Nonlinear Analysis of the Iterative Decoding of Parallel Concatenated Convolutional Codes

Frederic Lehmann and Gian Mario Maggio, *Senior Member, IEEE*

***Abstract*—In this correspondence, we introduce a simple one-dimensional (1-D) nonlinear map to describe the iterates of the bit-error rate (BER) of parallel-concatenated convolutional codes (PCCC) on the binary-input Gaussian channel. A lower bound on this map is derived based upon the weight enumerator of the constituent codes, thus enabling the characterization of the dynamics of the decoder in terms of fixed points, along with the associated stability analysis.**

***Index Terms*—Concatenated codes, density evolution, Gaussian densities, iterative decoding, nonlinear dynamics, stability condition.**

I. Introduction

Concatenated codes were first introduced by Elias [1] and Forney [2], as a class of powerful codes with high error-correcting capabilities. Low decoding complexity was achieved with suboptimum sequential hard-input/hard-output decoding of the constituent codes. The introduction of turbo decoding, which consists of iterative soft-input/soft-output (SISO) decoding of the constituent codes followed by the exchange of extrinsic information [3], [4], later showed that decoding performances close to the Shannon limit can be obtained with concatenated codes.

The very general framework of codes on graphs [5] enables to interpret the exchange of extrinsic information as a message-passing algorithm, updating the likelihood of variables in a graph. The first attempt to analyze message-passing decoding taking a dynamical system point of view is found in [6]. Recently, several techniques have been proposed to analyze iterative decoding by tracking the density of the extrinsic information exchanged by the constituent decoders. This procedure, known as *density evolution*, was originally introduced for low-density parity-check (LDPC) codes [7], and later extended to turbo codes [8]. The rationale behind density evolution is that for codes with large block lengths, the concentration theorem [7] ensures that the performance of a particular graph chosen at random may be assimilated to the average performance of the corresponding cycle-free graph, i.e., the messages exchanged at every iteration are independent and identically distributed (i.i.d.) random variables. Moreover, the density of the extrinsic information is symmetric ($f(x) = f(-x)e^x$). A general property of density evolution is the existence of an interesting threshold effect. If the channel SNR is below a certain threshold, the iterates of the bit-error rate (BER) converge to a fixed point which has in general an extremely large value, that makes it useless in practice.

In order to get a closed-form analysis [9] and/or avoid numerical evaluation of densities using Monte Carlo techniques [8], a convenient approximation introduced by Wiberg [10] considers that the extrinsic information is Gaussian distributed.

In this work, we propose an analysis of the iterative decoding of parallel-concatenated convolutional codes (PCCC) based on matching the BER at the output of the SISO decoders with the error rate corresponding to Gaussian distributed log-likelihood ratios, as originally suggested in [11]. The BER of the constituent decoders can be obtained by Monte Carlo simulation as in [11]. The drawback of this purely numerical method is that the dynamics of the iterative decoder cannot be related to the parameters of the constituent encoders. Therefore, we calculate a tight lower bound on the BER of the constituent codes when the extrinsic information has a large absolute value, based on weight enumerating techniques. This alternative tool to analyze iterative decoders is the main original contribution of this correspondence. We also emphasize the similarity of our work with [12], although our BER calculation is based on [13].

This correspondence is organized as follows. In Section II, we briefly review the principles of PCCC and iterative decoding. Section III presents our analysis of the iterative decoding based on the BER. Then, in Section IV, we investigate the nonlinear dynamics of the PCCC presented in Section II as a function of the parameters of the constituent codes, the channel signal-to-noise ratio (SNR), and the interleaver size. Finally, in Section V, we discuss the limitations of the proposed approach.

II. Parallel-Concatenated Convolutional Codes (PCCC) and Iterative Decoding

A. Parallel Concatenated Convolutional Codes (PCCC)

For the sake of simplicity, we restrict ourselves to PCCC involving two constituent convolutional codes separated by an interleaver. We assume that the trellis of each constituent is terminated. We let k, I, and R denote the number of information bits, the size of the interleaver, and the coding rate of the PCCC, respectively. Throughout the correspondence, binary linear codes are employed and the channel is the binary-input Gaussian channel (binary $0 \rightarrow +1$, binary $1 \rightarrow -1$); we let σ denote the standard deviation of the noise. Therefore, without loss of generality, we can assume that the all-0 codeword is transmitted.

PCCCs [14] are illustrated in Fig. 1(a) and (b). The k information bits are permuted by a random interleaver, then both nonpermuted and permuted bits are fed to the first and second constituent encoders, respectively. If the constituent codes are nonrecursive nonsystematic, the codeword is formed by multiplexing the outputs of the constituent encoders as shown in Fig. 1(a). If the constituent codes are recursive systematic, the codeword is formed by multiplexing the information bits with the redundancy produced by the constituent encoders, as shown in Fig. 1(b). Although it is already a well-known fact that iterative decoding performs badly for nonrecursive nonsystematic PCCC [15], we would like to reproduce this result using our method.

B. Iterative Decoding

A generic iterative decoder is illustrated in Fig. 2. The decoding is performed iteratively using two decoders denoted by SISO1 and SISO2, respectively. We consider only *maximum a posteriori* (MAP) decoding, although this is not always practically feasible. SISO1 uses channel observations Z and *a priori* information A_1 in the form of log-likelihood ratios to generate the *a posteriori* bit-by-bit log-likelihood ratios L_1. The extrinsic information is then defined as $E_1 = L_1 - Z - A_1$. After interleaving, E_1 is used as *a priori* information A_2, in conjunction with Z, by SISO2 to generate the *a posteriori* bit-by-bit log-likelihood ratios L_2. The extrinsic information is

Manuscript received August 22, 2002; revised February 23, 2005. This work was sponsored by STMicroelectronics, Inc, Advanced System Technology (AST) group. The material in this correspondence was presented in part at the IEEE International Symposium on Information Theory and Its Applications, Xi'an, China, October 2002.

F. Lehmann is with GET/INT, Department CITI, F-91011 Evry, France (e-mail: frederic.lehmann@int-evry.fr).

G. M. Maggio is with STMicroelectronics, Inc., Advanced System Technology (AST), San Diego, CA 92121 USA and with the Center for Wireless Communications (CWC), University of California, San Diego, La Jolla, CA 92093-0407 USA (e-mail: gian-mario.maggio@st.com; maggio@ieee.org).

Communicated by R. Urbanke, Associate Editor for Coding Techniques.

