On the Design of Arbitrarily Low-Rate Turbo-Codes.

Miguel Griot, Andres I. Vila Casado and Richard Wesel
Dept. of Electrical Engineering, University of California, Los Angeles, CA, 90095
{mgriot,avila,wesel}@ee.ucla.edu

Abstract— **This paper presents a design criteria for arbitrarily low-rate parallel concatenated convolutional codes (PCCCs). The purpose of this work is to find a family of turbo codes that work as close to the ultimate low-rate Shannon limit $E_b/N_0 \simeq -1.59$ dB as possible, given a certain constraint in the number of states of the constituent trellis codes and in the interleaver-length. We propose an optimization criteria and reduce the turbo-design problem to the design of block codes for the assignment of output sequences to the trellis branches of the constituent encoders. We show that BCH codes concatenated with repetition codes are optimal for labeling. Moreover, we show that for a fixed number of trellis states these codes achieve arbitrarily low rates, and hence arbitrarily low SNRs, with practically the same performance in terms of E_b/N_0. Simulation results are shown for 8-state and 16-state turbo codes with rates as low as 1/505, which with an interleaver-length of 8192 provide a BER $\simeq 10^{-5}$ at an SNR $\simeq -27.6$ dB ($E_b/N_0 \simeq -0.55$ dB), around 1dB away from the ultimate low-rate Shannon limit.**

Index Terms— **Channel coding, error probability, turbo code, information rates, low-rates, low-SNR.**

I. Introduction

Low-rate codes are of theoretical interest when approaching the ultimate low-rate Shannon limit of $E_b/N_0 = \ln 2 \simeq -1.59$ dB. They also have important applications in spread-spectrum multiple-access channels, such as code-division multiple-access (CDMA) [1]. Other applications include interleave-division multiple-access (IDMA) [2] and the deep-space network that require operation at very low signal-to-noise ratios.

There have been many contributions to the problem of designing low-rate codes. Recent papers have shown that turbo-like codes can work near the ultimate low-rate Shannon limit. Super-orthogonal turbo-codes [3] combine the principle of low-rate convolutional coding [1] with parallel concatenation. In [3], a Hadamard matrix is used to generate the output sequences of each branch of the constituent trellis code. Therefore, the output sequences of branches leaving different states and produced by the same input are mutually orthogonal. Also, the output sequences of branches leaving the same state or merging into the same state are antipodal (see Fig. 1). With m-memory-element constituent codes, super-orthogonal turbo codes have a rate of $1/(2^m - 1)$.

More recently, low-rate turbo-Hadamard codes have been proposed in [2]. In that work, each constituent code consists of a serial concatenation of an $(r+1, r)$ parity-check code, a rate-1/2 recursive systematic convolutional code and a Hadamard code of length 2^r. These component codes are concatenated M times, resulting in a code-rate of $R = r/(r + M(2^r - r))$. The complexity of the code increases both with the number of constituent codes M and with length of the Hadamard code. In [2], a turbo-Hadamard code with $r = 7$ and $M = 3$ and an interleaver length of 65534 is reported to achieve a performance of BER$< 10^{-5}$ at an $E_b/N_0 = -1.2$ dB.

However, both works require increasing complexity as the rate of the codes decrease. Super-orthogonal codes need to increase the number of memory elements, and turbo-Hadamard codes must either increase the number of component codes or the Hadamard code size. This work is concerned with the design of constituent trellis codes given a fixed number of memory elements, for arbitrarily low-rates.

In [4] [5], the *effective free distance* of turbo codes was introduced and shown to have a strong influence in their performance. We propose to use a normalized notion of the effective free distance as an optimization criteria, that enables the comparison of codes with different rates. We present a family of turbo codes of rate $1/(r(2^m - 1) + 1)$, where m is the number of memory elements of the trellis code, and r is any integer. We use BCH codes to design the output sequences of the trellis transitions (or branches). Simulation results show that given a constraint in the number of memory elements and an interleaver length, the performance in terms of bit error rate vs. E_b/N_0 of these codes remains practically the same for any value of r.

Section II defines the general structure of the codes, and introduces a normalized notion of the effective free distance of turbo codes as an optimization criteria. Section III shows that optimality under this criteria is reached for a family of rates by using BCH codes to produce the output sequences. Section IV shows the performance of 8-state and 16-state turbo codes on the AWGN channel. Section V delivers the conclusions.

