A Codeword Weight Lower Bound for a Class of Tail-Biting Turbo Codes

Zheng Yan-Xiu and Yu T. Su
Department of Communications Engineering
National Chiao Tung University, Hsinchu, TAIWAN
non2000.cm88g@nctu.edu.tw ytsu@mail.nctu.edu.tw

***Abstract*— This paper presents an achievable codeword weight lower bound associated with weight-2 input sequences of a class of turbo codes. The class of codes has an interleaver structure that encompasses most practical interleavers used by turbo codes. It partitions the incoming information sequence into blocks of the same size and the interleaver performs intra-block and inter-block permutations. Both pre- and post-permuted blocks are individually tail-biting encoded. Following [4], we refer to the codeword associated with a weight-2 input sequence as a weight-2 error event. We apply a special permutation function that incorporates the separate encoding concept to derive a lower bound of the weight-2 error event. This lower bound reveals that (i) a larger component code period gives better distance for the weight-2 error events, and (ii) separate encoding results in improved distance if the block length is suitably chosen and is large enough.**

I. Introduction

Consider a reasonable good interleaver of size N. Partitioning an N-bit group into $L = \lceil N/W \rceil$ or $\lfloor N/W \rfloor$-bit blocks, we find the interleaving rule renders an inter-block permutation structure like that shown in Fig. 1. Such a structure can be found in other codes such as product codes (block turbo codes, BTCs). Hence both classic convolutional turbo codes (CTCs) and BTCs can be considered as subclasses of the recently proposed inter-block permuted (IBP) turbo codes (IBPTCs) [3] whose interleaver performs consecutive intra- and then inter-block permutations.

However, an interleaver used in a classic CTC, after the above virtual partition, usually yields a non-regular local interleaving structure, i.e., the interleaving relation between a block and other blocks in the same group does not follow the same permutation rule. In contrast, product codes and some IBPTCs have much more regular local interleaving structures. An appropriate regular local interleaving (and deinterleaving) structure makes implementation easier and offers properties that are useful for parallel decoding, e.g., (memory access) contention-free and simpler routing requirement.

Another distinction between classic CTCs and other subclasses of IBPTCs is that, for a classic CTC with an interleaving size of N bits (in L *virtual* blocks), encoding of consecutive blocks is often continuous. On the other hand, a product code arranges N information bits in a two dimensional array and encodes each row and column separately (discontinuously). The class of IBP turbo codes (IBPTCs) can also encodes each block separately.

Between the two separate (discontinuous) encoding options, the tail-biting encoding scheme, since it can do without tail-bits, gives a higher spectral efficiency. Moreover, it was shown that [1], [2], as a tail-biting CTC can eliminate some error events across neighboring blocks, improved distance properties can be obtained. Weiss *et al.* [2] proposed a product code (without the check-on-check part) whose column and row vectors are tail-biting encoded convolutional codewords and derived some distance properties.

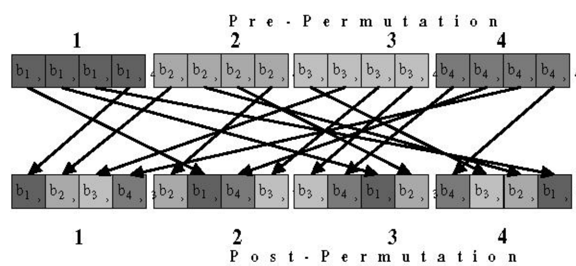

Fig. 1. The inherent inter-block interleaving structure can be found in most practical interleavers.

The codeword associated with a weight-2 input sequence was called a weight-2 error event by Breiling [4] for an obvious reason. Most CTC interleaver designs [6], [3] take this class of error events into account, trying to maximize the minimum weight of these error events. Breiling [4] suggested a novel partition strategy to derive upper bounds for the weight-2 error events. Although the upper bound is not as tight as more general upper bounds [4], [5] which consider other error events as well, weight-2 error event remains an important design concern.

