Analysis of serial concatenation schemes for non-binary modulations.

Fabio Fagnani
Dipartimento di Matematica
Politecnico di Torino
C.so Duca degli Abruzzi 24
10129 Torino, Italy
Email: fabio.fagnani@polito.it

Federica Garin
Dipartimento di Matematica
Politecnico di Torino
C.so Duca degli Abruzzi 24
10129 Torino, Italy
Email: federica.garin@polito.it

***Abstract*— In this paper we present a theoretical analysis of serial concatenation schemes for transmission over AWGN channels employing a geometrically uniform constellation having $\mathbb{Z}_m$ as a generating group. Our schemes possess a uniform error property both with respect to the word and to the symbol. This allows to prove exact convergence results on the probability of error. We then show that, as in the binary case, there is a natural concept of distance which, at the design level of the constituent encoders, should be maximized, in order to optimize performances.**

I. Introduction

In this paper we present a rigorous theoretical analysis of a class of serially concatenated codes for transmission over an AWGN channel with input restricted to a geometrically uniform constellation S which admits $\mathbb{Z}_m$ as a generating group. Relevant examples are m–PSK and (if we disregard border effects) m–QAM constellations.

Differently from most of the literature, where such coding schemes are designed in a 'pragmatic' way, coupling a 'good' binary concatenated scheme with a non-binary constellation, we here follow a more 'analytic' strategy and we construct such schemes appositely for the chosen non-binary constellation. In our construction the standard linear binary structure is replaced by a $\mathbb{Z}_m$–module structure.

This viewpoint has already been followed in [8] where a serially concatenated scheme for the 8–PSK modulation was designed using the generating group D_4. The reason for using a non-Abelian group was motivated by the need to obtain a bitwise version of the uniform error property, a fundamental fact which makes possible a theoretical analysis of these codes.

In this paper we take a different approach. We take $\mathbb{Z}_m$ as a generating group and we construct concatenated schemes where the encoders are truncation of $\mathbb{Z}_m$ convolutional codes and the coupling permutation acts on symbols. These schemes satisfy the uniform error property with respect to symbols, which allows a theoretical study of the symbol error probability.

Our contribution is exclusively theoretical. Following [1], we average the symbol error probability of such schemes, for given constituent encoders, over the group of all permutations. This allows to obtain precise asymptotic results when the block length tends to $+\infty$, establishing the classical interleaver gains (Theorems 1 and 2). We emphasize the fact that our derivations are fully rigorous: the upper bounds are obtained along the lines of [1], filling up the missing theoretical passages, and slightly improve the bounds in [9] (there obtained only in the binary case). The lower bound is totally new even in the binary case. Finally, we study the infinitesimal order, with respect to the Battacharija parameter of the channel, of the asymptotic term, introducing an analogous of the effective free distance proposed in [1] in the binary case. We finally notice that, as in the binary case, the range of application of our analysis is for high signal-to-noise ratio.

II. Codes for m–PSK constellation

In this paper, we consider an n–dimensional AWGN channel (with unquantized output) whose inputs are restricted to a geometrically uniform (GU) constellation $S \subset \mathbb{R}^n$ (for details on GU constellations see [7] and [10]).

Moreover, we assume that S admits as generating group $\mathbb{Z}_m$ for some $m \in \mathbb{N}$: this can be equivalently expressed by saying that we can find a one-to-one correspondence $\phi : \mathbb{Z}_m \to S$ such that $\mathrm{d_E}(\phi(i+k), \phi(j+k)) = \mathrm{d_E}(\phi(i), \phi(j))$, where '$\mathrm{d_E}$' denotes Euclidean distance in $\mathbb{R}^n$.

This case has special algebraic properties since $\mathbb{Z}_m$ has a ring structure, and is very important in the applications, as $\mathbb{Z}_m$ is a generating group for the m–PSK constellation.

A $\mathbb{Z}_m$–code $\mathcal{C}$ of length N is any subgroup of $S^N \simeq \mathbb{Z}_m^N$; $\mathcal{C}$ is itself a GU subconstellation of S^N. As a consequence, if such a code is used together with a minimum Euclidean distance decoding rule (fact that will be assumed throughout this paper), it possess the uniform error property, i.e. if X is a r.v. uniformly distributed on $\mathcal{C}$ and $\hat{X}$ is the decoded r.v. we have that $\mathrm{P}_w(e|X = x) := \mathrm{P}(\hat{X} \neq X|X = x)$ does not depend on $x \in \mathcal{C}$. In particular,

$$\mathrm{P}_w(e) := \mathbb{E}_X \mathrm{P}_w(e|X = x) = \mathrm{P}_w(e|X = 0)\,.$$

This property is a key point for the theoretical analysis of error probability.

