1 - k_3, d'_2]$, there exists an $[n + n_1 + n_2, k_1, d]$ linear code \mathcal{C}_{XX} where $d = \min\{d_4, d_3 + d'_1, d_2 + d'_2, d_1 + d'_1 + d'_2\}$.

3.2 Corollary. Let v be a vector of length n formed by the first n coordinates of a codeword of \mathcal{C}_{XX} . A codeword of \mathcal{C}_{XX} is a juxtaposition of codewords of \mathcal{B}_i and \mathcal{A}_i , where

$$\begin{array}{l} \left(\begin{array}{c|c|c} b_4 & 0 & 0 \end{array} \right) & \text{if } v \in \mathcal{B}_4, \\ \left(\begin{array}{c|c|c} b_3 & a_1 & 0 \end{array} \right) & \text{if } v \in \mathcal{B}_3, \\ \left(\begin{array}{c|c|c} b_2 & 0 & a_2 \end{array} \right) & \text{if } v \in \mathcal{B}_2, \\ \left(\begin{array}{c|c|c} b_1 & a_1 & a_2 \end{array} \right) & \text{if } v \in \mathcal{B}_1. \end{array}$$

From Corollaries 3.1 and 3.2, if we let $b_j = (u)p^{(1)}$ and $a_i = (p^{(i+1)})$ for some positive integers j and i , it is obvious that the codes obtained from Constructions X and XX follow the property of incremental redundancy codes. Cyclic codes of length n , with appropriate arrangement of their zeros, can be put in chain form and hence, they are good candidate

linear codes for Constructions X and XX. It is known from the literature that a cyclic code can have the highest minimum distance attainable by any $[n, k]$ linear code. Due to their nested structure, it is possible to extend cyclic codes using Construction X or XX to produce more codes which have the highest minimum distance, see [15, 16, 17, 18] as examples. We also know that narrow-sense BCH codes are nested and so are the extended codes.

Example 3.1: Consider the following chain of extended BCH codes of length 128, $[128, 113, 6] \supset [128, 92, 12] \supset [128, 78, 16] \supset [128, 71, 20]$. Applying Construction X to $[128, 113, 6] \supset [128, 92, 12]$ with an $[32, 21, 6]$ extended BCH code as auxiliary code, a $[160, 113, 12]$ code is obtained and we now have

$$[160, 113, 12] \supset [160, 92, 12] \supset [160, 78, 16] \supset [160, 71, 20].$$

Using a $[42, 35, 4]$ shortened extended Hamming code as the auxiliary code in applying Construction X to $[160, 113, 12] \supset [160, 78, 16]$, we have

$$[202, 113, 16] \supset [202, 92, 16] \supset [202, 78, 16] \supset [202, 71, 20].$$

Finally, applying Construction X to $[202, 113, 16] \supset [202, 71, 20]$ with the shortened extended Hamming code $[49, 42, 4]$ as the auxiliary code, we obtain

$$[251, 113, 20] \supset [251, 92, 20] \supset [251, 78, 20] \supset [251, 71, 20].$$

The resulting sequence of codes for IR-ARQ is $[128, 113, 6]$, $[160, 113, 12]$, $[202, 113, 16]$ and $[251, 113, 20]$.

Example 3.2: Refining the chain of extended BCH codes from Example 3.1, a lattice of extended cyclic codes shown in Fig. 1 can be constructed, where α is a primitive n th root of unity.

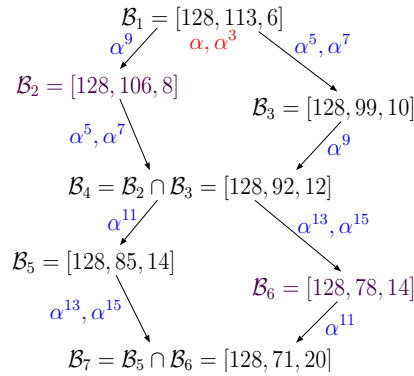


FIGURE 1: Lattice of extended cyclic codes. Note that α^j next to the arrow is a representative root added to a BCH code. All codes, except B_2 and B_6 , are extended BCH codes.