As mentioned before, a general IBP interleaver [3] encompasses many existing interleavers as special subclasses. It is built on smaller interleavers and uses some re-permutation across these interleavers to construct a larger interleaver. By using a suitable IBP rule, an IBPTC can possess good distance properties. It is therefore reasonable to conjecture that the distance spectrum of a CTC using an IBP interleaver and separate encoding would offer some desired properties. The purpose of this paper is to validate a part of this conjecture. We derive a general lower bound for the weight-2 error events associated with general IBP-interleaved CTCs. By analyzing the effects

1-4244-1429-6/07/$25.00 ©2007 IEEE

of selected particular system parameters on this general bound we obtain some useful design guidelines. We use a simplified partition rule presented in [4] and apply a regular permutation function to derive the bound. We also examine some special cases and evaluate distance lower bounds of the weight-2 error events for different block lengths.

The rest paper is organized as follows. The next section presents our derivation of the achievable weight-2 lower bound. In section III, we examine some special codes, evaluate the corresponding distance bounds and discuss the resulting design constraints. The last section contains some concluding remarks.

II. The achievable weight-2 input lower bound

For convenience of subsequent discourse, we need to define some notations to begin with.

Definition 1:

$$|X|_Y = X \mod Y. \quad (1)$$

Definition 2:

$$||X||_Y = \begin{cases} Y, & |X|_Y = 0 \\ |X|_Y, & |X|_Y \neq 0 \end{cases} \quad (2)$$

Definition 3: $scrb_{tb}^{L}(\mathbf{u})$ is the weight of a length$-L$ tail-biting convolutional code output for a input sequence $\mathbf{u}$.

Definition 4:

$$W_2(L) = \min_{i,j,|i-j|_{T_c}\neq 0, |L-i+j|_{T_c}\neq 0} scrb_{tb}^{L}(\mathbf{u}^{ij}), \quad (3)$$

where $\mathbf{u}^{ij}$ is a weight-2 input sequence with nonzero elements at coordinates i and j.

Definition 5:

$$W_1(L) = \min_{i} scrb_{tb}^{L}(\mathbf{u}^{i}), \quad (4)$$

where $\mathbf{u}^{i}$ is a weight-1 input sequence with the nonzero element located at coordinate i.

$scrb_{tb}^{L}(\mathbf{u}^{ij})$ is lower-bounded by $\alpha\frac{|i-j|}{T_c}+\beta$ or $\alpha\frac{(L-|i-j|)}{T_c}+\beta$ [4], where T_c is the period of the convolutional code used. Moreover $scrb_{tb}^{L}(\mathbf{u}^{ij}) \geq W_2(L)$ if $|i-j|_{T_c} \neq 0$ and $|L-|i-j||_{T_c} \neq 0$; otherwise $scrb_{tb}^{L}(\mathbf{u}^{ij}) = \alpha \cdot \min\left(\frac{|i-j|}{T_c}, \frac{(L-|i-j|)}{T_c}\right) + \beta$. Furthermore, if no puncturing is applied, the linearity of the convolutional code implies $\frac{\alpha\cdot(L-T_c)}{T_c} + \beta \leq W_2(L) \leq \frac{\alpha\cdot(L+T_c)}{T_c} + \beta$.

A. Partition rule

Systematic recursive convolutional code used in a CTC is equivalent to an IIR scrambler whose period has a great impact on the distance property of the associated CTC. A finite weight codeword can be generated by a weight-k input sequence, $k \geq 2$. If $k = 2$, the distance of these two nonzero coordinates must be divisible by the period. Breiling [4] applies this property to partition the coordinates of input sequences into some equivalence classes in which any two coordinates is associated with a finite weight codeword. He concluded that a larger component period implies a smaller probability in generating low weight codewords.

The simplified partition rule for the ith pre-permutation ($k = 0$) and post-permutation ($k = 1$) sets $F_i^{(k)}, k = 0, 1$ is given by

$$F_i^{(k)} = \begin{cases} \left\{i + T_c j : 0 \leq j < \left\lceil \frac{L}{T_c} \right\rceil\right\}, & 0 \leq i < |L|_{T_c} \\ \left\{i + T_c j : 0 \leq j < \left\lfloor \frac{L}{T_c} \right\rfloor\right\}, & |L|_{T_c} \leq i < T_c \end{cases} \quad (5)$$

An exemplary partition of (5) is shown in Fig. 2 where the integers represent the coordinates of either an pre-permutation or post-permutation sequence. Each row represents an index set $F_i^{(k)}$ and is of size 8 or 7.