II. Code structure and optimization criteria

It is well-known that recursive (or feedback) constituent encoders outperform feed-forward constituent encoders in parallel concatenated codes [6]. The effective free distance of a constituent recursive convolutional code is defined as the minimum (Hamming) distance of error events produced by input sequences with Hamming distance equal to 2, which we will call weight-2 error events. A common

This work was supported by the Defence Advanced Research Project Agency under SPAWAR Systems Center San Diego Grant N66001-02-1-8938.

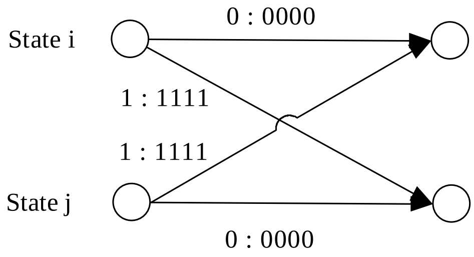

Fig. 1. Example of antipodal labeling of a group of two trellis states. Branches splitting from a state or merging into a state are the complement of each other.

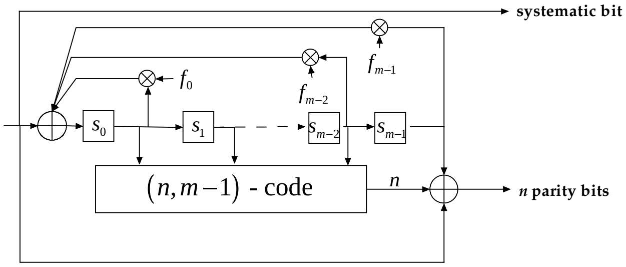

Fig. 2. General structure of 2^m-state rate $1/(n+1)$ systematic trellis code.

TABLE I

Feedback vectors $f_0, \cdots, f_{m-1}$ that maximize the minimum length of weight-2 error events, for different number of memory elements m

m	$f_0 \cdots f_{m-1}$
2	11
3	011
4	0011
5	00101

approach to the design of constituent codes is to maximize this parameter [4],[5]. Fig. 2 shows a rate $1/(n+1)$ systematic feedback encoder with m memory elements $\{s_0, \cdots, s_{m-1}\}$, where $f_0, \cdots, f_{m-1} \in \{0, 1\}$ represent the polynomial coefficients controlling the feedback into s_0.

For feedback encoders, in any trellis error event, two branches departing from a same state (i.e. a split) are produced by a different input, and any two branches merging into a state (i.e. a merge) are produced by a different input. Hence, weight-2 error events are produced by input sequences that differ in one symbol at the beginning of the error event (when the trellis paths split) and one symbol at the end of the error event (when the trellis paths merge), and are equal in every other trellis section. To maximize the effective free distance, such error events should traverse as many trellis sections as possible. For a given memory size m, and appropriately chosen $\{f_0, \cdots, f_{m-1}\}$, such error events can have a minimum length of 2^m trellis sections, including the split and the merge. For example, Table I shows feedback values that produce weight-2 error events of length 2^m for $m = 2, 3, 4, 5$. This is also an application of the well-known concept of maximal length shift registers.

Since every error event contains a split and a merge, we force the output sequences of branches splitting from a state or merging to a state to be the compliment of each other, as shown in Fig. 1. This same idea is used in super-orthogonal turbo codes [3]. Thus, only one output sequence and its complement are needed per two states of the trellis. As shown in Fig. 2 this can be done by forcing f_{m-1} to be 1, assigning an output sequence to each sub-set of two states defined by $\{s_0, \cdots, s_{m-2}\}$, and XORing the output with the input bit and s_{m-1}.

Given a certain number of parity bits n of the systematic trellis code, the output sequences of the 2^{m-1} pairs of states must be designed. Since the objective is to maximize the effective free distance, our goal is to maximize the minimum distance between the 2^{m-1} output labels, which not only maximizes the effective free distance but it also increases the distance spectrum of the code. This can be seen as the design of an $(n, m-1)$ block code maximizing its minimum distance $d_{\min}$. Using the structure of Fig. 2 and the feedback vectors of Table II, the resulting effective free distance $d_{\text{eff,free}}$ of the constituent code is lower bounded by

$$d_{\text{eff,free}} \geq (2^m - 2)d_{\min} + 2(n + 1). \tag{1}$$

As mentioned in Section I, the rate of the code is a parameter to be designed in order to provide the best possible performance in terms of BER vs. E_b/N_0. Considering a certain (n, k) code, on an AWGN channel the error probability is given by:

$$P_e \approx Q\left(\sqrt{2d_{\min}E_s/N_0}\right) = Q\left(\sqrt{2d_{\min}(k/n)E_b/N_0}\right), \tag{2}$$

where k/n is the rate of the code. Hence, the performance of the code is driven by the term $d_{\min} \cdot SNR = (k/n) \cdot d_{\min} \cdot E_b/N_0$.