Digital Object Identifier 10.1109/TIT.2005.847751

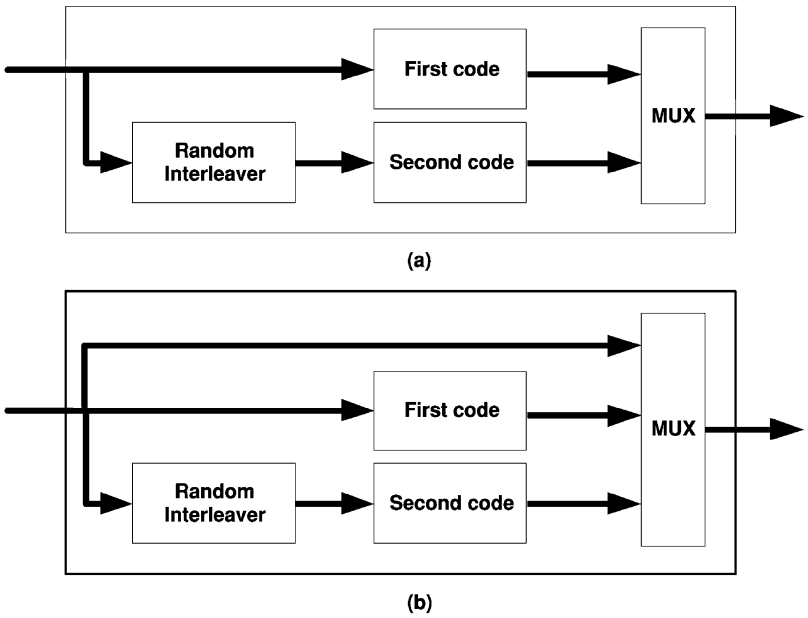

Fig. 1. Concatenated codes. (a) Nonrecursive nonsystematic PCCC. (b) Recursive systematic PCCC.

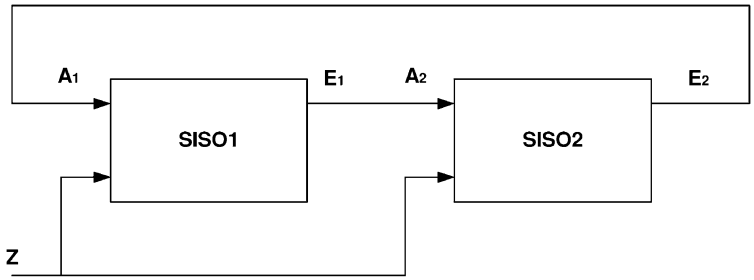

Fig. 2. Block diagram of the iterative decoder of a convolutional code.

then defined as $E_2 = L_2 - Z - A_2$, and is used as *a priori* information for SISO1 after deinterleaving. SISO1 and SISO2 correspond to the decoding of the first and second constituent code of the PCCC, respectively. Throughout the correspondence, we will assume that all the quantities exchanged by the decoder are in the form of log-likelihood ratios and can be modeled as i.i.d. random variables having a symmetric Gaussian distribution [7].

Remark 2.1: From the viewpoint of dynamical system theory, the iterative decoding system may be seen as a closed-loop dynamical system, where SISO1 and SISO2 act as the (nonlinear) constituent blocks in the corresponding open-loop system.

III. Nonlinear Analysis of the Iterative Decoding of PCCC

For simplicity, we make the standard assumption that the considered PCCC is formed by two identical constituent codes. Let $2x$ be equal to the mean of the *a priori* log-likelihood ratios at the input of either SISO. Let $f_{(1/\sigma^2)}$ and f_x be the density of the channel and *a priori* log-likelihood ratios at the input of a decoder, respectively. Then we have

$$f_{\frac{1}{\sigma^2}}(t) = \frac{q\left(\frac{t-\frac{2}{\sigma^2}}{2/\sigma}\right)}{2/\sigma}$$

$$f_x(t) = \frac{q\left(\frac{t-2x}{2\sqrt{x}}\right)}{2\sqrt{x}}$$

where $q(t) = (1/\sqrt{2\pi})e^{-t^2/2}$. We define $P(x,\sigma)$ as the post-decoding BER of a constituent code, assuming that the densities of the channel and *a priori* log-likelihood ratios are $f_{(1/\sigma^2)}$ and f_x, respectively. As mentioned before, numerical values of $P(x,\sigma)$ can be obtained through Monte Carlo simulation. The post-decoding log-likelihood ratio is the sum of the *a priori* and extrinsic log-likelihood ratios plus the channel log-likelihood ratio if available, so its density p is also a symmetric Gaussian defined solely by the mean m and we have

$$P(x,\sigma) = \int_{-\infty}^{0} p(t)dt = Q\left(\sqrt{\frac{m}{2}}\right)$$

where $Q(x) = \int_x^{+\infty} q(t)dt$. Therefore, the mean of the extrinsic log-likelihood ratio is given by

$$2([Q^{-1}(P(x,\sigma))]^2 - x)$$

for a nonrecursive nonsystematic constituent encoder (since channel log-likelihood ratios are not available) and by

$$2\left([Q^{-1}(P(x,\sigma))]^2 - \frac{1}{\sigma^2} - x\right)$$

for a recursive systematic constituent encoder (since channel log-likelihood ratios are available). It follows that the BER at the output of either SISO can be described, at each half iteration l, by $y_l = h(y_{l-1},\sigma)$, where h is the nonlinear map defined by

$$h(y,\sigma) = P\left([Q^{-1}(y)]^2 - P^{-1}(y,\sigma),\sigma\right) \quad (1)$$

for nonrecursive nonsystematic constituent encoders and by

$$h(y,\sigma) = P\left([Q^{-1}(y)]^2 - \frac{1}{\sigma^2} - P^{-1}(y,\sigma),\sigma\right) \tag{2}$$

for recursive systematic constituent encoders. The inverse function P^{-1} is well defined since P is bijective. The fixed points of the map for $y > 0$ are the solutions of $h(y,\sigma) = y$, which is equivalent to

$$[Q^{-1}(y)]^2 - 2P^{-1}(y,\sigma) = 0$$

for nonrecursive nonsystematic constituent encoders and to

$$[Q^{-1}(y)]^2 - 2P^{-1}(y,\sigma) = \frac{1}{\sigma^2}$$

for recursive systematic constituent encoders.

Remark 3.1: By definition of the noise threshold σ^*, when $\sigma \leq \sigma^*$, the iterates of the BER, y_l, starting at $y_0 = Q(1/\sigma)$ reach 0 without getting stuck in any other fixed point. We suggest that a possible method to evaluate σ^* consists of finding the highest value of σ for which $h(y,\sigma) = y$ admits one solution only, namely 0. Since the value of the fixed point responsible for the threshold effect is typically close to y_0, a valid expression of $P(x,\sigma)$ at high BER (evaluated numerically through Monte Carlo simulation, for instance) is required.

Theorem 3.2: Assume that $P(x,\sigma)$ is not available, but that we have a bijective lower bound $P_l(x,\sigma)$ which is a decreasing function of x such that $P_l(x,\sigma) \leq P(x,\sigma), \forall x \geq 0$. Let the corresponding map be defined by

$$h_l(y,\sigma) = P_l([Q^{-1}(y)]^2 - P_l^{-1}(y,\sigma),\sigma)$$

for nonrecursive nonsystematic constituent encoders and by

$$h_l(y,\sigma) = P_l\left([Q^{-1}(y)]^2 - \frac{1}{\sigma^2} - P_l^{-1}(y,\sigma),\sigma\right)$$

for recursive systematic constituent encoders. It follows that $h_l(y,\sigma) \leq h(y,\sigma), \forall y$.

The proof is postponed to Appendix A.