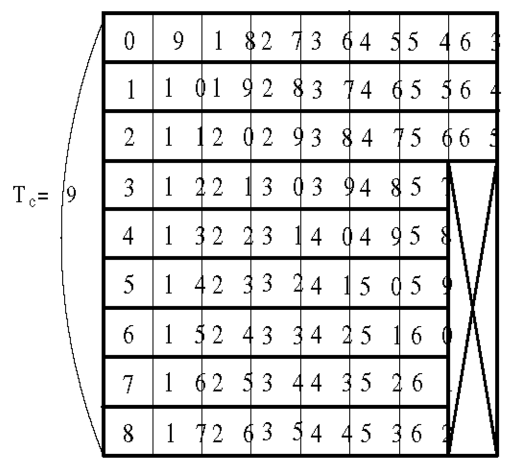

Fig. 2. Partition of equivalence classes; $L = 66$, $T_c = 9$.

B. Main Theorem

In this section we establish our main result whose proof needs the following two lemmas.

Lemma 1: For each integer set $S_X = \{0, 1, 2, ..., X-1\}$, there exists a permutation rule Π_X such that $\min_{i\neq j \in S_X}(|i-j|_X + |\pi_X(i)-\pi_X(j)|_X, |i-j|_X + X - |\pi_X(i)-\pi_X(j)|_X, X - |i-j|_X + |\pi_X(i)-\pi_X(j)|_X, 2X - |i-j|_X - |\pi_X(i) - \pi_X(j)|_X) \geq r+1$, where $r = \left\lceil \sqrt{X} \right\rceil - 1$. A permutation satisfying these constraints is

$$\pi_X(i) = \left| ri + \frac{i - |i|_q}{q} \right|_X, \; q = \frac{X}{\gcd(X, r)}. \quad (6)$$

Proof: It is obvious that the inequality holds if $|i-j|_X \geq r$ and $X - |i-j|_X \geq r$. Hence we consider $|i-j|_X < r$ or $X - |i-j|_X < r$ only.

When $i > j$ and $0 < i - j < r$, $\gcd(X, r) \leq r$ and $r = \lceil\sqrt{X}\rceil - 1 < \sqrt{X}$ implies that $q = X/\gcd(X, r) \geq \frac{X}{r} >$

$\sqrt{X} > r$ while $0 < i - j < r$ leads to

$$\begin{aligned} & \frac{i-j+|j|_q-|i|_q}{q} \\ = & \begin{cases} \frac{i-j+|q+j-i|_q}{q} = \frac{i-j+q+(j-i)}{q} = 1, \\ \quad \text{if } |j|_q - |i|_q > 0, \\ \frac{i-j-|i-j|_q}{q} = \frac{i-j-(i-j)}{q} = 0, \\ \quad \text{if } |j|_q - |i|_q < 0. \end{cases} \end{aligned} \quad (7)$$

It follows that

$$\begin{aligned} & |\pi_X(i) - \pi_X(j)|_X \\ = & \left| \left| ri + \frac{i-|i|_q}{q} \right|_X - \left| rj + \frac{j-|j|_q}{q} \right|_X \right|_X \\ = & \left| r(i-j) + \frac{i-j+|j|_q-|i|_q}{q} \right|_X \geq r \end{aligned}$$

and

$$\begin{aligned} & X - |\pi_X(i) - \pi_X(j)|_X \\ = & X - \left| \left| ri + \frac{i-|i|_q}{q} \right|_X - \left| rj + \frac{j-|j|_q}{q} \right|_X \right|_X \\ \geq & X - |r(r-1)+1|_X = X - r^2 + r - 1 \\ \geq & r^2 + 1 - r^2 + r - 1 = r. \end{aligned}$$

Therefore, $\min_{i,j \in S_x}(i - j + |\pi_X(i) - \pi_X(j)|_X, i - j + X - |\pi_X(i) - \pi_X(j)|_X) \geq r + 1$.

