A Class of High-Rate Double-Error-Correcting Convolutional Codes

Sudhakar M. Reddy, George I. Davida, and John P. Robinson

Department of Electrical Engineering, University of Iowa, Iowa City, Iowa 52240

A new class of double error correcting high rate convolutional codes are given. It is shown that these codes exhibit finite error propagation.

1. Introduction

A class of double error correcting linear convolutional codes are given. The codes are derived from double-error-correcting triple-error-detecting extended BCH codes. The codes being proposed are not covered by previous works ([7], [2], [3]). Error propagation in the proposed codes is discussed. For the sake of simplicity of arguments only binary codes are discussed. Extensions to nonbinary case is straightforward.

* The research reported in this paper is supported in part by a National Science Foundation grant GK-10025.

225
A convolutional code is defined as the linear vector space which is the null space of a semiinfinite parity check matrix [8]. The random error-correction capability of a convolutional code for feedback decoding can be investigated by analyzing the linear relationships among the columns of the finite matrix $A_N$, shown in Fig. 1.

Let $H_b$ (shown in Fig. 2) denote the parity check matrix of a linear block code of length $2^n$, $\alpha \geq 1$, where $\beta$ is a primitive element of $GF(2^n)$. The first $(\alpha + 1)$ rows of $H_b$ describe a linear code of minimum distance at least 4, and let us denote it by $H_1$, and the matrix formed by the remaining rows of $H_b$ by $H_2$ (for $\alpha = 1$, $H_2$ has no rows and for $\alpha = 2$, $H_2$ has one row, since repeated and all zeros rows are deleted). $H_b$, itself, describes a linear block code of minimum distance 6.

\[
H_b = \begin{bmatrix}
1 & 1 & \cdots & 1 & 1 \\
\beta & \beta^2 & \cdots & \beta^{n-1} & 0 \\
\beta^3 & \beta^6 & \cdots & \beta^{3(n-1)} & 0 \\
\end{bmatrix}
\]

Fig. 2. Parity check matrix of a $d_b = 6$ block code.

2. CONSTRUCTION

Let a convolutional code be described by the $B_0$ matrix of Fig. 3, where $H_3$ is obtained as follows. $H_1$ can be readily seen to be the parity check matrix of a $(\alpha - 1)$-th order Reed Muller code [1]. A specific representation of $H_1$ is given in Fig. 4. $H_3$ is formed by making its $i$-th row equal to the $(\alpha - i + 2)$-th row of $H_1$, $1 \leq i \leq \alpha - 1$. The $B_0$ matrix for $\alpha = 2$ is given in Fig. 5.

\[
B_0 = \begin{bmatrix}
H_1 \\
1 \cdot \cdots \cdot 1 \\
0 \cdot \cdots \cdot 0 \\
0 \cdot \cdots \cdot 0 \\
0 \cdot \cdots \cdot 0 \\
H_3 \\
H_2 \\
\end{bmatrix}
\]

Fig. 3. The null matrix of the codes being proposed.
The minimum distance of the codes described by $B_0$ matrix of Fig. 3 will now be proved to be equal to 5. The arguments given below effectively prove that there does not exist a linearly dependent set of four or less columns of the corresponding $A_N$ matrix, including at least one column from the first block of $A_N$. Next, a linear combination of five columns whose value is an all zeros column is exhibited. The possible linear combinations of four or less columns are divided into three cases. First, note that any all zeros linear combination including columns from the first block of $A_N$ must include an even number of columns from the first block since the first row of $B_0$ is all ones. Hence, we need to consider only the three cases given below:

![Fig. 4. A specific form of $H_1$.](image)

Case A. Two columns from the first block and two more columns from two other separate blocks.

![Fig. 5. The $B_0$ matrix for $\alpha = 2$.](image)
Case B. Two columns from the first block and two more columns from a separate but single block.

Case C. All four columns from the first block.

The case of $\alpha = 1$ is a special case ($n_A = 12$) and can be verified to have minimum distance 5 by exhaustive analysis. Proof in the case of $\alpha \geq 2$ follows.

**Theorem 2.1.** The linear convolutional code described above has minimum distance equal to 5, with code parameters $b = 2^{\alpha}, m = 1$, and $N_A = (5\alpha + 2)b$ for $\alpha > 2$, and $N_A = 44$ for $\alpha = 2$.