Incremental
redundancy
codes with
Construction
X

Incremental
redundancy
codes with
Construction
XX

Applying Construction XX to the lattice of \mathcal{B}_1 , \mathcal{B}_2 , \mathcal{B}_3 and \mathcal{B}_4 with auxiliary codes $\mathcal{A}_1 = [8, 7, 2]$ (single parity-check code) and $\mathcal{A}_2 = [20, 14, 4]$ (shortened extended Hamming code), we have the following chains

$$\begin{aligned} & [136, 113, 8] \supset [136, 92, 12] \supset [136, 78, 14] \supset [136, 71, 20], \\ & [156, 113, 12] \supset [156, 92, 12] \supset [156, 78, 14] \supset [156, 71, 20]. \end{aligned}$$

Using $\mathcal{A}_3 = [40, 28, 6]$ and $\mathcal{A}_4 = [47, 35, 6]$ (best known linear codes from [10]) as the auxiliary codes in applying Construction XX to the lattice of codes $[156, 113, 12] \supset [156, 85, 14]$ and $[156, 113, 12] \supset [156, 78, 14]$, where the subcodes are obtained by padding zeros to the codes \mathcal{B}_6 and \mathcal{B}_5 , we arrive at

$$\begin{aligned} & [196, 113, 14] \supset [196, 92, 14] \supset [196, 78, 14] \supset [196, 71, 20], \\ & [243, 113, 20] \supset [243, 92, 20] \supset [243, 78, 20] \supset [243, 71, 20]. \end{aligned}$$

The resulting the sequence of codes for IR-ARQ is $[128, 113, 6]$, $[136, 113, 8]$, $[156, 113, 12]$, $[196, 113, 14]$ and $[243, 113, 20]$.

$$G = \left(\begin{array}{c|c|c|c|c|c|c} I_{71} & & -R_5 & & 0 & 0 & 0 & 0 \\ \hline & I_{14} & & -R_4 & & & & \\ & & I_7 & & -R_3 & & & \\ 0 & & & I_{14} & & -R_2 & & \\ & & & & I_7 & & -R_1 & \\ \hline & & & & & G_{\mathcal{A}_1} & & \\ & & & & & & \tilde{G}_{\mathcal{A}_2} & \\ & & & & & & & G_{\mathcal{A}_3} \\ & & & & & & & & \tilde{G}_{\mathcal{A}_4} \end{array} \right) \quad (1)$$

The generator matrix of the $[243, 113, 20]$ code can be written in a form given by (1). On the left hand side of the double bar, we decompose the generator matrix of the code \mathcal{B}_1 along the chain $\mathcal{B}_1 \supset \mathcal{B}_2 \supset \mathcal{B}_4 \supset \mathcal{B}_5 \supset \mathcal{B}_7$ (see Lemma 3.1). The matrices $G_{\mathcal{A}_i}$ and $\tilde{G}_{\mathcal{A}_i}$ generate the corresponding auxiliary codes \mathcal{A}_i , where as an effect of Construction XX, the matrices $\tilde{G}_{\mathcal{A}_i}$ do not have full rank.

4 IR-ARQ Protocols, Error Detection Mechanisms and their Performance Analysis

The operation of an IR-ARQ scheme with M maximum transmissions can be described as follows. For the first transmission, we send a codeword of $\mathcal{C}^{(1)}$, and for the i th transmission, $2 \leq i \leq M$, we send parity checks $p^{(i)}$ such that the overall concatenated codeword is an element of $\mathcal{C}^{(i)}$. An IR-ARQ scheme requires a mechanism of error detection so that either ACK or NACK can be used to provide feedback to the transmitter. An ACK signal is fed back to the transmitter to indicate a successful decoding and no further parity-checks are required, whereas a NACK signal is sent to request for transmission of more parity-checks