This permutation function is q-invariant in that

$$\begin{aligned} & |\pi_X(|i-q|_X) - \pi_X(|j-q|_X)|_X \\ = & \left| \left| r(i-q) + \frac{(i-q)-|i-q|_q}{q} \right|_X \right. \\ & \left. - \left| r(j-q) + \frac{(j-q)-|j-q|_q}{q} \right|_X \right|_X \\ = & \left| \left| ri + \frac{i-|i|_q}{q} \right|_X - \left| rj + \frac{j-|j|_q}{q} \right|_X \right|_X \\ = & |\pi_X(i) - \pi_X(j)|_X \end{aligned}$$

We now show that both the remaining cases can be converted into the above case.

(A) For the case $i < j$ and $0 < j - i < r$, we have $|i-j|_X = |i + X - j|_X = |i + X - mq - (j - mq)|_X = |i' - j'|$ and $|\pi_X(|i+X-mq|_X) - \pi_X(|j-mq|_X)|_X = |\pi_X(i) - \pi_X(j)|_X$, $X > i' = |i + X - mq|_X > j' = |j - mq|_X \geq 0$ for some $m > 0$.

(B) If $i > j$, $X - |i-j|_X = |X + j - i|_X = |X + j - mq - (i - mq)| = |j' - i'|$ and $|\pi_X(|i-mq|_X) - \pi_X(|X+j-mq|_X)|_X = |\pi_X(i) - \pi_X(j)|_X$, $X > i' = |i + X - mq|_X > j' = |j - mq|_X \geq 0$ for some $m > 0$. ■

Lemma 2: Given N_1 distinct n-element sets and N_2 distinct $(n-1)$-element sets, where $n > 1$. If we arrange all elements in these $N_1 + N_2$ sets into a cycle, the minimum *separation* among elements in the same set is lower-bounded by $N_1 + N_2 - \lceil \frac{N_2}{n} \rceil$ for the $n-$element sets, and $N_1 + N_2 - \lfloor \frac{N_2}{n} \rfloor$ for the $(n-1)-$element sets. Moreover, there are at most $|N_2|_n$ element pairs with separation $N_1 + N_2 - \lceil \frac{N_2}{n} \rceil$ for these n-element sets.

Proof: We place the elements in the jth n-element set in a cycle by $j + i(N1 + N2 - \lfloor \frac{N_2}{n} \rfloor)$, where $0 \leq i < n$ and $0 \leq j < N_1$. The elements of the jth $(n-1)$-element set are placed at positions indexed by

$$\begin{cases} \left\lfloor \frac{iN_2+j-N_1}{M_1} \right\rfloor (N_1 + M_1) + N_1 + |iN_2 - N_1 + j|_{M_1}, \\ \qquad iN_2 + j \leq M_3, \\ N_1|N_2|_n + M_3 + \left\lfloor \frac{iN_2+j-N_1-M_3}{M_2} \right\rfloor (N_1 + M_2) + N_1 \\ \qquad + |iN_2 + j - N_1 - M_3|_{M_2}, \quad \text{otherwise,} \end{cases}$$

where $0 \leq i < n-1$, $N_1 \leq j < N_1 + N_2$, $M_1 = N_2 - \lfloor \frac{N_2}{n} \rfloor$, $M_2 = N_2 - \lceil \frac{N_2}{n} \rceil$ and $M_3 = M_1|N_2|_n$. It is easy to see that such an arrangement achieve the bounds and no larger minimum separation can be found. ■

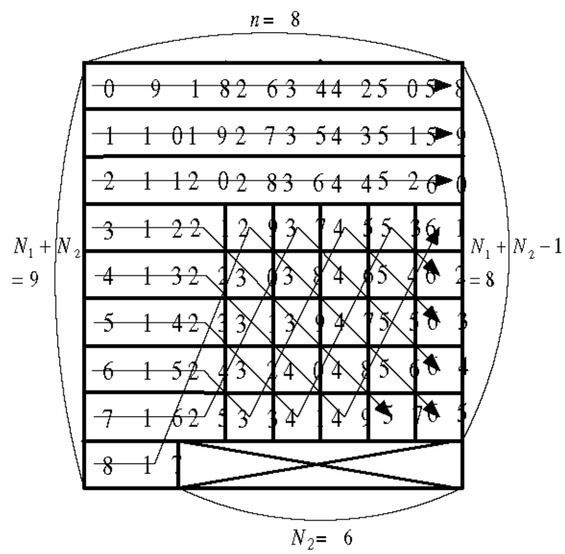

Fig. 3. Set mapping; $N_1 = 3$, $N_2 = 6$ and $n = 8$.

