NON-PUNCTURED NON-SYSTEMATIC $\frac{1}{2}$-RATE TURBO CODES

J. CASTIÑEIRA MOREIRA, D.M. PETRUZZI, M.C. LIBERATORI and J. C. BONADERO †

† Laboratorio de Comunicaciones, Depto. Electrónica, Facultad de Ingeniería, UNMDP, 7600, Mar del Plata, Arg.
casti@fi.mdp.edu.ar, petruuzzi@fi.mdp.edu.ar, mlibera@fi.mdp.edu.ar, jbona@fi.mdp.edu.ar

Abstract — This paper presents non-punctured non-systematic $\frac{1}{2}$-rate turbo codes designed using Finite State Sequential Machines (FSSMs) that operate over the Finite Field $GF(4)$. It is shown that these schemes do not show convergence problems in their iterative decoding, as it happens to similar schemes defined over the binary Field. Non-systematic turbo codes can be useful for the design of communication systems for which error correction and encryption are two important goals.

A relationship is found between the state transitions structure of the FSSM and the BER performance (or equivalently the form of the EXIT chart) of the designed turbo code. FSSMs defined over $GF(4)$ with all-zero input responses of the form of closed cycles are the best options as constituent encoders of non-punctured non-systematic $\frac{1}{2}$-rate turbo codes. A close relationship is also found between the BER performance and the coefficients that define the structure of those FSSMs.

Keywords — Turbo codes. EXIT charts. Non-systematic coding. Non-linear coding.

I. INTRODUCTION

Binary non-systematic turbo codes were introduced by Banerjee et al. (2005). In a non-systematic turbo code, the message symbols are not transmitted, thus only redundancy symbols appear at the output. Non-systematic turbo codes can be defined in any Finite Field of the form $GF(q)$, where usually $q=2^n$, and $n$ is an integer, and the most common definition is done over the Finite Field $GF(2)$, also known as the binary Field. In the classic form of a turbo code (Berrou et al., 1993) the rate of the code is controlled by applying puncturing, which is essentially performed by means of an output selector that transmit only determined output symbols. In this paper we present non-punctured non-systematic (NP-NS) $\frac{1}{2}$-rate turbo codes defined over $GF(4)$.

NP-NS $\frac{1}{2}$-rate turbo codes defined over the binary Field present convergence problems in their iterative decoding, such that for a suitable NS turbo code defined over this Field there is a need of generating three redundancy outputs (by means of the use of three convolutional encoders, or equivalently three Finite State Sequential Machines (FSSMs)) and of applying puncturing over these three outputs to convert the rate of the code from $\frac{1}{3}$ to $\frac{1}{2}$ (Banerjee et al., 2005). We show in this paper that the use of FSSMs defined over the Finite Field $GF(4)$ allows us the design of NS $\frac{1}{2}$-rate turbo codes that do not need to apply puncturing. The structure is shown in Fig. 1, and it consists on transmitting simply and alternately the corresponding redundancy outputs of two FSSMs.

In this paper we will show that in general, NS $\frac{1}{2}$-rate turbo codes present a slight loss in the Bit Error Rate (BER) performance with respect to their equivalent systematic schemes, in the waterfall region of the BER performance curve of the turbo code. However, Banerjee et al. (2005) shows that NS 1/3-rate schemes present lower floor effects in the BER performance curve of turbo codes with respect to their equivalent systematic schemes. We will concentrate our analysis on the waterfall region of the BER performance curve of NP-NS $\frac{1}{2}$-rate turbo codes defined over $GF(4)$.

In spite of their slight loss in BER performance in the waterfall region, NS $\frac{1}{2}$-rate turbo codes can be used in schemes where not only error-control coding, but also privacy is an important additional aim in the design of communications systems. The use of systematic turbo codes is related to the transmission of the message symbols that appear in the transmitted output, allowing a given eavesdropper to directly read this desired information. This is however not strictly speaking a problem in terms of security, because systematic information can be externally protected by applying an encryption algorithm over this message information. In a NS mode, message symbols are not present at the transmitted output, and this increases the levels of privacy with respect to the systematic mode. An application of NS $\frac{1}{2}$-rate turbo codes in secure communication is given in a previous work of the authors (Castiñeira Moreira et al., 2006). A cryptoanalysis (brute force and differential cryptoanalysis) is performed in that paper, for schemes where coefficients of the FSSMs that are constituent encoders of a turbo code are randomly varied during transmission. Under certain conditions, the scheme is shown to be robust against the above described attacks.

II. NON-SYSTEMATIC $\frac{1}{2}$-RATE TURBO CODES OVER $GF(4)$

A. An Encoder of a Non-Systematic $\frac{1}{2}$-Rate Turbo Code

The structure of a NP-NS $\frac{1}{2}$-rate turbo code defined over $GF(4)$ is seen in Fig. 1. The structure has a random interleaver of size $L=10000$.

The encoder is constructed using FSSMs that operate over $GF(4)$, and include a polynomial $g(x)$ between the two memory units of the FSSM. This polynomial is in general of the form:

$$g(x) = a_0 + a_1x + \ldots + a_mx^m,$$

where $m$ is an integer, and $a_i \in GF(q)$, $i=0, 1, \ldots, m$. 

201