New Classes of Algebraic Interleavers for Turbo-Codes[1]

Oscar Y. Takeshita
Dept. of Electrical Engineering
University of Notre Dame
Notre Dame, IN 46556
Email Takeshita.1@nd.edu

Daniel J. Costello, Jr.
Dept. of Electrical Engineering
University of Notre Dame
Notre Dame, IN 46556
Email Costello.2@nd.edu

Abstract — **In this paper we present classes of algebraic interleavers that permute a sequence of bits with nearly the same statistical distribution as a randomly chosen interleaver. When these interleavers are used in turbo-coding, they perform equal to or better than the average of a set of randomly chosen interleavers. They are based on a property of quadratic congruences over the ring of integers modulo powers of 2.**

I. Introduction

Interleavers that have a simple algebraic structure are interesting from both a theoretical and practical point of view. For parallel concatenated turbo-codes [1], some authors have investigated block interleavers [2] and other interleavers with a similar structure [3]. Those interleavers were found to be better than randomly chosen interlevears for turbo-codes with information block lengths smaller than 1000.

In this paper we assume rate 1/2 parallel concatenated turbo-codes, where $(37, 21)$ represents the feedback and feedforward polynomials of the systematic recursive convolutional component code in octal notation.

Let $\overline{x} =< x_0, x_1, \ldots, x_{N-1} >$ be a sequence in $\{0,1\}^N$. An interleaver $\mathcal{I}_N$ maps $\overline{x}$ to a sequence $\overline{y} =< y_0, y_1, \ldots, y_{N-1} >$ such that $\overline{y}$ is a permutation of the elements of $\overline{x}$, i.e., if we consider $\overline{x}$ and $\overline{y}$ as a pair of sets with N elements, there is a one-to-one and onto correspondence $x_i \leftrightarrow y_j$ between every element of $\overline{x}$ and every element of $\overline{y}$. Let $A = \{0, \ldots, N-1\}$; $\mathcal{I}_N$ can then be defined by the one-to-one and onto *index mapping function* $d_{\mathcal{I}_N} : A \to A$, $d_{\mathcal{I}_N} : i \mapsto j$, $i, j \in A$, and can be expressed as an ordered set called the *permutation vector* $\overline{\mathcal{I}}_N = [d_{\mathcal{I}_N}(0), d_{\mathcal{I}_N}(1), \ldots, d_{\mathcal{I}_N}(N-1)]$.

Theorem I.1 *For any N equal to a power of 2, the function $c(m) \equiv \frac{km(m+1)}{2} \pmod N$, $0 \le m < N$, k an odd constant, is bijective.*

We immediately have a permutation $\mathcal{D}_{N:CN}$ with a single N-cycle if we define $d_{\mathcal{D}_{N:CN}}$ as its *index mapping function* $d_{\mathcal{D}_{N:CN}} : c(m) \mapsto c(m+1) \pmod N$, $0 \le m < N$.

Example I.1 *For the length $N = 8$ $\mathcal{D}_{8:CN}|_{k=1}$ interleaver, we have $(c(0), c(1) \ldots, c(7)) = (0, 1, 3, 6, 2, 7, 5, 4)$. Then the* index mapping function *becomes $d_{\mathcal{D}_{8:CN}|_{k=1}} : 0 \mapsto 1, d_{\mathcal{D}_{8:CN}|_{k=1}} : 1 \mapsto 3, \ldots,$ and the* permutation vector *representation becomes $\overline{\mathcal{D}}_{8:CN}|_{k=1} = [1, 3, 7, 6, 0, 4, 2, 5]$.*

Further, we can cyclically shift the *permutation vector* representation of $\overline{\mathcal{D}}_{N:CN} = [d_{\mathcal{D}_{N:CN}}(0), \ldots, d_{\mathcal{D}_{N:CN}}(N-1)]$ to the right by a constant h, $0 \le h \le N-1$, without changing the essential properties of the interleaver, since the relative positions are only slightly disturbed.

[1]This work was supported by NSF Grant NCR95-22939 and NASA Grant NAG5-557.

Theorem I.2 *A shift of $h = N/2$ in the* permutation vector *of a $\mathcal{D}_{N:CN}$ interleaver produces an interleaver whose* permutation vector *is now composed of 1-cycles and 2-cycles.*

We thus have a second class of interleavers that we call $\mathcal{D}_{N:C2}$. Decoders for turbo-codes need interleaver-deinterleaver pairs. The $\mathcal{D}_{N:C2}$ interleavers provide an interesting implementation advantage, since deinterleaving is identical to interleaving.

Example I.2 $\overline{\mathcal{D}}_{8:C2}|_{k=1,h=4} = [0, 4, 2, 5, 1, 3, 7, 6]$.

In Fig. 1 we show the BER performance of turbo-codes using the new deterministic $\mathcal{D}_{N:CN}$ and $\mathcal{D}_{N:C2}$ interleavers compared with the average performance of 7 randomly chosen interleavers $< \mathcal{R}_N >_7$ of the same size.

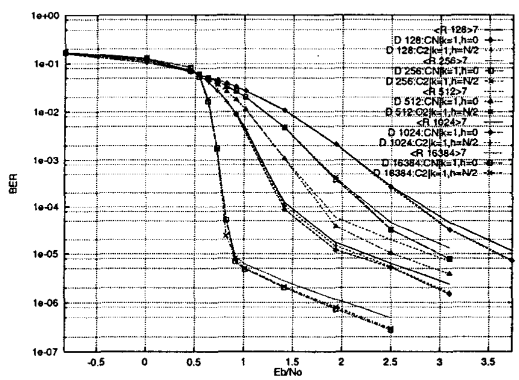

Fig. 1: Simulation results for the new $\mathcal{D}_{N:CN}$ and $\mathcal{D}_{N:C2}$ interleavers for lengths 128, 256, 512, 1024, and 16384 compared with the average performance of 7 random $< \mathcal{R}_N >_7$ interleavers with the same respective lengths.

References

[1] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: turbo-codes," ICC Proceedings, pp. 1064-1070, May 1993.

[2] A. S. Barbulescu and S. S. Pietrobon, "Interleaver design for turbo codes," *Electronics Letters*, vol. 30, no. 25, pp. 2107-2108, December 1994.

[3] S. Dolinar and D. Divsalar, "Weight distributions of turbo codes using random and nonrandom permutations," JPL TDA Progress Report 42-122, pp. 56-65, August 15, 1995.

[4] O. Y. Takeshita and D. J. Costello, "On deterministic linear interleavers for turbo-codes," *Proc. 35th Annual Allerton Conference on Communication, Control and Computing,* pp. 711-712, Sept. 1997.

0-7803-5000-6/98/$10.00 © 1998 IEEE.