Exploiting the ring structure of $\mathbb{Z}_m$, we can consider a $\mathbb{Z}_m$–module M and define an $(M, \mathbb{Z}_m)$–encoder as a module

homomorphism $\Sigma : M^K \to \mathbb{Z}_m^N$. We will consider as codes the images of $(M, \mathbb{Z}_m)$–encoders: naturally they are $\mathbb{Z}_m$–codes.

We can now define also the symbol error probability, which depends on the encoder and not only on the code, and which is an extension of the classical definition of bit error probability ('symbol' here means an element of M):

$$\mathrm{P}_s(e) := \frac{1}{K} \sum_{j=1}^{K} \mathrm{P}(\hat{U}_j \neq U_j)\,,$$

where U is the r.v. uniformly distributed on M^K, representing information word, and $\hat{U}$ is the decoded word.

In the setting we are considering, it can be shown that uniform error property holds true also for symbol error probability.

III. Convolutional codes over $\mathbb{Z}_m$

In order to study turbo-like coding schemes, we must consider convolutional codes over $\mathbb{Z}_m$ and their system-theoretic properties; to do so, we will refer mainly to [4], [5], [6] and [11]. We will recall here the most important definitions.

Given a finitely generated $\mathbb{Z}_m$–module M, the set of Laurent series over M is

$$M((D)) := \left\{ \sum_{t=-\infty}^{+\infty} u_t D^t : \exists\, t_0 \in \mathbb{Z} \text{ with } u_t = 0\, \forall t \leq t_0 \right\}.$$

An important submodule of $M((D))$ is the set of rational functions,

$$M(D) := \Big\{ A(D) \in M((D)) : \exists\, P(D) \in M[D, D^{-1}]\,, \quad q(D) \in \mathscr{M} \quad \text{such that} \quad q(D)A(D) = P(D) \Big\},$$

where $M[D, D^{-1}] := \left\{ \sum_{t=-\infty}^{+\infty} u_t D^t \ : \ \exists t_0,\, t_1 \in \mathbb{Z} \text{ such that } u_t = 0\ \forall t \leq t_0 \text{ and } \forall t \geq t_1 \right\}$

is the $\mathbb{Z}_m$–module of Laurent polynomials over M and

$$\mathscr{M} := \left\{ p(D) \in \mathbb{Z}_m[D, D^{-1}] : p(D) = \sum_{t=t_0}^{t_1} p_t D^t,\, p_{t_0} \in \mathbb{Z}_m^* \right\}$$

is the set of the elements in $\mathbb{Z}_m[D, D^{-1}]$ that have an inverse in $\mathbb{Z}_m((D))$.

Given M_1 and M_2 two finitely generated $\mathbb{Z}_m$–modules, we note that $\mathrm{Hom}_{\mathbb{Z}_m}(M_1, M_2)$, the set of homomorphisms from M_1 to M_2, is itself a $\mathbb{Z}_m$–module, so it makes sense to consider $\mathrm{Hom}_{\mathbb{Z}_m}(M_1, M_2)(D)$. The elements of this set act as homomorphisms from $M_1((D))$ to $M_2((D))$, as a formal 'à la Cauchy' product: given $u(D) \in M_1((D))$,

$$c(D) = A(D)u(D)$$

is defined by $c_t := \sum_s A_{t-s} u_s$ (where the summation is on a finite number of terms, as $u(D)$ and $A(D)$ are Laurent series).

In this paper, a 'convolutional encoder' will always mean a rational function $A(D) \in \mathrm{Hom}_{\mathbb{Z}_m}(M_1, M_2)(D)$. As in the binary case, it can be shown that these rational transformations can be represented by a finite-state trellis. This is the main reason for imposing rationality on the definition of convolutional encoders. In the following, without any loss of generality, we will consider only encoders which are causal, i.e. their representation as a Laurent series $\sum_{t=-\infty}^{+\infty} \Sigma_t D^t$ has $\Sigma_t = 0$ for all $t < 0$.

In this paper, we will consider only the case when M_1 and M_2 are free modules, i.e. $M_1 = \mathbb{Z}_m^k$, $M_2 = \mathbb{Z}_m^n$; in this case, $\mathrm{Hom}_{\mathbb{Z}_m}(M_1, M_2)(D)$ is isomorphic to $\mathbb{Z}_m^{k\times n}(D)$ and also to $\mathbb{Z}_m(D)^{k\times n}$.

We want to introduce now for convolutional encoders some concepts that are well known in the classical case.