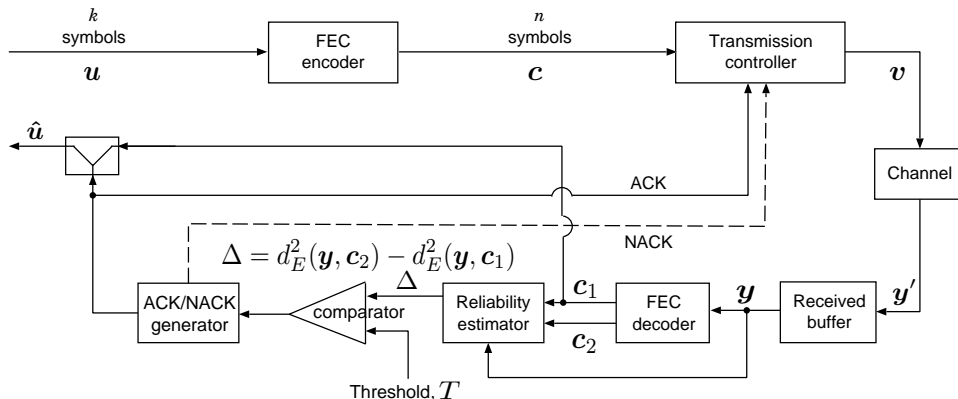


FIGURE 2: IR-ARQ using the confidence of FEC output

In the following subsections, two approaches to error detection are discussed and for analytical purposes, it is assumed that binary antipodal signalling, which maps coordinates of $\mathbf{c}^{(i)} = (c_0^{(i)}, c_1^{(i)}, \dots, c_{n_i-1}^{(i)}) \in \mathcal{C}^{(i)}$ to the real coordinate space \mathbb{R}^{n_i} , is employed. The antipodal mapping function is defined as $\psi(c^{(i)}) = 2c^{(i)} - 1$. Furthermore, we assume an additive-white-Gaussian-noise (AWGN) channel.

4.1 Error Detection based on Cyclic-Redundancy-Check

The cyclic-redundancy-check (CRC) is the simplest and the most commonly used mechanism for error detection in IR-ARQ schemes. For an $(k - m)$ bit CRC, m bits of user information u are CRC encoded to produce a vector x of length k bits, which is then passed to the forward-error-correction (FEC) encoder. At the decoding end at the i th transmission, the output of an FEC decoder $\hat{c}^{(i)}$ is passed to a CRC decoder. If no error is detected, an ACK is transmitted; otherwise a NACK is transmitted.

The length of the CRC provides a trade-off between throughput and the error probability. A short CRC increases throughput, but the undetected error probability increases and results in an early error-floor which dominates the frame-error-rate (FER) of the system.

4.2 Error Detection based on the Confidence of FEC Output

Error detection can also be reliably achieved by considering the output of an FEC decoder which, in this case, has to be a soft-decision list decoder. This CRC-less approach to error detection, whose block diagram is given in Fig. 2, can be described as follows.

Let the squared Euclidean distance between the received vector $\mathbf{y}^{(i)} \in \mathbb{R}^{n_i}$ and a codeword $\mathbf{c}^{(i)} \in \mathcal{C}^{(i)}$, be defined as

$$d_E^2(\mathbf{y}^{(i)}, \psi(\mathbf{c}^{(i)})) = \frac{1}{n_i} \sum_{j=0}^{n_i-1} (y_j^{(i)} - \psi(c_j^{(i)}))^2.$$

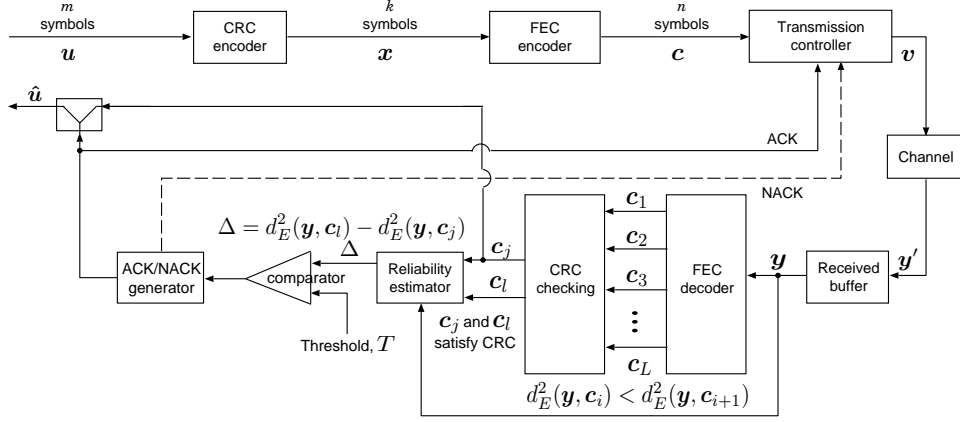


FIGURE 3: IR-ARQ using the confidence of FEC output and CRC

Given the transmitted codeword $\mathbf{c}^{(i)} \in \mathcal{C}^{(i)}$, the most likely codewords $\hat{\mathbf{c}}^{(i)} \in \mathcal{C}^{(i)}$ and the next most likely codeword $\bar{\mathbf{c}}^{(i)} \in \mathcal{C}^{(i)}$ at the i th transmission, the confidence of FEC output at the i th transmission is defined as