IV. Nonlinear Dynamics of the Iterative Decoding of PCCC

For each PCCC presented in Section II, we study the dynamics of the iterative decoding. Lower bounds on the BER based on weight enumerating techniques enable to establish a link between the decoding process and the parameters of the constituent codes.

A. Nonrecursive Nonsystematic PCCC

A lower bound on the BER of information bits for nonrecursive nonsystematic terminated convolutional codes is obtained as

$$P_l(x,\sigma) = Q\left(\sqrt{x + \frac{d_{\min}}{\sigma^2}}\right) \tag{3}$$

where $d_{\min}$ denotes the free distance of the code.

Proof: Since the all-zero codeword is sent, let $\boldsymbol{i}^0 = (i_1^0,\ldots,i_k^0)$ and $\boldsymbol{c}^0 = (c_1^0,\ldots,c_n^0)$ be the corresponding information sequence and transmitted codeword. Let $\boldsymbol{c}^{w,d} = (c_1^{w,d},\ldots,c_n^{w,d})$ be any other codeword with information weight w and weight d, and $\boldsymbol{i}^{w,d} = (i_1^{w,d},\ldots,i_k^{w,d})$ be the corresponding information sequence. Since each SISO performs MAP decoding, the probability of confusing $\boldsymbol{c}^0$ with $\boldsymbol{c}^{w,d}$ is

$$P_{w,d} = \Pr\left(\ln\frac{P(\boldsymbol{y}\,|\,\boldsymbol{c}^0)P(\boldsymbol{c}^0)}{P(\boldsymbol{y}\,|\,\boldsymbol{c}^{w,d})P(\boldsymbol{c}^{w,d})} < 0\right)$$

where $\boldsymbol{y} = (y_1,\ldots,y_n)$ is the received sequence, given that $\boldsymbol{c}^0$ was transmitted.

On the binary-input Gaussian channel, the likelihood of $\boldsymbol{c}^0$ and $\boldsymbol{c}^{w,d}$ is calculated by a SISO as

$$P(\boldsymbol{y}\,|\,\boldsymbol{c}^0)P(\boldsymbol{c}^0) = C\exp\left[\sum_{j=1}^{n}\left(1-2c_j^0\right)\frac{y_j}{\sigma^2} + \sum_{j=1}^{k}\left(1-2i_j^0\right)A_j/2\right]$$

$$P(\boldsymbol{y}\,|\,\boldsymbol{c}^{w,h})P(\boldsymbol{c}^{w,h}) = C\exp\left[\sum_{j=1}^{n}\left(1-2c_j^{w,h}\right)\frac{y_j}{\sigma^2} + \sum_{j=1}^{k}\left(1-2i_j^{w,h}\right)A_j/2\right]$$

where C is a constant and $\boldsymbol{A} = (A_1,\ldots,A_k)$ is the vector of *a priori* log-likelihood ratios. It follows that

$$\ln\frac{P(\boldsymbol{y}\,|\,\boldsymbol{c}^0)P(\boldsymbol{c}^0)}{P(\boldsymbol{y}\,|\,\boldsymbol{c}^{w,h})P(\boldsymbol{c}^{w,h})} = 2\left(\sum_{j:c_j^{w,d}=1}\frac{y_j}{\sigma^2} + \sum_{j:i_j^{w,d}=1}A_j/2\right).$$

This expression is a random variable with a symmetric Gaussian density and mean $2(wx + d/\sigma^2)$. We recall that for a PCCC, $\boldsymbol{A}$ is zero for redundancy bits and a Gaussian symmetric random variable with mean $2x$ for information bits. Therefore, $P_{w,d} = Q(\sqrt{wx + d/\sigma^2})$. Let $A_{w,d}$ represent the number of codewords in the terminated constituent code with information weight w and weight d. A lower bound on the bit-error probability of the information bits is obtained as the first term of the union bound ($w = 1$)

$$P_l(x,\sigma) = \sum_{d\geq d_{\min}}\frac{1}{k}A_{1,d}Q\left(\sqrt{x+\frac{d}{\sigma^2}}\right).$$

Noting that for a terminated nonrecursive nonsystematic convolutional code, $A_{1,d_{\min}} = k$ and $A_{1,d} = 0$ for $d > d_{\min}$, the desired result follows. It is also interesting to note that this lower bound is tight when the value of x is large. □

Applying Theorem 3.2, we immediately obtain a lower bound on the map describing the iterative decoder as

$$h_l(y,\sigma) = Q\left(\sqrt{\frac{2d_{\min}}{\sigma^2}}\right) \tag{4}$$

which is both independent of y and tight for small values of y. Consequently, the iterative decoding trajectory will reach a stable fixed point at $Q(\sqrt{2d_{\min}/\sigma^2})$. Note that the performances of iteratively decoded nonrecursive nonsystematic PCCC are only 3 dB better than the performances of the constituent codes. This explains why nonrecursive nonsystematic constituent codes make poor turbo codes, as shown previously in [15].

Example 4.1: We consider terminated rate-$1/2$ nonrecursive nonsystematic convolutional constituent codes with generators $g_0(D) = 1 + D + D^2$ and $g_1(D) = 1 + D^2$ and $k = 1024$ information bits. The resulting turbo code is a rate-$1/4$ PCCC with interleaver size $I = 1024$. For $E_b/N_0 = 5$ dB, Fig. 3, illustrates the BER $P(x,\sigma)$ obtained through Monte Carlo simulation (solid) along with the lower bound (3) (dash-dotted). Note the tightness of the lower bound when $x > 5$. The turbo decoding trajectory (simulated average BER versus average *a priori* information) is marked by circles. As expected, starting from

