Group Structure of Turbo-codes with Application to the Inter-leaver Design[1]

A. K. Khandani

Dept. of Elec. and Comp. Eng., University of Waterloo, Waterloo, ON, Canada, N2L 3G1

Abstract — **It is shown that the interleaving in Turbo-codes provides a homomorphism between the encoded streams and consequently can not break all the low weight input sequences. A method is presented to optimize the structure of the interleaver. It is show that for large block lengths optimization of the interleaver does not affect the code performance.**

Turbo-codes make use of Recursive Convolutional Codes (RCC) with a Maximum Length Sequence (MLS) impulse response. Assuming a code generator $G(d) = N(d)/D(d)$, if $D(d)$ is a primitive polynomial, then the period of the impulse response of $G(d)$ is a factor of 2^m-1 where m is the memory length of the code [1]. If the period is equal to 2^m-1, it is called an MLS. This is the case if 2^m-1 is a prime number. An MLS is composed of 2^m-1 non-zero interlaced sequences (called phases) which are time shifts of each other. This set of phases (plus the all zero sequence) constitute a group [1]. Group structure of Turbo-codes has been also discussed in some prior research works including [2, 3, 4].

Consider the set of 2^N input sequences where N is the block length. The sequences resulting in a zero phase form a subgroup of cardinality 2^{N-m}. The interleaver provides a homomorphism with respect to the addition of phases which tries to map the elements of the zero phase subgroup into its cosets (breaking of the zero phase sequences). It is shown that: (i) a single interleaver can at best reduce the number of the zero phase sequences from 2^{N-m} to 2^{N-2m}, (ii) there exists an interleaver which breaks all the weight two sequences with a span limited to $(2^m-1)^2$, (iii) there does not exist an interleaver which breaks all the weight two sequences of a larger span.

It is shown that for $N \to \infty$, the weight of the systematic and parity check sequences has a Gaussian distribution. The corresponding correlation coefficients are shown by ρ_{ij}, $i,j = 1,2,3$ where $1,2,3$ refer to the systematic and the parity check sequences, respectively. It is desirable to minimize the ρ_{ij}'s, however, it is shown that for a bit error probability bounded away from zero, we have: (i) $\rho_{ij} > 0$, $i,j = 1,2,3$, (ii) $\rho_{12}, \rho_{13} \to 0$ as $N \to \infty$, (iii) $\rho_{23} \to 0$ as $N \to \infty$ for almost any random interleaver. This means that for $N \to \infty$, the weight of the three coded steams become independent of each other which is the best one can obtain.

To optimize the interleaver structure for small block lengths, we consider an integer K which is prime with respect to 2^m-1 and refer to time positions which are congruent to i modulo K as C_i. We define an optimality criterion based on the distances between pairs of bit positions (incorporating the edge effects) and iteratively permute C_i's such that this objective function is maximized. We use a set of variables δ_m^n where $\delta_m^n = 1$ if the mth position of a given C_i is assigned to $n \neq m$ position. If the contribution of this assignment to the overall objective function is $d_m^n(i)$, we obtain,

$$\text{Max} \quad \sum_{m=1}^{N}\sum_{n=1}^{N} \delta_m^n d_m^n(i)$$

$$\text{S. to:} \quad \sum_{m=1}^{N} \delta_m^n = 1, \ \sum_{n=1}^{N} \delta_m^n = 1, \ \delta_m^n \in \{0,1\}, \ \forall m,n$$

This problem can be solved very efficiently using the Hungarian method. We have performed this optimization for a rate 1/3 code with $m = 2$, generator $(D,N) = (7,5)$, $K = 7$, $N = 196$, using 20 iterations. Prior to the optimization, we divide the block into consecutive sub-blocks of length K and apply i circular shifts to the ith sub-block. Fig. 1 shows the bit error probability of a random vs. optimized interleaver.

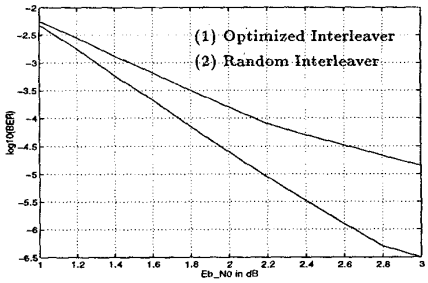

Figure 1: Bit error performance of a random vs. optimized interleaver.

References

[1] S. W. Golomb, "Shift register sequences,", Holden-Day, 1967.

[2] D. Divsalar, F. Pollara, "On the Design of Turbo Codes", *JPL TDA Progress Report 42-123*, Nov.95.

[3] S. Benedetto, G. Montorsi, "Design of parallel concatenated convolutional codes", *IEEE Trans. Commun.*, vol.44, pp. 591-600, May 96.

[4] L. C. Perez, J. Seghers, and D. J. Costello, Jr., "A distance spectrum interpretation of turbo codes", *IEEE Trans. Inform. Theory*, vol. 42, pp. 1698-1709, Nov 96.

[1]This work has been supported by the Information Technology Research Centre (ITRC) of Canada.