$$\Delta^{(i)} = d_E^2(\mathbf{y}^{(i)}, \psi(\hat{\mathbf{c}}^{(i)})) - d_E^2(\mathbf{y}^{(i)}, \psi(\bar{\mathbf{c}}^{(i)})).$$

Defining $\mathbf{v}^{(i)} = \psi(\mathbf{c}^{(i)})$, $\Delta^{(i)}$ can be expressed as

$$\Delta^{(i)} = \frac{2}{n_i} \sum_{j=0}^{n_i-1} y_j^{(i)} (\bar{v}_j^{(i)} - \hat{v}_j^{(i)}).$$

Since, for some integer j , $y_j^{(i)} = v_j^{(i)} + \bar{n}_j^{(i)}$ and $\hat{y}_j^{(i)} = \psi(c_j^{(i)} + e_j^{(i)}) = v_j^{(i)} + 2e_j^{(i)}$, where $\mathbf{e}^{(i)} = (\mathbf{c}^{(i)} + \hat{\mathbf{c}}^{(i)}) \in \mathcal{C}^{(i)}$ and $\bar{n}_j^{(i)}$ is the Gaussian noise at the j position,

$$\Delta^{(i)} = \frac{2}{n_i} \left\{ \left(\sum_{j=0}^{n_i-1} v_j^{(i)} \bar{v}_j^{(i)} \right) + \left(\sum_{j=0}^{n_i-1} \bar{n}_j^{(i)} (\bar{v}_j^{(i)} - v_j^{(i)}) \right) - n_i \right\} - \frac{2}{n_i} \left\{ \left(\sum_{j=0}^{n_i-1} 2e_j^{(i)} (v_j^{(i)} + \bar{n}_j^{(i)}) \right) \right\}$$

Let $\bar{\mathbf{e}}^{(i)} = \mathbf{c}^{(i)} - \bar{\mathbf{c}}^{(i)}$ and $\bar{w}_i = |\text{sup}(\mathbf{e}^{(i)})|$, $\Delta^{(i)}$ becomes

$$\Delta^{(i)} = -\frac{4}{n_i} \left(\bar{w}_i - \sum_{j \in \text{sup}(\bar{\mathbf{e}}^{(i)})} \pm \bar{n}_j^{(i)} \right) - \frac{4}{n_i} \left(\sum_{j \in \text{sup}(\mathbf{e}^{(i)})} (v_j^{(i)} + \bar{n}_j^{(i)}) \right). \quad (2)$$

Without loss of generality, assume that $\mathbf{c}^{(i)} = (\mathbf{0})^{n_i}$ (all zeros codeword of length n_i) and $\mathbf{c}^{(i)} = \hat{\mathbf{c}}^{(i)}$, we have $\mathbf{e}^{(i)} = (\mathbf{0})^{n_i}$ and (2) simplifies to

$$\Delta_c^{(i)} = -\frac{4}{n_i} \left(\bar{w}_i - \sum_{j \in \text{sup}(\bar{\mathbf{e}}^{(i)})} \bar{n}_j^{(i)} \right). \quad (3)$$

On the other hand, if $\hat{c}^{(i)} \neq c^{(i)}$, equation (2) now becomes

$$\Delta_e^{(i)} = \underbrace{-\frac{4}{n_i} \left(\bar{w}_i - \sum_{j \in \text{sup}(\bar{e}^{(i)})} \bar{n}_j^{(i)} \right)}_{\Delta_1} + \underbrace{\frac{4}{n_i} \left(\hat{w}_i - \sum_{j \in \text{sup}(e^{(i)})} \bar{n}_j^{(i)} \right)}_{\Delta_2} \quad (4)$$

where $\hat{w}_i = |\text{sup}(e^{(i)})|$.