To do so, we need to recall some definitions concerning Laurent series.

Definition 1: Given $\boldsymbol{u} = \sum_{t=t_0}^{+\infty} u_t D^t \in \mathbb{Z}_m^k((D))$, we define:

- the *support* $\operatorname{supp} \boldsymbol{u} = \{t \in \mathbb{Z} : \boldsymbol{u}_t \neq 0\}$;
- the *Hamming weight* $\mathrm{w_H}(\boldsymbol{u}) = \sum_{t=t_0}^{+\infty} \mathrm{w_H}(\boldsymbol{u}_t)$, where the Hamming weight of the vector $\boldsymbol{u}_t \in \mathbb{Z}_m^k$ is defined, as usual, as the number of its non-zero elements.

Now we can define some properties of particular convolutional encoders, which will be fundamental in the error probability analysis.

Definition 2: Given $\Sigma \in \mathbb{Z}_m^{k\times n}(D)$, we will say that

- Σ is *non catastrophic* if every output with compact support comes from an input with compact support;
- Σ is *recursive* if no output with compact support comes from an input with Hamming weight one.

Both non-catastrophicity and recursiveness are properties which can be effectively checked.

Non catastrophic encoders are characterized by having a sliding-window right inverse (for details see [6]).

For recursiveness, first of all we note that it is sufficient to consider scalar encoders $\Sigma \in \mathbb{Z}_m(D)$: when the encoder is a matrix $\Sigma \in \mathbb{Z}_m(D)^{k\times n}$, we see that Σ is recursive if and only if every row of the matrix has at least one element which is a scalar recursive encoder.

The important fact is that the problem of checking recursiveness can always be reduced to a check for convolutional codes over fields, where it becomes a standard easy problem. For the sake of simplicity, we will illustrate this only in the case $m = 2^a$: in this case the recursiveness of $\Sigma \in \mathbb{Z}_{2^a}((D))$ is equivalent to the recursiveness of $2^{a-1}\Sigma$, which can be interpreted as an element of $\mathbb{Z}_2((D))$ (with the substitution $2^{a-1} \to 1$). In the general case, we have to consider the prime factors decomposition of m, and then test the recursiveness of as many encoders as the number of prime factors.

IV. Serial concatenation schemes over $\mathbb{Z}_m$

As in the classical case, we can define block encoders coming from the convolutional ones and inheriting their properties. This can be done with two techniques: truncation and trellis termination. Given $\Sigma : \mathbb{Z}_m^k((D)) \to \mathbb{Z}_m^n((D))$, the truncated encoder $\Sigma^N : \mathbb{Z}_m^{kN} \to \mathbb{Z}_m^{nN}$ is obtained by considering only

a finite window $[0, N]$ of the encoder's trellis, while the terminated encoder $\tilde{\Sigma}^N : \mathbb{Z}_m^{kN} \to \mathbb{Z}_m^{n(N+\nu)}$, is obtained by forcing the trellis state to return to zero at the end of the encoding.

Given two causal convolutional encoders $\Sigma^o \in \mathbb{Z}_m^{k\times r}(D)$ and $\Sigma^i \in \mathbb{Z}_m^{r\times n}(D)$, we consider their block truncations

$$\Sigma^{o,N} : \mathbb{Z}_m^{kN} \to \mathbb{Z}_m^{rN} \qquad \text{and} \qquad \Sigma^{i,N} : \mathbb{Z}_m^{rN} \to \mathbb{Z}_m^{nN}$$

We couple them in serial concatenation through a permutation σ of length rN (which will act on symbols), as follows:

$$\mathbb{Z}_m^{kN} \xrightarrow{\Sigma^{o,N}} \mathbb{Z}_m^{rN} \xrightarrow{\sigma} \mathbb{Z}_m^{rN} \xrightarrow{\Sigma^{i,N}} \mathbb{Z}_m^{nN} .$$

We formally define the *serial turbo concatenation* by the map composition $\Sigma_\sigma^N := \Sigma^{i,N} \circ \sigma \circ \Sigma^{o,N}$.

Notice that the encoder Σ_σ^N is a $(\mathbb{Z}_m, \mathbb{Z}_m)$–encoder, according to the definition given in Section II. Thus, we can consider its word and symbol error probability, where the symbol is an element of $\mathbb{Z}_m$.

In particular, we analyze the symbol error rate for such schemes, averaged over all possible permutations. Namely we consider the averaged symbol error probability

$$\overline{\mathrm{P}_s(e)}^N := \frac{1}{(rN)!} \sum_{\sigma\in S_{rN}} \mathrm{P}_s(e|\sigma) ,$$

where $\mathrm{P}_s(e|\sigma)$ is the symbol error probability of Σ_σ^N.