Fig. 3 shows a exemplary placement for $N_1 = 3$, $N_2 = 6$ and $n = 8$. The minimum septation in these N_1 8-element and N_2 7-element sets is at least 7 and 8, respectively. Moreover, there are only $|N_2|_8 = 6$ element pair with separation 7 for these 8 element sets.

Since the scrambler output weight of the weight-2 error events is lower-bounded by the difference of an (i, j) coordinate pair, the weight of a tail-biting encoded CTC is lower-bounded by

$$\min_{i,j} (2 + W(i, j, L) + W(\pi(i), \pi(j), L)) \quad (8)$$

where π is a length L permutation function and

$$W(i, j, L) = \begin{cases} \alpha \frac{|i-j|}{T_c} + \beta & , |i-j|_{T_c} = 0 \\ \alpha \frac{L-|i-j|}{T_c} + \beta & , |L - |i-j||_{T_c} = 0 \\ W_2(L) & , \text{ otherwise} \end{cases} . \quad (9)$$

Based on the above results, we can prove

Theorem 1: There exists a separate tail-biting encoded CTC of block length L whose minimum codeword weight $w_{2,min}$

for weight-2 input sequences is lower-bounded by

$$w_{2,min} \geq 2 + 2\beta + \min \Big(W_2(L) + \alpha D_{min} - \beta, \alpha D_{min} \min\left(\left\lceil \sqrt{N_{max}} \right\rceil, 2|N_2|_{N_{max}}\right) + \alpha D_{max} \max\left(\left\lceil \sqrt{N_{max}} \right\rceil - 2|N_2|_{N_{max}}, 0\right)\Big), \quad (10)$$

where $2W_1(L) \geq 2 + \alpha D_{min} + W_2(L) + \beta$, $D_{min} = dT_s - \left\lceil \frac{N_2}{N_{max}} \right\rceil$, $D_{max} = dT_s - \left\lfloor \frac{N_2}{N_{max}} \right\rfloor$, $N_2 = dT_s - ||\frac{L}{d}||_{dT_s}$, $N_{max} = \left\lceil \frac{L}{d^2 T_s} \right\rceil$, d=gcd$(|L|_{T_c}, T_c)$ and T_s is the number of blocks involved in encoding.

Proof: Tail-biting encoding results in low-weight codewords whose nonzero coordinates are confined to the tail and the head parts of two consecutive sets. This happens if one nonzero coordinate of a weight-2 input sequence belongs to $\mathcal{F}_i^{(k)}$ and the other one belongs to $\mathcal{F}^{(k)}_{|i+T_c-|L|_{T_c}|_{T_c}}$. One can then place the set $\mathcal{F}^{(k)}_{|i+T_c-|L|_{T_c}|_{T_c}}$ right after the set $\mathcal{F}_i^{(k)}$ so that they form a cycle. If gcd$(|L|_{T_c}, T_c) = d$, we have d cycles with the mth cycle being $\widetilde{\mathcal{F}}_m^{(k)} = \Big\{\mathcal{F}_m^{(k)}, \mathcal{F}^{(k)}_{|m+T_c-|L|_{T_c}|_{T_c}}, \mathcal{F}^{(k)}_{|m+2(T_c-|L|_{T_c})|_{T_c}}, \cdots, \mathcal{F}^{(k)}_{|m+(\frac{T_c}{d}-1)(T_c-|L|_{T_c})|_{T_c}}\Big\}$, where $0 \leq m < d$.