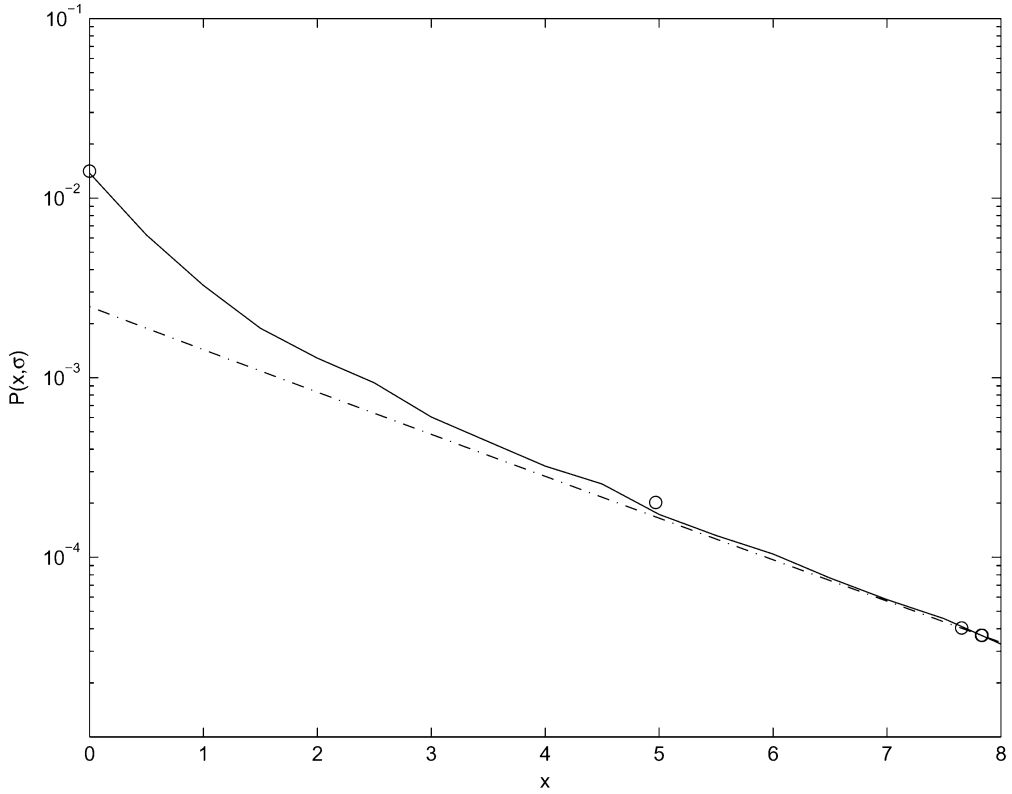

Fig. 3. $P(x,\sigma)$ at E_b/N_0 =5 dB for a PCCC with rate-$1/2$ state-4 nonrecursive nonsystematic convolutional code (solid line) versus the corresponding lower bound (dash-dotted line).

no *a priori* information ($x = 0$), the BER is decreasing as the number of iterations increases until it reaches a fixed point at 3.55×10^{-5} which is consistent with (4), since $d_{\min} = 5$.

Fig. 4 illustrates the iterative decoding map $h(y,\sigma)$ defined by (1) (solid) along with the lower bound (4) (dash-dotted). It can be seen that the iterative decoding trajectory (circles) is bouncing back and forth between the curves $z = h(y,\sigma)$ (solid) and $z = y$ (dashed).[1]

B. Recursive Systematic PCCC

A lower bound on the BER of information bits for recursive systematic terminated convolutional codes is obtained as

$$P_l(x,\sigma) = \sum_h \frac{2}{I} A_{2,h} Q\left(\sqrt{2\left(\frac{1}{\sigma^2}+x\right)+h\frac{1}{\sigma^2}}\right) \qquad (5)$$

where $A_{2,h}$ denotes the number of codewords with information weight 2 and redundancy weight h.

Proof: We modify the proof of (3) by taking into account that information bits and redundancy bits are sent on the binary-input Gaussian channel. Therefore, the probability of confusing $\boldsymbol{c}^0$ with any other codeword $\boldsymbol{c}^{w,h}$ with information weight w and redundancy weight h can be written as

$$P_{w,h} = Q(\sqrt{w(1/\sigma^2+x)+h/\sigma^2}.$$

A lower bound on the bit-error probability of the information bits is obtained as the first term of the union bound. Since the code is recursive systematic, the terms corresponding to $w = 1$ are negligible (information weight-$w = 1$ codewords have an infinite number of nonzero redundancy bits when $I \to \infty$), so the desired result is obtained by taking into account the terms corresponding to $w = 2$. This lower bound is tight when the value of x is large. □

Applying Theorem. 3.2, we immediately obtain a lower bound on the map describing the iterative decoder from (5).

Example 4.2: We consider terminated rate-$1/2$ recursive systematic convolutional constituent codes with generators

$$g_0(D) = 1 + D + D^2 \quad \text{and} \quad g_1(D) = 1 + D^2$$

and $k = 8192$ information bits. The resulting turbo code is a rate-$1/3$ PCCC with interleaver size $I = 8192$. For $E_b/N_0 = 2$ dB, Fig. 5 illustrates the BER $P(x,\sigma)$ obtained through Monte Carlo simulation (solid) along with the lower bound (5) (dash-dotted). Note the tightness of the lower bound when $x > 7$. The turbo decoding trajectory (average BER versus average *a priori* information) is denoted by circles. Starting from no *a priori* information ($x = 0$), the BER is decreasing as the number of iterations increases until a fixed point $\approx 10^{-6}$ is reached. Unfortunately, the four last decoding iterations are not lying on the curve $y = P(x,\sigma)$, indicating that the assumption of i.i.d. extrinsic information breaks down for a large number of iterations.

Fig. 6, illustrates the iterative decoding map $h(y,\sigma)$ defined by (2) (solid) along with the lower bound obtained from (5) (dash-dotted), which becomes tight for small values of y, and the $z = y$ curve (dashed). The iterative decoding trajectory (circles) goes through the *decoding tunnel* [15] between the $z = h(y,\sigma)$ and the $z = y$ curves, until convergence is reached close to $y \approx 10^{-6}$. Observe that the map $z = h(y,\sigma)$ is not able to predict the existence of this fixed point,

[1]Note that when considering a one-dimensional (1-D) map of the form $x_{k+1} = f(x_k)$, the trajectory starting from a certain initial condition, x_0, may be constructed geometrically by "bouncing" back and forth between the map itself and the bisectrix defined by $x_{k+1} = x_k$ [17]. Also, the fixed points of the map are defined by $x^* = f(x^*)$, thus, the intersections of the map with the bisectrix.

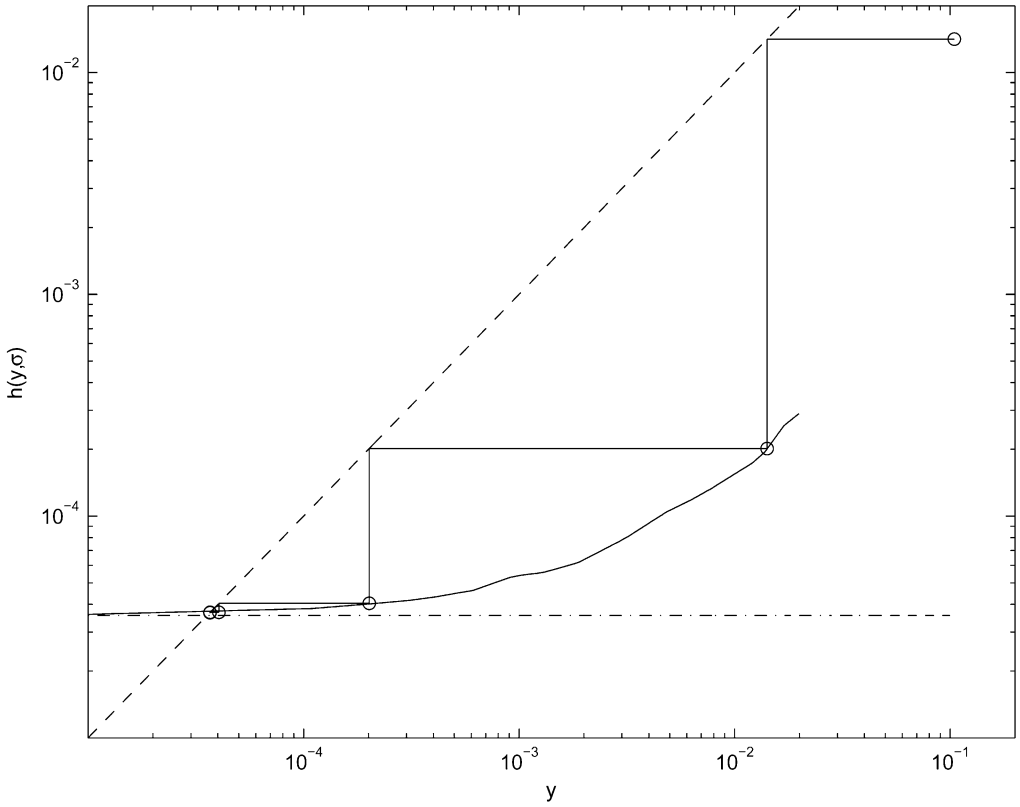

Fig. 4. $h(y, \sigma)$ at $E_b/N_0 = 5$ dB for a PCCC with rate-$1/2$ state-4 nonrecursive nonsystematic constituent convolutional codes (solid), along with the lower bound (dash-dot) and the bisectrix (dash).