A similar concatenation scheme can be built also using terminated instead of truncated encoders. We note that termination is just an addition of redundancy, so the error probability can only be improved by this technique. For this reason, we will consider truncation to upper bound the error probability, and termination for the lower bound, so that all the results will hold true in both cases.

V. Main result: interleaver gain

Following the analysis introduced for the classical case in [1], we study the interleaver gain, i.e. the asymptotic behavior of $\overline{\mathrm{P}_s(e)}^N$ as $N \to \infty$, for fixed (sufficiently small) values of the parameter $\gamma = e^{-RE_S/(4N_0)}$ describing the quality of the channel ($R = k/n$ is the encoder's rate and E_S/N_0 is the signal-to-noise ratio, with E_S the average energy per symbol).

We find out that the most important parameter is the free distance (i.e. the minimum Hamming weight among all codewords excepted the all-zero word) of the outer encoder, that we will denote with d_f^o.

First of all, we have obtained the following upper bound.

Theorem 1 (Upper bound): Assume the following hypotheses on the two convolutional encoders:

- $\Sigma^o \in \mathbb{Z}_m^{k\times r}(D)$ is causal, non-catastrophic with a free distance $d_f^o \geq 2$;
- $\Sigma^i \in \mathbb{Z}_m^{r\times n}(D)$ is causal, non catastrophic and recursive.

Then, there exist a constant $\gamma_0 > 0$ such that, for every $\gamma < \gamma_0$, there exist $A(\gamma) > 0$ such that

$$\overline{\mathrm{P}_s(e)}^N \leq A(\gamma) N^{-\frac{d_f^o+1}{2}} + o\left(N^{-\frac{d_f^o+1}{2}}\right) \quad N \to \infty ,$$

where $\gamma = e^{-RE_S/(4N_0)}$. □

When m is a power of 2, we also have established the following lower bound.

Theorem 2 (Lower bound): If $m = 2^a$ for some $a \in \mathbb{N}$, under the same assumptions on Σ^o and Σ^i made in Theorem 1, there exist $C > 0$ such that

$$\forall N \in \mathbb{N} , \quad \overline{\mathrm{P}_s(e)}^N \geq C N^{-\frac{d_f^o+1}{2}} . \qquad \square$$

Note that, if $m = 2$, the symbol error probability is the usual bit error probability. Hence, in this case, Theorem 1 formally proves the estimation proposed in [1], which is slightly stronger than the result proved in [9]. The lower bound presented in Theorem 2 is instead completely new even in the binary context.

Theorems 1 and 2 together establish the exact rate of convergence of $\overline{\mathrm{P}_s(e)}^N$ and they represent our main result.

The proofs of both theorems are quite technical and will be given elsewhere; here we just give a very short comment on the techniques we have used.

The proof of Theorem 1 follows the idea presented in [1]. Our rigorous results are obtained exploiting the system-theoretic structure of the convolutional encoders over modules and developing some combinatorial arguments similar to those introduced in [3] for parallel concatenations.

For Theorem 2, our result is first established for $m = 2$, using the same technique exploited in [2] to study binary parallel concatenations. The main idea is the following inequality:

$$\forall d > 0, \quad \overline{\mathrm{P}_w(e)}^N \geq p^d \, \mathbb{P}(d_f(\sigma) \leq d) ,$$

with p (the equivocation probability) a constant depending only on the channel and with $d_f(\sigma)$ the free distance of Σ_σ^N. We fix $d = \lfloor d_f^o/2 \rfloor \, d_2^i + w$, where

$$d_2^i := \min_{\boldsymbol{v}:\mathrm{w_H}(\boldsymbol{v})=2} \mathrm{w_E}(\Sigma^i \boldsymbol{v})$$

is the effective free distance of the inner encoder, as defined in [1], and w is a constant needed when d_f^o is odd. With such d, we prove that, for some $c > 0$,

$$\mathbb{P}(d_f(\sigma) \leq d) \geq c \, N^{-\frac{d_f^o+1}{2}+1} .$$

This result is obtained by considering the subset $E_0 \subseteq S_{rN}$ of the permutations which split a fixed outer codeword $\boldsymbol{c}$ with $\mathrm{w_H}(\boldsymbol{c}) = d_f^o$ in couples of inputs for $\Sigma^{i,N}$ each giving an output weighting d_2^i; we also define E_s in the same way but considering a translated $D^s\boldsymbol{c}$. Clearly $\sigma \in E := \bigcup E_s$ implies $d_f(\sigma) \leq d$, so $\mathbb{P}(d_f(\sigma) \leq d) \leq \mathbb{P}(\sigma \in E)$. We complete our proof estimating $\mathbb{P}(\sigma \in E)$ by union-intersection bound and counting arguments.