Mapping the coordinates in $\widetilde{\mathcal{F}}_m^{(k)}$ sequentially to the integers in the interval $\left[0, |\widetilde{\mathcal{F}}_m^{(k)}| - 1 = \frac{L}{d} - 1\right]$, we obtain the set $S_{|\widetilde{\mathcal{F}}_m^{(k)}|} = \left\{0, 1, 2, \cdots, \frac{L}{d} - 1\right\}$. We further partition $S_{|\widetilde{\mathcal{F}}_m^{(k)}|}$ into dT_s sets $\{S_i\}$, where $|S_i| = N_{max} = \left\lceil \frac{L}{d^2 T_s} \right\rceil$ for $0 \leq i < N_1 = ||\frac{L}{d}||_{dT_s}$ and $|S_i| = N_{min} = \left\lfloor \frac{L}{d^2 T_s} \right\rfloor$ for $dT_s - N_2 = ||\frac{L}{d}||_{dT_s} \leq i < dT_s$. According to *Lemma 2*, we can maximize the minimum separation of S_i to $D_{min} = dT_s - \left\lceil \frac{N_2}{N_{max}} \right\rceil$ and $D_{max} = dT_s - \left\lfloor \frac{N_2}{N_{max}} \right\rfloor$ for $0 \leq i < N_1$ and $dT_s - N_2 \leq i < dT_s$ respectively.

We can construct an IBP rule such that $p \in S_i$ and $q \in S_j$ are permuted to the same block iff $|i - j|_{T_s} = 0$. Since all blocks can apply the same partition rule for permutation, such an IBP rule does exist.

Incorporating separate encoding results in that two indexes in two different blocks produce a codeword weight larger than the bound, either the pre-permuted or the post-permuted pair makes the codeword weight $2W_1(L)$. Therefore we consider the case two indexes are permuted to the same block.

There are d sets S_i and d sets $S_{|\widetilde{\mathcal{F}}_m^{(2)}|}$. All $S_i \subset S_{|\widetilde{\mathcal{F}}_m^{(1)}|}$ can be permuted to different $S_{|\widetilde{\mathcal{F}}_m^{(2)}|}$. If two indexes are in two different S_i's, either the pre-permuted or the post-permuted pair makes the codeword weight $\geq W_2(L)$, which is larger than the bound. Therefore we only have to consider the case when a coordinate pair belongs to the same S_i before and after permutation.

According to *Lemma 1*, the separation sum of pre-permutation and post-permutation for S_i with N_{max} and N_{min} elements can be $\left\lceil \sqrt{N_{max}} \right\rceil$ and $\left\lceil \sqrt{N_{min}} \right\rceil$ respectively. According to *Lemma 2*, the minimum separation of two adjacent indexes is D_{min} and there are at most $|N_2|_{N_{max}}$ pairs with such a separation. The minimum codeword weight is thus lower-bounded by $2 + \alpha D_{min} \min(2|N_2|_{N_{max}}, \lceil \sqrt{N_{max}} \rceil) + \alpha D_{max} \max(\lceil \sqrt{N_{max}} \rceil - 2|N_2|_{N_{max}}, 0) + 2\beta$.

Finally, we notice that small weight error event occurs when the two coordinate pair $(i, j) \in \widetilde{\mathcal{F}}_m$ is such that $|i - j|_{T_c} \neq 0$ and $|L - |i-j||_{T_c} \neq 0$ and the separation of the permuted pair $(\pi_{|\widetilde{\mathcal{F}}_m|}(i), \pi_{|\widetilde{\mathcal{F}}_m|}(j))$ is greater than $T_c D_{min}$. The corresponding codeword weight will be at least $2 + W_2(L) + \alpha D_{min} + \beta$. Therefore, we have

$$w_t(\mathbf{X}^{ij}) \geq 2 + 2\beta + \min_{i,j} \Big(W_2(L) + \alpha D_{min} - \beta, \alpha D_{min} \min\left(2|N_2|_{N_{max}}, \left\lceil \sqrt{N_{max}} \right\rceil\right) + \alpha D_{max} \max\left(\left\lceil \sqrt{N_{max}} \right\rceil - 2|N_2|_{N_{max}}, 0\right)\Big). \quad (11)$$