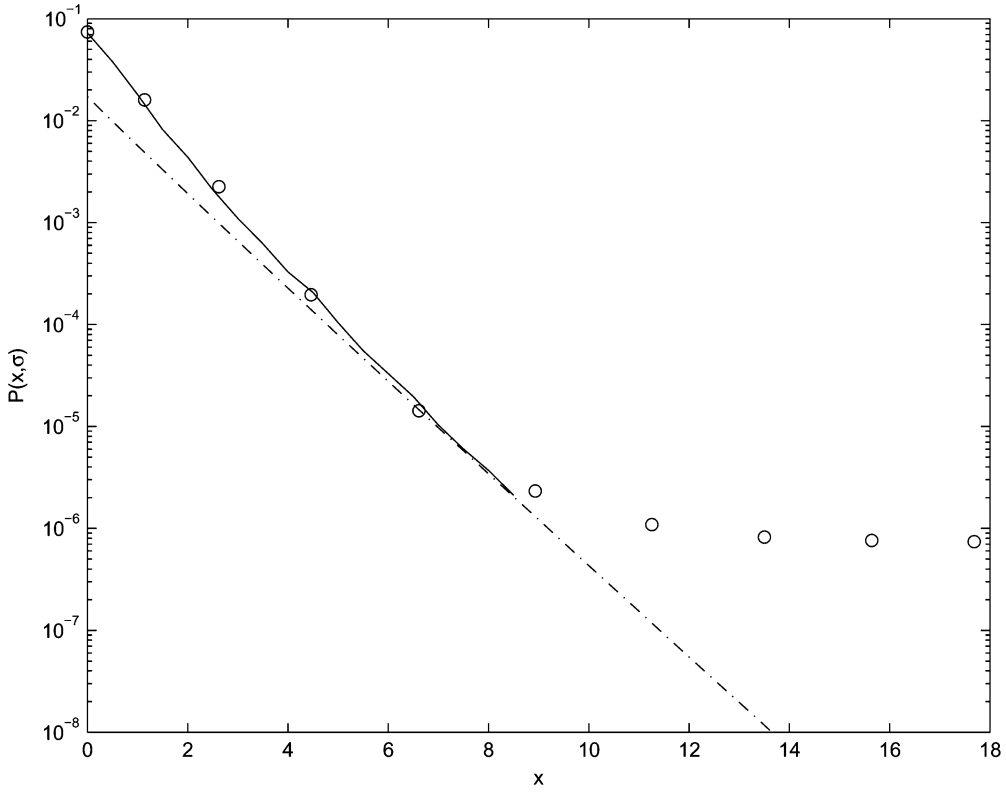

Fig. 5. $P(x, \sigma)$ at $E_b/N_0 = 2$ dB for a PCCC with rate-$1/2$ state-4 recursive systematic convolutional code (solid), lower bound (dash-dot) and turbo decoding trajectory (circles).

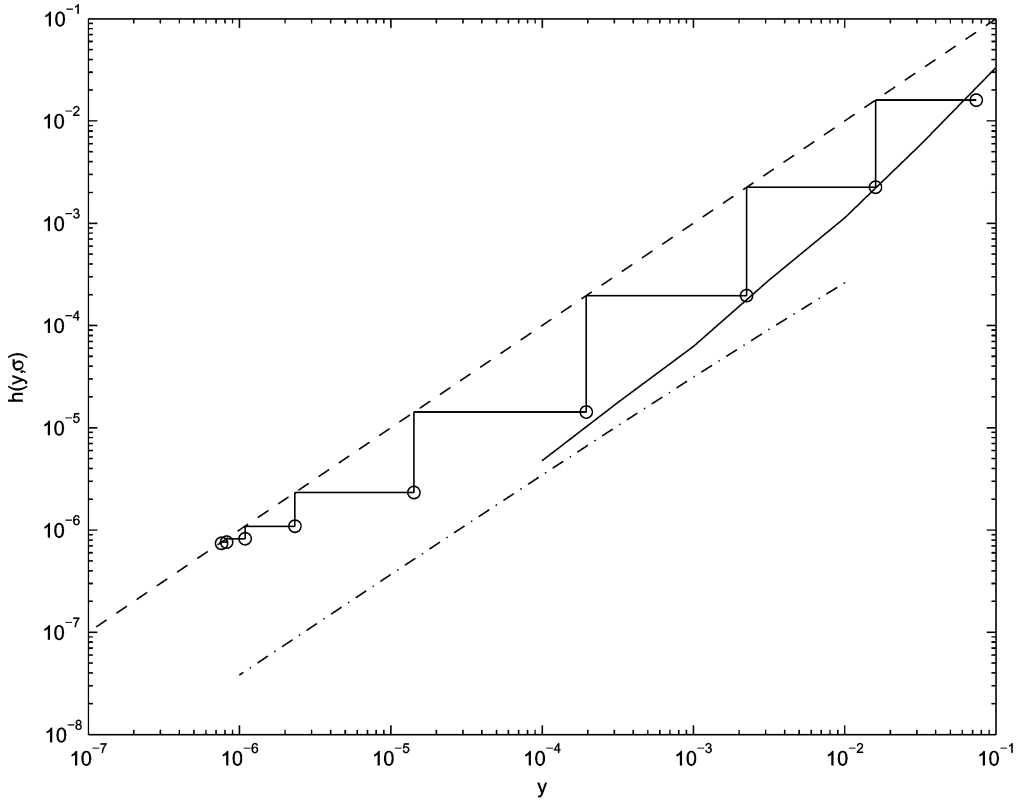

Fig. 6. $h(y,\sigma)$ at E_b/N_0 =2 dB for a PCCC with rate-$1/2$ state-4 recursive systematic constituent convolutional codes (solid line). As usual, the dash-dotted curve represents the lower bound, while the bisectrix line is dashed.

which is due to the correlation of the extrinsic information when the number of iterations is large.