We apply the same criteria to the distance between branches to make a fair comparison between constituent encoders of different rates. Therefore, we reduce the labeling design and the decision on the optimal rate of the turbo code to the following optimization problem: Given a fixed number of labels (or codewords) $M = 2^k$ (where $k = m-1$), find the number of parity bits n, and an (n, k) code that maximizes the normalized minimum distance $d_{\min}/n$.

III. Binary BCH codes for labeling

In this section we show that BCH codes with the appropriately chosen blocklength n are optimal under the criteria presented in Section II. We first introduce an upper bound to the normalized minimum distance in the following theorem:

Theorem III.1: Every (n, k) code must satisfy:

$$\frac{d_{\min}}{n} \leq \frac{2^{k-1}}{2^k - 1} \tag{3}$$

and equality holds if and only if for every pair of codewords (c_i, c_j)

$$d_H(c_i, c_j) = d_{\min}, \quad \forall i, j \in 0, \cdots, 2^k - 1. \tag{4}$$

Proof:

Consider any (n, k) code. Without loss of generality, suppose the all-zero word is a valid codeword, and denote it c_0. Suppose the code provides equally likely ones and zeros. Then the sum of the Hamming weights of all the codewords is half the number of codewords multiplied by their length

$$\sum_{i=0}^{2^k-1} W_H(c_i) = \frac{2^k \cdot n}{2} = 2^{k-1} \cdot n. \tag{5}$$

Now consider the sum of the Hamming distances between the all-zero codeword and the other 2^k-1 codewords. Using (5), and the fact that $W_H(c_0) = 0$, then

$$(2^k - 1)d_{\min} \leq \sum_{i=1}^{2^k-1} d_H(c_0, c_i) = 2^{k-1} \cdot n. \tag{6}$$

Rearranging terms in (6), we obtain (3). Also, from (6), equality holds only when $d_H(c_0, c_i) = d_{\min}$ for all $i = 1, \cdots, 2^k-1$. It is easy to see that with a proper transformation, any codeword can be the all-zero codeword in an equivalent code. Hence, equality holds if and only if (4) is satisfied.

If the codeword doesn't provide equally likely ones and zeros, we can assume without loss of generality that

$$\sum_{i=0}^{2^k-1} W_H(c_i) < 2^{k-1} \cdot n. \tag{7}$$

and the proof still holds. Moreover, equality on (3) can never be reached with unequal output probabilities.

We prove now that the bound on (3) can be achieved with equality if one chooses n as a multiple of $2^k - 1$, using binary BCH codes. First, we design a (n, k) binary BCH code with $n = 2^k-1$ as follows: Use the Galois Field GF(2) as the ground field and GF(2^k) as the extended field. There exists an order-k element α of GF(2^k). Denote as $M_\alpha(x)$ the minimal polynomial of α (a primitive polynomial) over GF(2), and define the generator polynomial of the BCH code as

$$g(x) = \frac{x^{2^k-1} - 1}{M_\alpha(x)}. \tag{8}$$

Since the degree of $M_\alpha(x)$ is k, the degree of $g(x)$ is $2^k - 1 - k$. Thus, this is a $(2^k - 1, k)$ binary BCH code.

Now,

$$M_\alpha(x) = \prod_{i=0}^{k-1}(x - \alpha^{2^i}) = (x - \alpha)(x - \alpha^2)\cdots(x - \alpha^{2^{(k-1)}}). \tag{9}$$

Hence, $g(x)$ can be described as the Lowest Common Multiple (LCM) of the $(2^k - 1) - 2^{(k-1)}$ consecutive powers of α as follows:

$$g(x) = \text{LCM}(M_{\alpha^{2^{(k-1)}+1}}, M_{\alpha^{2^{(k-1)}+2}}, \cdots, M_{\alpha^{2^k-2}}, M_{\alpha^{2^k-1}}), \tag{10}$$