The theorem is then extended to $m = 2^a$. We consider a binary concatenated scheme obtained restricting Σ^o and Σ^i to elements of $\frac{m}{2}\mathbb{Z}_m \simeq \mathbb{Z}_2$. At first we show that the average word error probability of the binary scheme is a lower bound to $\overline{\mathrm{P}_w(e)}^N$, then we prove that both outer encoders (binary and non-binary) have the same free distance d_f^o.

VI. The effective free distance and examples

A joint asymptotic study of the error probability's behavior as $N \to \infty$ and $\gamma \to 0$ is too complex, but, in order to find some design parameters for the constituent encoders, we can follow the technique introduced in [1]: we let $N \to \infty$ at first, and then we look at the upper bound given by Theorem 1 and we study the infinitesimal order of $A(\gamma)$ for $\gamma \to 0$.

We will show that this infinitesimal order can be characterized as a sort of distance which will be called the effective free distance and will depend on both the inner and outer decoder. Differently from the binary case, where the effective free distance only depends on the inner encoder and is given through a very simple formula, in our setting, the computation of this distance is quite more complicate, and involves both encoders through a combinatorial optimization problem.

We start with some preliminaries. First of all, not only Hamming weight is involved, but also Euclidean distances. In particular, we will use the *normalized Euclidean weight* $\mathrm{w_E}(\boldsymbol{u})$ of a vector $\boldsymbol{u} \in \mathbb{Z}_m^N$. It makes sense to give this definition only after having fixed a GU constellation $S \subset \mathbb{R}^n$ with generating group $\mathbb{Z}_m$, and a map $\phi : \mathbb{Z}_m \to S$ as introduced in Section II. Using again '$\mathrm{d_E}$' to indicate the Euclidean distance in $\mathbb{R}^n$, we can define

$$\mathrm{w_E}(\boldsymbol{u}) := \frac{1}{E_S} \sum_{t=0}^{N} \mathrm{d_E}\left(\phi(\boldsymbol{u}_t),\, \phi(0)\right)^2 .$$

We also need the definition of the *weights vector* of $\boldsymbol{u} \in \mathbb{Z}_m^N$: using '$\#A$' as a notation for the cardinality of a set A, we define $\mathbf{w}(\boldsymbol{u}) := \boldsymbol{w} \in \mathbb{N}^{m-1}$ such that, for all $j \in \mathbb{Z}_m \setminus \{0\}$,

$$\boldsymbol{w}_j = \#\left\{i \in \{1, \cdots N\} : \boldsymbol{u}_i = j\right\} .$$

Given a convolutional encoder $\Sigma \in \mathbb{Z}_m^{k \times n}$, we define an *error event* for Σ with activity window $[t_0, t_1]$ as an input word $\boldsymbol{u} \in \mathbb{Z}_m^k((D))$ such that $\boldsymbol{u}_t = 0$ for all $t < t_0$ and $t > t_1$ and the corresponding state sequence (sequence of states in the trellis) is always non-zero in $[t_0, t_1]$ and is zero everywhere else.

If we consider Σ^N a block truncation of Σ, we will say that an error event $\boldsymbol{u}$ for Σ is a *complete error event* for Σ^N if the activity window is $[t_0, t_1] \subseteq [0, N]$ and is an *incomplete error event* if $t_1 > N$ and so the state at time N is not zero.

Now we consider our serially concatenation scheme

$$\mathbb{Z}_m^{kN} \xrightarrow{\Sigma^{o,N}} \mathbb{Z}_m^{rN} \xrightarrow{\sigma} \mathbb{Z}_m^{rN} \xrightarrow{\Sigma^{i,N}} \mathbb{Z}_m^{nN}$$

and we introduce two subsets of $\mathbb{N}^{m-1}$ whose definition involves the Hamming weights of outer codewords:

$$W_f := \left\{\mathbf{w}(\boldsymbol{v}) : \boldsymbol{v} \in \Sigma^o\left(\mathbb{Z}_m^k((D))\right) \text{ and } |\mathrm{w_H}(\boldsymbol{v})| = d_f^o\right\} \text{ and}$$

$$W_f^{(1)} := \left\{\mathbf{w}(\boldsymbol{v}) : \boldsymbol{v} \in \Sigma^o\left(\mathbb{Z}_m^k((D))\right) \text{ and } |\mathrm{w_H}(\boldsymbol{v})| = d_f^o + 1\right\} .$$