**Proof.** At least two columns from the first block have to be taken to obtain an all zeros column, that is, a linear combination of the columns of $A_N$ with nonempty choice from the first block. The first $(\alpha + 1)$ rows of $A_N$ form a single error correcting code of Wyner and Ash [8]. This implies that at least one more column must be chosen from the first through $(\alpha + 1)$-th block. If another column is chosen from the first block, then clearly a fourth column must also be chosen from the first block, but no four columns from the first block can sum to zero, because of $H_b$ (Case C).

If the third column is chosen from 2nd through $(\alpha + 1)$-th block, then one more column from 2nd through $(2\alpha + 1)$-th blocks must be chosen, because of the all ones $(\alpha + 2)$-th row of $B_0$ followed by $(2\alpha + 1)$ all zeros rows. If the choice of these two columns is from different blocks (Case A), then they introduce two 1's into different rows in the range $(\alpha + 1)$-th through $3(\alpha + 1)$-th rows of the vector formed by the linear combination of the above columns, because of the all zeros rows of $B_0$ $[(\alpha + 3)$-th through $3(\alpha + 1)$-th rows].

Therefore, the only other possibility to obtain an all zeros linear combination with at most 4 columns is to choose two columns from the first block and two columns from a single block in the range 2nd through $(\alpha + 1)$-th blocks (Case B). Even in this case, the linear combination cannot be all zeros within rows 2nd through $(\alpha + 1)$-th and rows $[3(\alpha + 1) + 1]$-th through $[3(\alpha + 1) + \alpha - 2]$-th, for $\alpha \geq 2$. The linear combination of the two columns chosen from the first block must not have a one in its second row, since then adding two more columns from a single block of the remaining blocks of $A_N$ cannot create a zero in this position. Furthermore, the ones and zeros in the 3rd through $(\alpha + 1)$-th rows of the sum of the two columns in the first block are recreated in the reverse order in the $[3(\alpha + 1) + \alpha - 1]$-th rows. If the last one in the 3rd through $(\alpha + 1)$-th row of the sum of the two columns of the first block is at $j$-th row $3 \leq j \leq \alpha + 1$, then the next
one is at \[3(\alpha + 1) + (\alpha + 1) - j + 1\]-th row. To create zeros in both these positions by adding two more columns from a single block in the range 2nd through \((\alpha + 1)\) blocks is not possible because of the need to create ones in the sum of these two columns at \(j\)-th position and \[3(\alpha + 1) + (\alpha + 1) - j + 1\]-th position without creating any ones in the intermediate rows.

The above analysis implies that there does not exist a linear combination of at most four columns with nonempty selection from the first block that is all zeros. It can be readily shown that some four columns from the first block and a column from the last \(\alpha\) blocks can be added to get an all zeros column, for \(\alpha \geq 2\).

3. Error Propagation

It can be readily shown that the proposed codes have minimum distance of 3 in the definite decoding mode [5]. If bounded distance decoding is used [7], then the decoder is guaranteed to return to correct operation from error propagation situation when a region of two constraint lengths less one block of error free region is encountered [5].

4. Remarks

Codes equivalent or some times better than the proposed codes can be constructed in terms of rate and decoding constraint length using earlier techniques ([7], [3]) but the block lengths of such codes are much larger. For example, when \(\alpha = 5\) the proposed code has block length 32, redundancy 1/32, and constraint length 864; while Wyner's [7] construction yields a code with block length 255, redundancy 8/255, and constraint length 765. One of the major advantages of convolutional codes is the feasibility of codes of given error correction ability at smaller block lengths. Codes with block lengths other than \(2^\alpha\) can be constructed using the arguments presented in the paper. Finally, it has been shown that the best possible minimum distance of linear convolutional code that has a single error-correcting code as a prefix and constraint length of the proposed codes is 7 [6]. It is our feeling that the best possible minimum distance is actually 6, if at all it is possible.

The codes can be put into canonical form without increasing the decoding
constraint length such that the minimum distance does not decrease. This can be proved by observing that the last column in each block can be made to correspond to a parity bit position for the canonical code.

The only other codes with the same \( b \) and \( m \) for which constructive procedures are known are the self-orthogonal codes [4]. The minimum decoding constraint length of such codes is \( [(2^\alpha - 1) 6 + 1]b \), which is considerably higher than that for the codes proposed. For example, when \( \alpha = 3 \), the proposed code has \( N_A = 136 \) and for self-orthogonal codes \( N_A \) is at least 344.

Received: May 19, 1969; revised: October 27, 1969

References