■

If $L \geq (T_c + 2d)M$, we have

$$\begin{aligned}
& T_c D_{min} \min(2|N_2|_{N_{max}}, \sqrt{N_{max}}) \\
& + T_c D_{max} \max(\sqrt{N_{max}} - 2|N_2|_{N_{max}}, 0) \\
\leq \;& T_c d T_s \left\lceil \sqrt{\left\lceil \frac{L}{d^2 T_s} \right\rceil} \right\rceil \\
< \;& Md \left(\sqrt{\frac{L}{d^2 T_s} + 1} + 1 \right) \\
\leq \;& \sqrt{T_c^2 T_s L + d^2 M^2} + dM \\
\leq \;& \sqrt{(L - 2dT_c T_s)L + d^2 M^2} + dM \\
\leq \;& \sqrt{L^2 - 2dML + d^2 M^2} + dM = L, \qquad (12)
\end{aligned}$$

where $M = T_c T_s$. Then

$$\begin{aligned}
& \alpha D_{min} \min\left(2|N_2|_{N_{max}}, \left\lceil \sqrt{N_{max}} \right\rceil\right) \\
+ \;& \alpha D_{max} \max\left(\left\lceil \sqrt{N_{max}} \right\rceil - 2|N_2|_{N_{max}}, 0\right) + \beta \\
\leq \;& \frac{\alpha L}{T_c} + \beta \leq W_2(L) + \alpha, \qquad (13)
\end{aligned}$$

if no puncturing is applied for the scrambler.

Corollary 1: If the block length L is greater than $(T_c + 2d)M$ and no puncturing is applied, then there exists a separate encoding tail-biting turbo code whose minimum codeword weight $w_{2,min}$ for weight-2 input sequences is lower-bounded by

$$w_{2,min} \geq 2 + \alpha D_{min} \min\left(2|N_2|_{N_{max}}, \left\lceil \sqrt{N_{max}} \right\rceil\right) + \alpha D_{max} \max\left(\left\lceil \sqrt{N_{max}} \right\rceil - 2|N_2|_{N_{max}}, 0\right) + 2\beta, \quad (14)$$

where $2W_1(L) > 2 + \alpha D_{min} + W_2(L) + \beta$, $M = T_c T_s$, $D_{min} = dT_s - \left\lceil \frac{N_2}{N_{max}} \right\rceil$, $D_{max} = dT_s - \left\lfloor \frac{N_2}{N_{max}} \right\rfloor$, $N_2 = dT_s - ||\frac{L}{d}||_{dT_s}$, $N_{max} = \left\lceil \frac{L}{d^2 T_s} \right\rceil$, d=gcd$(|L|_{T_c}, T_c)$ and T_s is the number of blocks involved in encoding.

III. Numerical Examples

We evaluates lower bounds for the scramblers given in Table I. Figs. 4-6 plot the lower bounds for various interleaver length

TABLE I

(α, β) FOR SOME SCRAMBLERS.

Scramblers	T_c	(α, β)
$\frac{1+D^2}{1+D+D^2}$	3	$(2, 2)$
$\frac{1+D+D^3}{1+D^2+D^3}$	7	$(4, 2)$
$\frac{1+D^2+D^3+D^4}{1+D+D^4}$	15	$(8, 2)$

$T_s L$. Larger component code periods generally give better bounds, as indicated by these curves.

Separate encoding improves the lower bounds for some interleaver lengths but also imposes constraints on interleaver lengths. These figures shows 10–50 weight improvements on the lower bound for long interleaver lengths but $W_2(L)$ is small for short interleaver lengths. Fig. 6 indicates that, the lower bound is a decreasing function of T_s for short block length. *Corollary 1* says that $W_2(L)$ is not a dominant factor of the lower bound if the block length constraint $L \geq (T_c + 2d)M$ is satisfied.

Fig. 4 compares the upper bound [4] and the lower bound we derived. The large "gap" between the upper and lower bounds is due to the fact that [4] does not consider the weight-2 error events resulted from adjacent partitions but our derivation does. The gap would be much reduced if these events were taken into account.