Given $\boldsymbol{w} \in \mathbb{N}^{m-1}$ we define, with respect to the inner encoder:

$$\mathrm{h}(\boldsymbol{w}) := \min\Big\{\mathrm{w_E}(\Sigma^{i,N}\boldsymbol{v}) :\ \boldsymbol{v} \in \mathbb{Z}_m^{rN},\ \mathbf{w}(\boldsymbol{v}) = \boldsymbol{w} \text{ and } \boldsymbol{v} \text{ is a complete error event for } \Sigma^{i,N}\Big\};$$

and we define $\tilde{\mathrm{h}}(\boldsymbol{w})$ in the same way except that we ask $\boldsymbol{v}$ to be an *incomplete* error event.

By convention, we will consider $\mathrm{h}(\boldsymbol{w}) = +\infty$ when no complete error event $\boldsymbol{v}$ with $\mathbf{w}(\boldsymbol{v}) = \boldsymbol{w}$ exists.

When d_f^o is even, we define the effective free distance as

$$h^* := \min\Big\{\mathrm{h}(\boldsymbol{w}_1) + \ldots + \mathrm{h}(\boldsymbol{w}_{d_f^o/2}) :\ \sum_{i=1}^{d_f^o/2} \boldsymbol{w}_i \in W_f \text{ and } |\boldsymbol{w}_i| = 2\ \forall i\Big\}. \quad (1)$$

If d_f^o is odd, the definition is a bit more complicated. We first define:

$$h_1^* := \min\Big\{\mathrm{h}(\boldsymbol{w}_1) + \ldots + \mathrm{h}(\boldsymbol{w}_{(d_f^o-1)/2}) + \tilde{\mathrm{h}}(\bar{\boldsymbol{w}}) :\ \sum_{i=1}^{(d_f^o-1)/2} \boldsymbol{w}_i + \bar{\boldsymbol{w}} \in W_f,\ |\bar{\boldsymbol{w}}| = 1 \text{ and } |\boldsymbol{w}_i| = 2\ \forall i \le \tfrac{d_f^o-1}{2}\Big\};$$

$$h_2^* := \min\Big\{\mathrm{h}(\boldsymbol{w}_1) + \ldots + \mathrm{h}(\boldsymbol{w}_{(d_f^o-3)/2}) + \mathrm{h}(\bar{\boldsymbol{w}}) :\ \sum_{i=1}^{(d_f^o-3)/2} \boldsymbol{w}_i + \bar{\boldsymbol{w}} \in W_f,\ |\bar{\boldsymbol{w}}| = 3 \text{ and } |\boldsymbol{w}_i| = 2\ \forall i \le \tfrac{d_f^o-3}{2}\Big\};$$

$$h_3^* := \min\Big\{\mathrm{h}(\boldsymbol{w}_1) + \ldots + \mathrm{h}(\boldsymbol{w}_{(d_f^o+1)/2}) :\ \sum_{i=1}^{(d_f^o+1)/2} \boldsymbol{w}_i \in W_f^{(1)} \text{ and } |\boldsymbol{w}_i| = 2\ \forall i \le \tfrac{d_f^o+1}{2}\Big\}.$$

Now we can define, for odd d_f^o, the effective free distance as

$$h^* := \min\left\{h_1^*,\, h_2^*,\, h_3^*\right\} . \quad (2)$$

Finally, after all these definitions, we can state our result.

Theorem 3: The coefficient $A(\gamma)$ defined in Theorem 1 has infinitesimal order h^* when $\gamma \to 0$, where h^* is defined by Equation (1) if d_f^o is even and (2) if it is odd. □

In order to clarify the definition of h^* given above, we present here two very simple examples, where the minimization problem can be solved by hand by exhaustive enumeration. In both following examples we will consider the encoding scheme

$$\mathbb{Z}_4^N \xrightarrow{\Sigma^{o,N}} \mathbb{Z}_4^{2N} \xrightarrow{\sigma} \mathbb{Z}_4^{2N} \xrightarrow{\Sigma^{i,N}} \mathbb{Z}_4^{2N}$$

and we will use the 4–PSK constellation with average energy $E_S = 1$; we have $\mathrm{d_E}(\phi(1),\, \phi(0))^2 = \mathrm{d_E}(\phi(3),\, \phi(0))^2 = 2$ and $\mathrm{d_E}(\phi(2),\, \phi(0))^2 = 4$.

Example 1 (even d_f^o): $\Sigma^o = [1, 1]$ and $\Sigma^i = \begin{bmatrix} \frac{1}{1+3D} & 0 \\ 0 & \frac{1}{1+3D} \end{bmatrix}$.