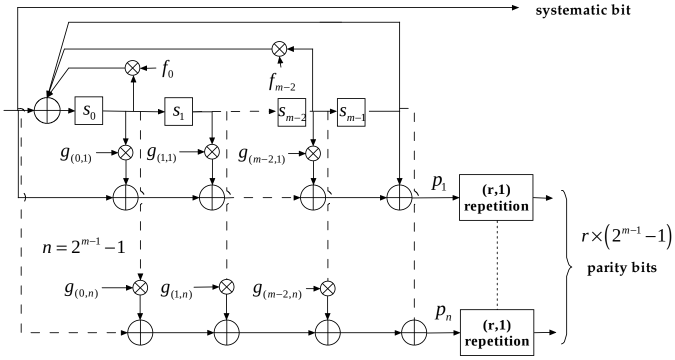

Fig. 3. Constituent code: 2^m-state rate $1/(r(2^{m-1} - 1) + 1)$ systematic convolutional code.

where obviously $\alpha^{2^k-1} = \alpha^0$. Thus, using the BCH bound, by design:

$$d_{\min} \geq (2^k - 1) - 2^{(k-1)} + 1 = 2^{k-1}, \tag{11}$$

and

$$\frac{d_{\min}}{n} = \frac{d_{\min}}{2^k - 1} \geq \frac{2^{k-1}}{2^k - 1}. \tag{12}$$

Using Theorem III.1 and (12), then (3) is satisfied with equality.

Also, for $n = r \cdot (2^k - 1)$ the bound can be achieved with equality by repeating r times the output of the $(2^k - 1, k)$ binary BCH code.

The BCH code can be expressed with a $k \times (2^k - 1)$ generator matrix $\mathbf{G}$ where the $2^k - 1$ columns of $\mathbf{G}$ are all the non-zero vectors of length k. Each of the columns $\{g_{(0,i)}, \cdots, g_{(k-1,i)}\}$ represent the connections between the k input bits and the i^{th} output bit of the code. Hence, the structure of the 2^m-state turbo code that achieves optimality under the criteria defined in Section II can be constructed as shown in Fig. 3. Moreover, the BCH code is equivalent to the code produced by the upper half of a $2^m \times 2^m$ Hadamard matrix, with the first bit punctured, which is the labeling proposed for super-orthogonal turbo-codes in [3].

As mentioned before, given the proper selection of the feedback polynomial $\vec{f}$, the effective free distance of the code is lower bounded by (1). The structure we propose gives a $d_{\min} = 2^{m-1}$ between parity labels of branches produced by a same input. Hence, the effective distance of the proposed structure is

$$d_{\text{eff,free}} = 2 + 2r(4^{m-1} - 1). \tag{13}$$

The effective free distance increases exponentially with the number of memory elements m. It also increases linearly with r but the rate decreases also linearly with r. In fact, if one considers only the parity bits, adding the repetition code does not change the code performance with respect to E_b/N_0, it only decreases its rate. The presence of a systematic bit produces two opposite effects. The systematic bit has a stronger negative impact on the overall rate (it decreases it) as r decreases. This favors the idea of using very

TABLE II

Parameters of simulated turbo codes.

m	r	n	rate	$d_{\min}$	$d_{\min}/n$	$d_{\text{eff,free}}$
3	1	3	1/7	2	2/3	32
3	8	24	1/49	16	2/3	242
4	1	7	1/15	4	4/7	128
4	9	63	1/127	36	4/7	1136
4	36	252	1/505	144	4/7	4538

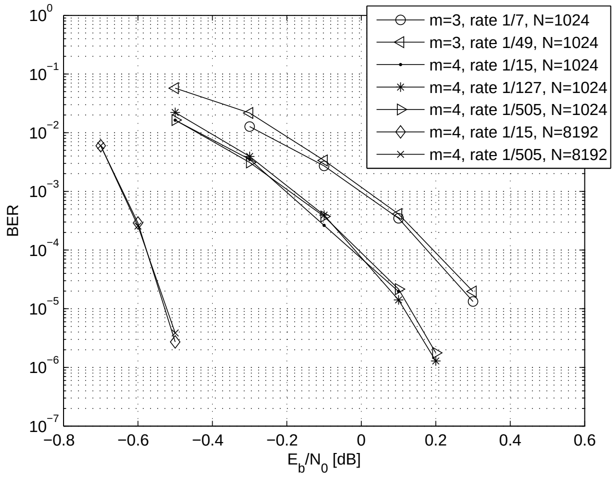

Fig. 4. BER vs. E_b/N_0 of low-rate turbo codes for a number of memory elements $m = 3, 4$, and interleaver lengths $N = 1024, 8192$, and different rates.

low rates (large r). However, the systematic bit is used by both SISO decoders, and the smaller r is, the more reliable the systematic bit is. As will be shown in Section IV, these two effects cancel each other, and the performance of the turbo-code vs. E_b/N_0 is the same for different values of r. Thus, the turbo-code performance is driven by the number of states of the constituent codes, and the interleaver length.