We now study qualitatively the behavior of iterative decoding close to $y = 0$. Using $Q(\sqrt{z+y}) \approx Q(\sqrt{z})e^{-y/2}$, (5) can be approximated as

$$P_l(x,\sigma) \approx \beta(\sigma) Q(\sqrt{2x}) \tag{6}$$

where

$$\beta(\sigma) = \frac{2}{I} \sum_h A_{2,h} \left[e^{-\frac{1}{2\sigma^2}} \right]^{h+2}. \tag{7}$$

Then the corresponding lower bound on $h(y,\sigma)$ becomes

$$h_l(y,\sigma) \approx \beta(\sigma) Q\left(\sqrt{2\left([Q^{-1}(y)]^2 - \frac{1}{\sigma^2} - \frac{1}{2}\left[Q^{-1}\left(\frac{y}{\beta(\sigma)} \right) \right]^2 \right)} \right).$$

As shown in Appendix B (by choosing $A = B = 2$ and $\epsilon = \beta(\sigma)$), we have $\lim_{y\to 0} h_l(y,\sigma) = 0$ and $\lim_{y\to 0}(\partial h_l(y,\sigma)/\partial y) = (\beta(\sigma)e^{1/2\sigma^2})^2$. It follows that $y = 0$ is a fixed point of h_l, whose stability condition is given by

$$\beta(\sigma) e^{\frac{1}{2\sigma^2}} < 1. \tag{8}$$

Let the noise threshold σ^* be the solution of $\beta(\sigma)e^{1/2\sigma^2} = 1$, if $\sigma > \sigma^*$, a decoding trajectory starting close to $y = 0$ will diverge. A similar result has already appeared in [12].

Example 4.3: We consider terminated rate-$1/2$ recursive systematic convolutional constituent codes with generators

$$g_0(D) = 1 + D^2 + D^3 \quad \text{and} \quad g_1(D) = 1 + D + D^3$$

and $k = 8192$ information bits. The resulting turbo code is a rate-$1/3$ PCCC with interleaver size $I = 8192$. The noise threshold calculated from (8) is $\sigma^* = 1.62$ and the corresponding bit energy to noise power spectral density is $(E_b/N_0)^* = -2.4$ dB. This value is below the Shannon limit, therefore, a decoding tunnel is always open close to $y = 0$ for practical values of SNRs. Fig. 7 illustrates the evolution of the average extrinsic log-likelihood ratio as a function of the average *a priori* log-likelihood ratio at each half-iteration l for $E_b/N_0 = -3$ dB (squares) and $E_b/N_0 = -2$ dB (triangles), starting with i.i.d. Gaussian distributed *a priori* log-likelihood ratios with mean 15. Clearly, iterative decoding diverges below the threshold $(E_b/N_0)^*$ since the average extrinsic information recedes to a value close to 0. Above the threshold, the average extrinsic information increases until it reaches a fixed point close to 20.

V. Discussion

Although the model we develop in this correspondence is not able to provide an explanation for some typical nonlinear phenomena such as quasi-periodic and periodic phase trajectories reported in [21], the closed-form model we propose enables to link the dynamics of the iterative decoding system to the parameters of the constituent codes. Another limitation of the proposed method is that the predicted error floor can reach zero. This is due to the fact that i.i.d. log-likelihood ratios are considered in our analysis. This hypothesis is no longer valid when the number of iterations becomes large. An analysis based on stopping sets and pseudocodewords [22], [23] is available to explain this error floor.

VI. Conclusion

In this correspondence, we have presented an approximate analytical model for the iterative decoding of PCCC. Assuming that the density of the extrinsic information can be approximated by a Gaussian, we

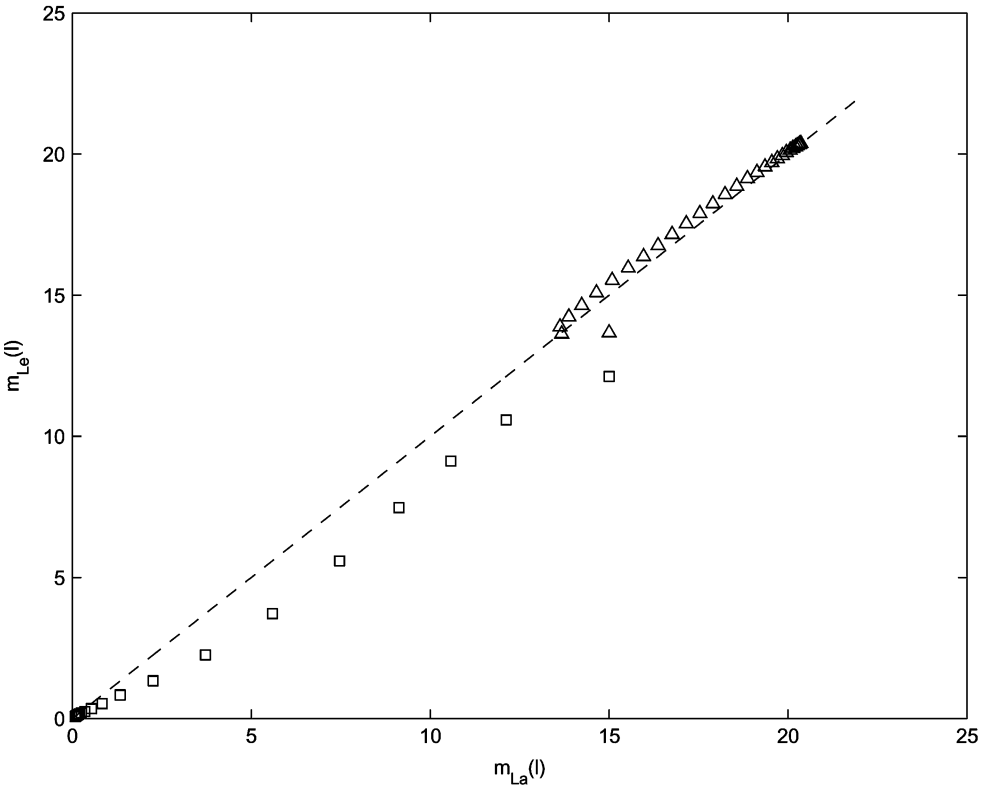

Fig. 7. Average extrinsic log-likelihood ratio versus average *a priori* log-likelihood ratio at each half-iteration $l$for a PCCC with rate-$1/2$ state-8 recursive systematic constituent convolutional codes, with $E_b/N_0 = -3$ dB (squares) and $E_b/N_0 = -2$ dB (triangles), respectively.

described the evolution of the BER at the output of the constituent decoders as the iterates of a nonlinear map for the binary-input Gaussian channel.

We showed how the fixed points of the iterative decoding system and their stability depend on the parameters of the constituent codes. For nonrecursive nonsystematic constituent codes, information weight-1 codewords generate a stable fixed point decreasing with the channel SNR and the free distance. For recursive systematic constituent codes, information weight-2 codewords generate a decoding tunnel which is open only if a stability condition is verified. Possible extensions of this work include threshold evaluation, application to multiple concatenations, and other channel models.