We have $d_f^o = 2$ and $W_f = \{[2, 0, 0],\, [0, 2, 0],\, [0, 0, 2]\}$.

Note that $\frac{1}{1+3D} = \sum_{t \ge 0} D^t$.

Thus, we clearly have $\mathrm{h}([2, 0, 0]) = +\infty$, because all inputs for the inner encoder of the kind $\boldsymbol{v} = [D^{t_1} + D^{t_2}, 0]$, $\boldsymbol{v} = [D^{t_1}, D^{t_2}]$ or $\boldsymbol{v} = [0, D^{t_1} + D^{t_2}]$ produce outputs which do not have compact support.

For the same reason, $\mathrm{h}([0, 0, 2]) = +\infty$.

Finally, $\mathrm{h}([0,2,0]) = 4$, because $(2+2D)\frac{1}{1+3D} = 2$.
We conclude that $h^* = 4$. □

Example 2 (odd d_f^o): $\Sigma^o = [1,\ 1+3D]$, $\Sigma^i = \begin{bmatrix} \frac{1}{1+3D} & 0 \\ 0 & \frac{1}{1+3D} \end{bmatrix}$.

Here $d_f^o = 3$ and $W_f = \{[2,0,1],\ [0,3,0],\ [1,0,2]\}$.
Now we also need $W_f^{(1)} = \{[3,0,1],\ [0,4,0],\ [1,0,3]\}$.

By enumeration of all cases, we calculate:

$$\begin{aligned} h_1^* &= \min\{\mathrm{h}(\boldsymbol{w}) + \tilde{\mathrm{h}}(\bar{\boldsymbol{w}}) : \boldsymbol{w} + \bar{\boldsymbol{w}} \in W_f,\ |\bar{\boldsymbol{w}}| = 1,\ |\boldsymbol{w}| = 2\} \\ &= \mathrm{h}([0,2,0]) + \tilde{\mathrm{h}}([0,1,0]) = 4 + 4 = 8\,; \\ h_2^* &= \min\{\mathrm{h}(\bar{\boldsymbol{w}}) : \bar{\boldsymbol{w}} \in W_f,\ |\bar{\boldsymbol{w}}| = 3\} = +\infty\,; \\ h_3^* &= \min\{\mathrm{h}(\boldsymbol{w}_1) + \mathrm{h}(\boldsymbol{w}_2) : \boldsymbol{w}_1 + \boldsymbol{w}_2 \in W_f^{(1)}, |\boldsymbol{w}_1| = |\boldsymbol{w}_2| = 2\} \\ &= \mathrm{h}([0,2,0]) + \mathrm{h}([0,2,0]) = 4 + 4 = 8\,. \end{aligned}$$

Finally we have
$h^* = \min\{h_1^*,\ h_2^*,\ h_3^*\} = 8$. □

In the binary case, the expression of h^* becomes much simpler. First of all, in this case Euclidean normalized weight is directly proportional to Hamming weight: $\mathrm{w_E}(\boldsymbol{u}) = 4E_b \mathrm{w_H}(\boldsymbol{u})$. In addition, the elements of W_f and $W_f^{(1)}$ are natural numbers, not vectors.

When d_f^o is even, we simply have $h^* = \frac{1}{2} d_f^o d_2^i$. When d_f^o is odd, we need two more definitions:

$$d_3^i := \min_{\boldsymbol{v}:\mathrm{w_H}(\boldsymbol{v})=3} \mathrm{w_E}(\Sigma^i \boldsymbol{v})\,,\ d_1^i := \min_{\boldsymbol{v}:\mathrm{w_H}(\boldsymbol{v})=1} \mathrm{w_E}(\Sigma^{i,N} \boldsymbol{v})\,.$$

We find that

- $h_1^* = \frac{d_f^o - 1}{2} d_2^i + d_1^i$;
- $h_2^* = \frac{d_f^o - 3}{2} d_2^i + d_3^i$;
- $h_3^* = \frac{d_f^o + 1}{2} d_2^i$.

We note that $h_1^* \le h_3^*$ always holds true: $d_1^i \le d_2^i$, because every complete error event of weight 2 can be seen as the sum of two incomplete error events of weight 1.

On the contrary, the following two examples show that no general ordering holds true for h_1^* and h_2^*.

Example 3 ($h_1^* < h_2^*$): $\Sigma^i = \left[1,\ \frac{1}{1+D}\right]$.