4.1 Lemma. The first and second terms, Δ_1 and Δ_2 respectively, of (4) satisfy the inequalities $\Delta_1 \geq 0$ and $|\Delta_2| > |\Delta_1|$.

Proof. The proof is obvious since $d_E^2(\mathbf{y}^{(i)}, \bar{v}^{(i)}) \leq d_E^2(\mathbf{y}^{(i)}, \mathbf{v}^{(i)})$ and $\Delta_e^{(i)} < 0$. ■

Since $|\Delta_2| > |\Delta_1|$, on average, it is more likely that $\Delta_e^{(i)}$ is close to zero and $|\Delta_c^{(i)}| > |\Delta_e^{(i)}|$. In order to accept codewords of high confidence level only, a threshold T_i on $|\Delta^{(i)}|$ is employed and at the i th transmission, the threshold is set to $T_i = 4\kappa/n_i$ for some constant $\kappa \in \mathbb{R}$. Using the threshold T_i , if $|\Delta^{(i)}| > T_i$, we accept $\hat{c}^{(i)}$ as the correct output and transmit an ACK; otherwise a NACK is transmitted. Clearly, the threshold T_i provides a trade-off between the throughput and the error probability. The higher the threshold T_i , the lower the probability of error and, consequently, the lower the throughput of the system.

An undetected error occurs if $|d_E^2(\mathbf{y}^{(i)}, \psi(\hat{c}^{(i)}) - d_E^2(\mathbf{y}^{(i)}, \psi(\bar{c}^{(i)}))| > T_i$ and $\hat{c}^{(i)} \neq c^{(i)}$. While we can reduce the number of undetected errors by simply increasing T_i , many correct decisions will also be discarded. A preferred alternative approach is to employ a CRC as well to obtain an overall more reliable estimate for threshold comparison. The block diagram of this hybrid approach is depicted in Fig. 3. As shown in the figure, the FEC decoder produces L most-likely codewords, but only a subset of these L codewords will satisfy the CRC. The squared Euclidean distance, with respect to the received vector \mathbf{y} , of the first two most-likely codewords that satisfy CRC are used to generate either ACK or NACK.

5 Numerical Results

Computer simulations using the sequence of codes given in Example 3.2 have been carried using an ordered reliability decoder [19, 20, 21], which has quasi maximum-likelihood performance, when configured as a list decoder using 10^6 codewords and hard and soft decision outputs. The 8-bit CRC employed is defined by the polynomial $(1+x)(1+x^2+x^5+x^6+x^7)$. The protocol assumes that an ACK is transmitted if no error is detected or the maximum number of transmissions has been reached; and a NACK is transmitted otherwise.

From Fig. 4 and 5, it can be seen that the conventional CRC approach shows good throughput, but exhibits an early error floor of the FER which is due to undetected error events. By using the thresholding method, the FER improves considerably, especially for larger κ . The thresholding approach