APPENDIX A

We give here the Proof of Theorem 3.2 stated in Section III. We restrict ourselves to the case of nonrecursive nonsystematic constituent encoders. The proof is similar for recursive systematic encoders. By definition, $P(x,\sigma)$ is the error probability of a constituent code, therefore, it is a bijective and decreasing function of x. We assume that the lower bound $P_l(x,\sigma)$ is also a bijective and decreasing function of x. It follows that $\forall y,\ P_l^{-1}(y,\sigma) \leq P^{-1}(y,\sigma)$. Using the fact that $P(x,\sigma)$ is decreasing, we have

$$P([Q^{-1}(y)]^2 - P^{-1}(y,\sigma),\sigma) \geq P([Q^{-1}(y)]^2 - P_l^{-1}(y,\sigma),\sigma).$$

Using the fact that P_l is a lower bound on P, we get

$$P([Q^{-1}(y)]^2 - P^{-1}(y,\sigma),\sigma) \geq P_l([Q^{-1}(y)]^2 - P_l^{-1}(y,\sigma),\sigma)$$

which is the desired result.

APPENDIX B

In order to study the properties of the approximated maps introduced in Section IV, we define the function

$$f(y,\sigma) = \epsilon Q\left(\sqrt{A\left([Q^{-1}(y)]^2 - \frac{1}{\sigma^2} - \frac{1}{B}\left[Q^{-1}\left(\frac{y}{\epsilon}\right)\right]^2\right)}\right) \quad (9)$$

where A, B are integers > 1 and $y \geq 0, \epsilon$ are real numbers. Unless otherwise specified, the control parameter σ is a fixed positive real number.

A. Limit of $f(y,\sigma)$ When $y \to 0$

Using the inequality

$$\left(1 - \frac{1}{x^2}\right) < \sqrt{2\pi}xe^{x^2/2}Q(x) < 1$$

when $x > 0$, we obtain

$$\lim_{x\to+\infty} \sqrt{2\pi}Q(x)xe^{x^2/2} = 1.$$

When $0 < y < 1/2$, we choose $x = Q^{-1}(y)$ and $x = Q^{-1}(y/\epsilon)$ to obtain

$$\lim_{y\to 0} \sqrt{2\pi}yQ^{-1}(y)e^{\frac{1}{2}[Q^{-1}(y)]^2} = 1$$
$$\lim_{y\to 0} \sqrt{2\pi}\frac{y}{\epsilon}Q^{-1}\left(\frac{y}{\epsilon}\right)e^{\frac{1}{2}\left[Q^{-1}\left(\frac{y}{\epsilon}\right)\right]^2} = 1. \quad (10)$$

Consequently

$$\lim_{y\to 0} \frac{e^{\frac{1}{2}\left[Q^{-1}\left(\frac{y}{\epsilon}\right)\right]^2}Q^{-1}\left(\frac{y}{\epsilon}\right)}{\epsilon e^{\frac{1}{2}[Q^{-1}(y)]^2}Q^{-1}(y)} = 1. \quad (11)$$

From L'Hôpital's rule, we have

$$\lim_{y\to 0}\frac{Q^{-1}\left(\frac{y}{\epsilon}\right)}{Q^{-1}(y)} = \lim_{y\to 0}\frac{\frac{\partial Q^{-1}\left(\frac{y}{\epsilon}\right)}{\partial y}}{\frac{\partial Q^{-1}(y)}{\partial y}} = \lim_{y\to 0}\frac{e^{\frac{1}{2}\left[Q^{-1}\left(\frac{y}{\epsilon}\right)\right]^2}Q^{-1}\left(\frac{y}{\epsilon}\right)}{\epsilon e^{\frac{1}{2}[Q^{-1}(y)]^2}Q^{-1}(y)}$$

and (11) implies that

$$\lim_{y\to 0}\frac{Q^{-1}\left(\frac{y}{\epsilon}\right)}{Q^{-1}(y)} = 1. \tag{12}$$

Using the inequality $Q(x) < e^{-x^2/2}$ and (9), we get

$$0 \le f(y,\sigma) \le \epsilon e^{\frac{A}{2\sigma^2}}\exp\left\{-\frac{A}{2}[Q^{-1}(y)]^2\left(1-\frac{1}{B}\frac{\left[Q^{-1}\left(\frac{y}{\epsilon}\right)\right]^2}{[Q^{-1}(y)]^2}\right)\right\}. \tag{13}$$

Since $A > 1, B > 1$, and $\lim_{y\to 0} Q^{-1}(y) = +\infty$, combining (12) and (13) leads to $\lim_{y\to 0} f(y,\sigma) = 0$.

B. Derivative of $f(y,\sigma)$ With Respect to y

The expression of the partial derivative with respect to y is

$$\frac{\partial f(y,\sigma)}{\partial y} = C(A,B,\epsilon)\gamma(y,B,\epsilon)\delta(y,A,B,\epsilon) \ge 0 \tag{14}$$

where

$$C(A,B,\epsilon) = \epsilon^2 e^{\frac{A}{2\sigma^2}}\sqrt{A\left(1-\frac{1}{B}\right)}$$

$$\gamma(y,B,\epsilon) = \sqrt{1-\frac{1}{B}}\frac{\frac{[Q^{-1}(y)]^2}{\left[Q^{-1}\left(\frac{y}{\epsilon}\right)\right]^2}}{\sqrt{\frac{[Q^{-1}(y)]^2}{\left[Q^{-1}\left(\frac{y}{\epsilon}\right)\right]^2}-\frac{1}{B}-\frac{1/\sigma^2}{\left[Q^{-1}\left(\frac{y}{\epsilon}\right)\right]^2}}} \times\frac{1}{B-1}\left(B-\frac{e^{\frac{1}{2}\left[Q^{-1}\left(\frac{y}{\epsilon}\right)\right]^2}Q^{-1}\left(\frac{y}{\epsilon}\right)}{\epsilon e^{\frac{1}{2}[Q^{-1}(y)]^2}Q^{-1}(y)}\right)$$

$$\delta(y,A,B,\epsilon) = \frac{e^{\frac{A}{2B}\left[Q^{-1}\left(\frac{y}{\epsilon}\right)\right]^2}Q^{-1}\left(\frac{y}{\epsilon}\right)}{\epsilon e^{\frac{A-1}{2}[Q^{-1}(y)]^2}Q^{-1}(y)}. \tag{15}$$

Since $\lim_{y\to 0} Q^{-1}(y/\epsilon) = +\infty$, from (11) and (12), we have immediately that $\lim_{y\to 0}\gamma(y,B,\epsilon) = 1$. Thus, the limit of $(\partial f(y,\sigma)/\partial y)$ is determined solely by the behavior of $\delta(y,A,B,\epsilon)$, for $y \to 0$.

We assume that A and B span the integers strictly larger than one, therefore, we can introduce two distinct cases, namel,y $A = B = 2$ and $\max(A,B) > 2$.