As $\frac{1}{1+D} = \sum_{t \ge 0} D^t$, we have $d_2^i = 4 \cdot 3$ and $d_3^i = +\infty$, so, considering that $d_1^i \le d_2^i$, we have $d_3^i > d_2^i + d_1^i$ and then $h_2^* > h_1^*$. □

Example 4 ($h_1^* > h_2^*$): $\Sigma^i = \left[1,\ \frac{1}{1+D+D^2}\right]$

As $\frac{1}{1+D+D^2} = \frac{1+D}{1-D^3} = (1+D)\sum_{t \ge 0} D^{3t}$, here we have $d_2^i = 4 \cdot 4$, $d_3^i = 4 \cdot 4$ and $d_1^i = 4 \cdot 2$.
Hence $d_3^i < d_2^i + d_1^i$ and then $h_2^* < h_1^*$. □

Finally we can state that

$$h^* = \begin{cases} \frac{1}{2}\, d_f^o\, d_2^i & \text{if } d_f^o \text{ is even} \\ \\ \frac{d_f^o - 3}{2} d_2^i + \min\left\{d_3^i,\ d_2^i + d_1^i\right\} & \text{if } d_f^o \text{ is odd} \end{cases}$$

Note that this result coincides with the exponent proposed in [1], except that we have here the additional term with d_1^i, as we are considering truncated encoders, while in [1] terminated encoders are considered and so no incomplete error event can appear.

VII. Conclusion

We have formally proved the interleaver gain for serial turbo-like concatenations of convolutional encoders over free $\mathbb{Z}_m$–modules, and we have proposed an important design parameter to be maximized, the effective free distance, which should be particularly relevant in the high signal/noise ratio range.

As the binary classical scheme is a particular case of our setting, our result also proves the estimation proposed in [1]. Anyhow, even for the binary case, some questions are still open: it would be interesting to find results averaged only over subsets of all the permutations, in order to find some indications on how to choose good interleavers. In the non-binary case, many generalizations can be done: other rings can be chosen instead of $\mathbb{Z}_m$ (this will make more difficult the system-theoretic study of convolutional encoders) and non-free modules can be studied (this will complicate the combinatorics).

In addition, we are working on simulations, which will show if the parameters found in our theoretical analysis under maximum likelihood decoding correctly describe error probability in the applications, where sub-optimal SISO iterative algorithm is used.

References

[1] S. Benedetto, D. Divsalar, G. Montorsi and F. Pollara, "Serial Concatenation of Interleaved Codes: Performance Analysis, Design, and Iterative Decoding", *IEEE Trans. on Information Theory*, vol. 44, no. 3, pp. 909-926, May 1998.

[2] F. Fagnani, "A performance of parallel concatenated coding schemes", internal report no. 31, DIMAT, Politecnico di Torino, November 2004.

[3] F. Fagnani, R. Garello, B. Scanavino and S. Zampieri, "Analysis and design of geometrically uniform parallel concatenated coded modulation schemes" *submitted to IEEE Trans. on Information Theory*.

[4] F. Fagnani and S. Zampieri, "Convolutional codes over finite Abelian groups: some basic results", in *Codes, Systems and Graphical Models*, B. Marcus and J. Rosenthal editors, IMA Volumes in Mathematics and its Applications, vol. 123, pp. 327-346, Springer Verlag, Berlin, 2000.

[5] F. Fagnani and S. Zampieri, "System-Theoretic Properties of Convolutional Codes Over Rings", *IEEE Trans. Information Theory*, vol. 47, no. 6, pp. 2256-2274, September 2001.

[6] F. Fagnani and S. Zampieri, "Minimal and systematic convolutional codes over finite Abelian groups", *Elsevier – Linear Algebra and its Applications*, no. 378, pp. 31-59, 2004.

[7] G. D. Forney, Jr., "Geometrically Uniform Codes", *IEEE Trans. on Information Theory*, vol. 37, pp. 1241-1260, 1991.

[8] R. Garello, G. Montorsi, S. Benedetto, D. Divsalar and F. Pollara, "Labelings and Encoders With the Uniform Bit Error Property With Applications to Serially Concatenated Trellis Codes", *IEEE Trans. on Information Theory*, vol. 48, pp. 123-136, 2002.

[9] H. Jin and R. J. McEliece, "Coding theorems for turbo code ensembles" *IEEE Trans. on Information Theory*, vol. 48 (6), pp. 1451–1461, 2002.

[10] H.-A. Loeliger, "Signal Sets Matched To Groups", *IEEE Trans. on Information Theory*, vol. 37, no. 6, pp. 1675-1679, November 1991.

[11] H.-A. Loeliger and T. Mittelholzer, "Convolutional Codes Over Groups", *IEEE Trans. on Information Theory*, vol. 42, no. 6, pp. 1660-1686, November 1996.