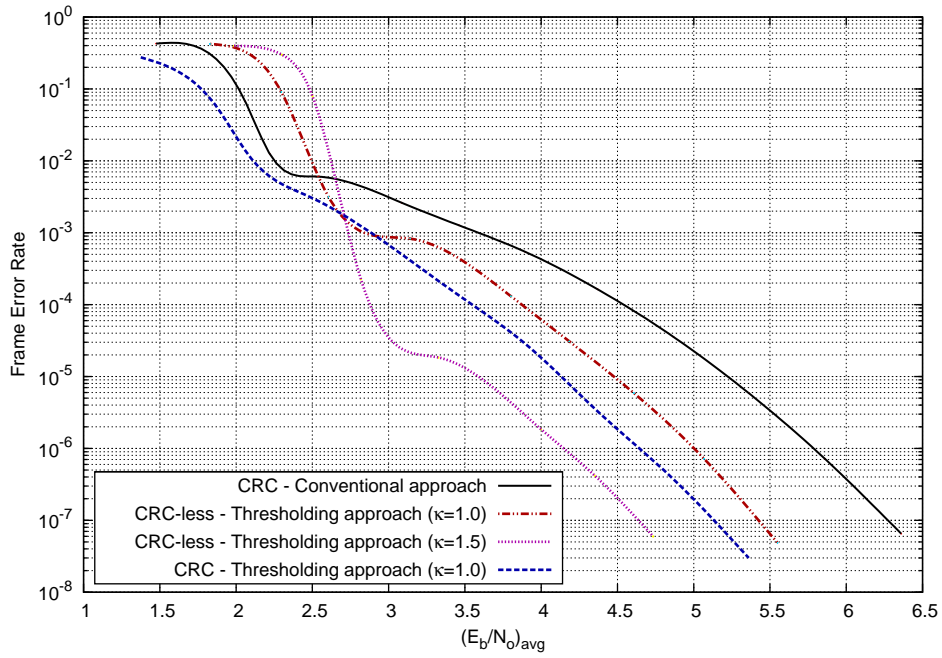


FIGURE 4: FER performance of the IR-ARQ scheme based on extended BCH codes of length 128

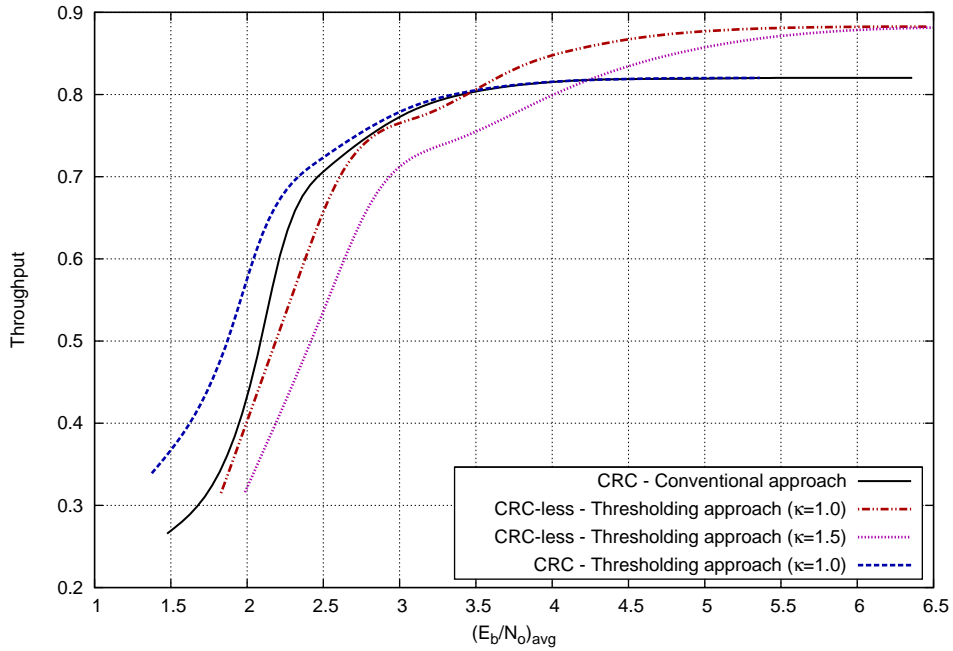


FIGURE 5: Average code-rate and throughput of the IR-ARQ scheme based on extended BCH codes of length 128

provides an attractive trade-off between throughput and performance. The throughput is upper-bounded by the largest code-rate of the code in the sequence and, in this respect, CRC-less approach is clearly more attractive especially in the high SNR region. Fig. 4 and 5 also show that the hybrid approach has better overall FER and throughput performance than the conventional approach.

It is worth mentioning that, although we take examples from algebraic codes, the CRC-less error detection proposed in this paper can be applied to any type of code [22], regardless of the length, provided a list decoder is used with soft-decision output. Future work will explore alternative code constructions and the possible benefits of adaptive variation of the confidence level factor κ .