IV. Results

We have simulated 8-state and 16-state turbo codes for various rates, ranging from 1/7 to 1/505 and interleaver lengths of 1024 and 8192. Table II shows a full description of the turbo codes considered. In all simulations, 12 iterations are used in the decoding. Also, the interleavers have been designed using the semi-random interleaver design criteria presented in [7].

Fig. 4 shows the BER performance of these codes vs. E_b/N_0 on an AWGN channel. It can be observed that their performance is driven by the number of states in the constituent encoders and interleaver length, and it is invariant for different rates. Fig. 5 shows their performance vs. the signal-to-noise ratio. The 16-state turbo code with a rate of 1/505, and an interleaver-length of 8192 provide a BER $\simeq 10^{-5}$ at an SNR$\simeq -27.58$ dB ($E_b/N_0 = -0.55$ dB), around 1dB away from the ultimate low-rate Shannon limit.

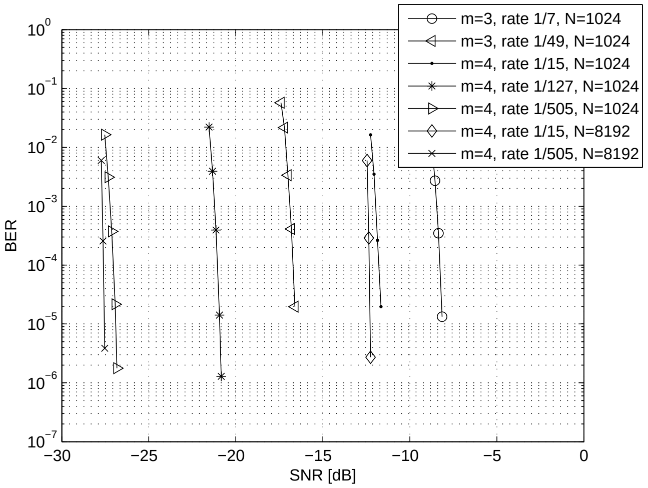

Fig. 5. BER vs. SNR of low-rate turbo codes for a number of memory elements $m = 3, 4$, interleaver lengths $N = 1024, 8192$, and different rates.

V. Conclusions

This work has presented a design criteria for arbitrarily low-rate turbo-codes for a certain constrain in decoding complexity, driven by the number of states of the constituent codes and the interleaver length. These codes are of special interest in spread-spectrum or very low signal-to-noise ratio applications. We present a design criteria, based on the notion of effective free distance, with a normalization that makes comparable turbo codes of different rates at the design stage. We prove that the concatenation of a BCH code with a repetition code to label the output sequences of the trellis transitions leads to optimal performance under this criteria. Without repetition, these codes are equivalent to the super-orthogonal turbo codes. Simulation results show that these turbo-codes can approach arbitrarily low SNRs with the same complexity and the same BER performance vs. E_b/N_0.

References

[1] Andrew J. Viterbi. Very low rate convolutional codes for maximum theoretical performance of spread-spectrum mulitple-access channels. *IEEE Journal on Selected Areas in Communications*, 8, May 1990.

[2] Li Ping, Lihai Liu, Keying Wu, and W.K. Leung. Interleave division multiple-access. *IEEE Transactions on Wireless Communications*, 5:938–947, April 2006.

[3] Petri Komulanien and Kari Pehkonen. Performance evaluation of superorthogonal turbo codes in AWGN and flat rayleigh fading channels. *IEEE Journal on Selected areas in Communications*, 16, Feb 1998.

[4] S. Benedetto and G. Montorsi. Design of parallel concatenated convolutional codes. *IEEE Trans. on Comm.*, 44, May 1996.

[5] D. Divsalar and R.J. McEliece. Effective free distance of turbo codes. *IEEE Electronics Letters*, 32, Feb 1996.

[6] S. Benedetto and G. Montorsi. Unveiling turbo codes: Some results on parallel concatenated coding schemes. In *IEEE Trans. on Info. Theory*, volume 42, Mar 1996.

[7] C. Fragouli and R.D. Wesel. Turbo-encoder design for symbol-interleaved parallel concatenated trellis-coded modulation. *IEEE Trans. on Comm.*, 49, Mar 2001.