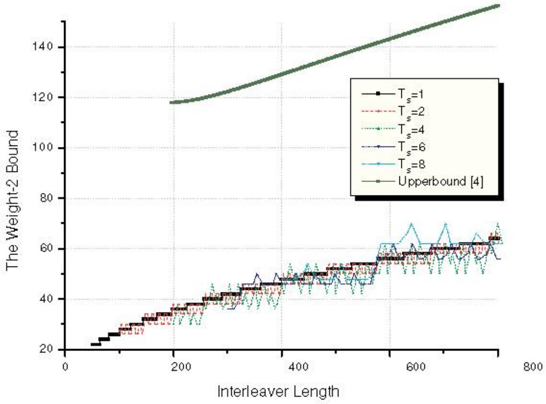

Fig. 4. The weight 2 lower bound for the Scrambling function $\frac{1+D^2}{1+D+D^2}$.

IV. Conclusion

This paper derives a general achievable codeword weight lower bound for the weight-2 error events when a separate tail-biting encoded CTC uses two identical scramblers (component codes) and an IBP interleaver. The bound implies separate encoding stands a better chance to obtain a weight-2 lower bound larger than that of the conventional continuous encoding scheme if the block length is not too small and is properly chosen. The relationships between these two parameters and the lower bound provide useful design guideline for the separate tail-biting encoded CTCs.

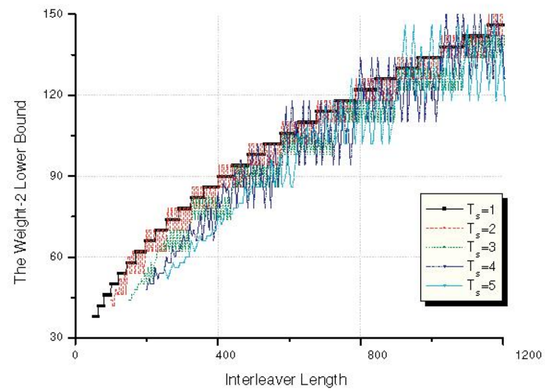

Fig. 5. The weight 2 lower bound for the Scrambling function $\frac{1+D+D^3}{1+D^2+D^3}$.

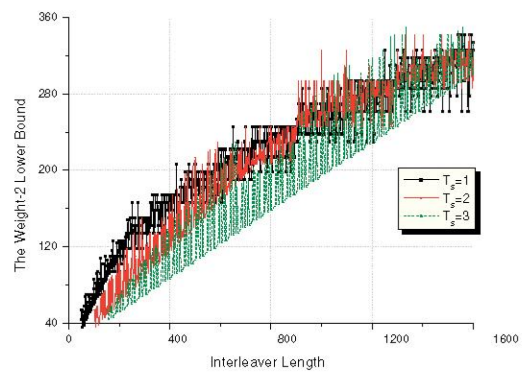

Fig. 6. The weight 2 lower bound for the Scrambling function $\frac{1+D^2+D^3+D^4}{1+D+D^4}$.

References

[1] C. Weiss, C. Bettstetter, S. Riedel, D. J. Costello, "Turbo decoding with tail-biting trellis," in *Proc. ISSSE'98*, Pisa, Italy, pp. 343-348, 1998.

[2] C. Weiss, C. Bettstetter, S. Riedel, "Code construction and decoding of parallel concatenated tail-biting codes," *IEEE Trans. Inform.*, vol. 47, no. 1, pp. 366-386 , Jan. 2001.

[3] Y.-X. Zheng, Y. T. Su, "On the inter-block permutation and turbo codes," in *Proc. 3nd Inter. Sympo. Turbo codes*, Brest, France, pp. 107-110, Sep. 2003.

[4] M. Breiling, J. B. Huber, "Combinatorial analysis of the minimum distance of turbo codes," *IEEE Trans. Inform. Theory*, vol. 47, no 7, pp. 2737-2750, Nov. 2001.

[5] A. Perotti, S. Benedetto, "A new upper bound on the minimum distance of turbo codes," *IEEE Trans. Inform. Theory*, vol. 50, no. 12, pp. 2985-2997, Dec. 2004.

[6] C. Fragouli, R. D. Wesel,"Semi-random interleaver design criteria," in *Proc. Globecom'99*, Rio de Janeiro, Brazil, pp. 2352-2356, 1999.