References

- [1] G. Davida and S. Reddy, "Forward-error correction with decision feedback," *Inform. Contr.*, vol. 21, pp. 117–133, 1972. (Cited on page 2.)
- [2] D. Mandelbaum, "An adaptive-feedback coding scheme using incremental redundancy," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 388–389, May 1974. (Cited on page 2.)
- [3] S. Lin and D. J. Costello, Jr., *Error Control Coding: Fundamentals and Applications*. Pearson Education, Inc, 2nd ed., 2004. (Cited on page 2.)
- [4] K. Narayanan and G. Stuber, "A novel ARQ technique using the turbo coding principle," *IEEE Commun. Lett.*, vol. 1, pp. 49–51, Mar. 1997. (Cited on page 2.)
- [5] R. Liu, P. Spasojević, and E. Soljanin, "Punctured turbo code ensembles," in *Proc. IEEE Information Theory Workshop*, (Paris, France), pp. 249–252, 31 Mar–4 Apr 2003. (Cited on page 2.)
- [6] S. Sesia, G. Caire, and G. Vivier, "Incremental redundancy hybrid ARQ schemes based on low-density parity-check codes," *IEEE Trans. Commun.*, vol. 52, pp. 1311–1321, Aug. 2004. (Cited on page 2.)
- [7] E. Soljanin, N. Varnica, and P. Whiting, "Punctured vs rateless codes for hybrid ARQ," in *Proc. IEEE Information Theory Workshop*, (Punta del Este, Uruguay), 13–16 Mar. 2006. (Cited on page 2.)
- [8] N. J. Sloane, S. M. Reddy, and C. L. Chen, "New binary codes," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 503–510, July 1972. (Cited on pages 2 and 3.)
- [9] W. O. Alltop, "A Method of Extending Binary Linear Codes," *IEEE Trans. Inform. Theory*, vol. 30, pp. 871–872, Nov. 1984. (Cited on pages 2 and 4.)
- [10] M. Grassl, "Code Tables: Bounds on the parameters of various types of codes," 2007. <http://www.codetables.de>. (Cited on pages 2 and 6.)

- [11] H. Krishna and S. Morgera, "A new error control scheme for hybrid ARQ systems," *IEEE Trans. Commun.*, vol. 35, pp. 981–990, Oct. 1987. (Cited on page 2.)
- [12] D. Cygan and E. Offer, "Short linear incremental redundancy codes having optimal weight structure profile," *IEEE Trans. Inform. Theory*, vol. 37, pp. 192–195, Jan. 1991. (Cited on page 2.)
- [13] S. Wicker and M. Bartz, "The design and implementation of Type-I and Type-II hybrid-ARQ protocols based on first-order Reed-Muller codes," *IEEE Trans. Commun.*, vol. 42, pp. 979–987, Feb./Mar./Apr. 1994. (Cited on page 2.)
- [14] S. Lin and P. S. Yu, "A hybrid arq scheme with parity retransmission for error control of satellite channels," *IEEE Trans. Commun.*, vol. 30, pp. 1701–1719, July 1982. (Cited on page 2.)
- [15] J. Bierbrauer and Y. Edel, "Extending and Lengthening BCH-codes," *Finite Fields and Their Applications*, vol. 3, pp. 314–333, 1997. (Cited on pages 4 and 5.)
- [16] M. Grassl, "New binary codes from a chain of cyclic codes," *IEEE Trans. Inform. Theory*, vol. 47, pp. 1178–1181, March 2001. (Cited on page 5.)
- [17] C. Tjhai, M. Tomlinson, M. Grassl, R. Horan, M. Ahmed, and M. Ambroze, "New linear codes derived from cyclic codes of length 151," *IEE Proc., Commun.*, vol. 153, pp. 581–585, Oct. 2006. (Cited on page 5.)
- [18] C. Tjhai and M. Tomlinson, "Results on binary cyclic codes," *Electron. Lett.*, vol. 43, pp. 234–235, Feb. 2007. (Cited on page 5.)
- [19] B. G. Dorsch, "A decoding algorithm for binary block codes and J -ary output channels," *IEEE Trans. Inform. Theory*, vol. 20, pp. 391–394, May 1974. (Cited on page 9.)
- [20] M. Fossorier and S. Lin, "Soft-decision decoding of linear block codes based on ordered statistics," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1379–1396, Sep. 1995. (Cited on page 9.)
- [21] M. Tomlinson, C. Tjhai, and M. Ambroze, "Extending the dorsch decoder towards achieving maximum likelihood decoding for linear codes," *IET Proc., Commun.*, vol. 1, pp. 479–488, Jun. 2007. (Cited on page 9.)
- [22] M. Tomlinson and C. Tjhai, "Incremental redundancy coding system." US Patent Application 11/751313, 2007. (Cited on page 11.)