1) Case $A = B = 2$: Using (11) again, we get

$$\lim_{y\to 0}\delta(y,A,B,\epsilon) = 1$$

thus,

$$\lim_{y\to 0}\frac{\partial f(y,\sigma)}{\partial y} = C(2,2,\epsilon) = \left(\epsilon e^{\frac{1}{2\sigma^2}}\right)^2. \tag{16}$$

2) Case $\max(A,B) > 2$: From (10) we deduce

$$\lim_{y\to 0}\left(\sqrt{2\pi}yQ^{-1}(y)e^{\frac{1}{2}[Q^{-1}(y)]^2}\right)^{A-1} = 1$$

$$\lim_{y\to 0}\left(\sqrt{2\pi}\frac{y}{\epsilon}Q^{-1}\left(\frac{y}{\epsilon}\right)e^{\frac{1}{2}[Q^{-1}\left(\frac{y}{\epsilon}\right)]^2}\right)^{\frac{A}{B}} = 1. \tag{17}$$

It follows that

$$\lim_{y\to 0}\delta(y,A,B,\epsilon) = \lim_{y\to 0}\frac{(\sqrt{2\pi})^{A-1}y^{A-1}[Q^{-1}(y)]^{A-2}}{(\sqrt{2\pi})^{\frac{A}{B}}\frac{1}{\epsilon^{\frac{A}{B}-1}}y^{\frac{A}{B}}\left[Q^{-1}\left(\frac{y}{\epsilon}\right)\right]^{\frac{A}{B}-1}} = \lim_{y\to 0}(\sqrt{2\pi})^{A\left(1-\frac{1}{B}\right)-1}\epsilon^{\frac{A}{B}-1} \times\left(\frac{Q^{-1}\left(\frac{y}{\epsilon}\right)}{Q^{-1}(y)}\right)^{1-\frac{A}{B}}(yQ^{-1}(y))^{A\left(1-\frac{1}{B}\right)-1}.$$

Finally, (12) leads to

$$\lim_{y\to 0}\delta(y,A,B,\epsilon) = (\sqrt{2\pi})^{A(1-\frac{1}{B})-1}\epsilon^{\frac{A}{B}-1}\lim_{y\to 0}(yQ^{-1}(y))^{A(1-\frac{1}{B})-1}. \tag{18}$$

We use the inequality $Q(x) < e^{-x^2/2}, x > 0$. When $0 < y < 1/2$, we choose $x = Q^{-1}(y)$ and after some straightforward manipulations we obtain the bound

$$0 < Q^{-1}(y) < \sqrt{-2\ln y}.$$

It is immediate that

$$0 < (yQ^{-1}(y))^{A(1-\frac{1}{B})-1} < (-2y^2\ln y)^{\frac{1}{2}[A(1-\frac{1}{B})-1]}. \tag{19}$$

Notice that $\lim_{y\to 0} y^2\ln y = 0$ and $A(1-1/B)-1 > 0$, since $A > 1$ and $B > 1$, thus, combining (19) with (18) results in $\lim_{y\to 0}\delta(y,A,B,\epsilon) = 0$. We conclude that

$$\lim_{y\to 0}(\partial f(y,\sigma)/\partial y) = 0, \qquad \text{when } \max(A,B) > 2.$$

ACKNOWLEDGMENT

The authors would like to thank Dr. Ljupco Kocarev (UCSD), Prof. Rüdiger Urbanke (EPFL), and Henry Pfister (UCSD) for the stimulating discussions.

REFERENCES

[1] P. Elias, "Error-free coding," *IRE Trans. Inf. Theory*, vol. IT-4, no. 4, pp. 29–37, Sep. 1954.
[2] G. Forney, *Concatenated Codes*. Cambridge, MA: MIT Press, 1966.
[3] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo codes," in *Proc. Int. Conf. Communications (ICC 1993)*, Geneva, Switzerland, May 1993, pp. 1064–1070.
[4] R. M. Pyndiah, "Near optimum decoding of product codes: Block turbo codes," *IEEE Trans. Commun.*, vol. 46, no. 8, pp. 1003–1010, Aug. 1998.
[5] F. R. Kschischang, B. J. Frey, and H.-A. Loeliger, "Factor graphs and the sum-product algorithm," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 498–519, Feb. 2001.
[6] T. J. Richardson, "The geometry of turbo-decoding dynamics," *IEEE Trans. Inf. Theory*, vol. 46, no. 1, pp. 9–23, Jan. 2000.
[7] T. J. Richardson and R. L. Urbanke, "The capacity of low-density parity-check codes under message-passing decoding," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 599–618, Feb. 2001.
[8] T. Richardson and R. Urbanke, "Thresholds for turbo codes," in *Proc. IEEE Int. Symp. Information theory (ISIT 2000)*, Sorrento, Italy, Jun. 2000, p. 317.
[9] S.-Y. Chung, T. J. Richardson, and R. L. Urbanke, "Analysis of sum-product decoding of low-density parity-check codes using a Gaussian approximation," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 657–670, Feb. 2001.
[10] N. Wiberg, "Codes and Decoding on General Graphs," Ph.D. dissertation, Linköping University, Linköping, Sweden, 1996.
[11] S. ten Brink, "Convergence behavior of iteratively decoded parallel concatenated codes," *IEEE Trans. Commun.*, vol. 49, no. 10, pp. 1727–1737, Oct. 2001.

[12] M. Lentmaier, D. V. Truhachev, and K. Sh. Zigangirov, "On the theory of low-density convolutional codes," *Probl. Pered. Inform.*, vol. 37, no. 4, pp. 288–306, Oct.–Dec. 2001.
[13] F. Lehmann and G. M. Maggio, "Analysis of the iterative decoding of LDPC and product codes using the Gaussian approximation," *IEEE Trans. Inf. Theory*, vol. 49, no. 11, pp. 2993–3000, Nov. 2003.
[14] S. Benedetto and G. Montorsi, "Unveiling turbo-codes: Some results on parallel concatenated coding schemes," *IEEE Trans. Inf. Theory*, vol. 42, no. 2, pp. 409–428, Mar. 1996.
[15] D. Divsalar, S. Dolinar, and F. Pollara, "Iterative turbo decoder analysis based on density evolution," *IEEE J. Sel. Areas Commun.*, vol. 19, no. 5, pp. 891–907, May 2001.
[16] S. Benedetto, D. Divsalar, G. Montorsi, and F. Pollara, "Serial concatenation of interleaved codes: Performance analysis, design, and iterative decoding," *IEEE Trans. Inf. Theory*, vol. 44, no. 3, pp. 909–926, May 1998.
[17] E. Ott, *Chaos in Dynamical Systems*, Cambridge, U.K.: Cambridge Univ. Press, 1993.
[18] R. L. Devaney, *A First Course in Chaotic Dynamical Systems*. New York: Addison-Wesley, 1992.
[19] S. Benedetto, G. Montorsi, and R. Garello, "Concatenated codes with interleaver for digital transmission over mobile channels," in *Proc. Int. Conf. Communications (ICC 2001)*, vol. 10, Helsinki, Finland, Jun. 2001, pp. 3026–3030.
[20] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 619–637, Feb. 2001.
[21] D. Agrawal and A. Vardy, "The turbo decoding algorithm and its phase trajectories," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 699–722, Feb. 2001.
[22] C. Di, D. Proietti, İ. E. Telatar, T. J. Richardson, and R. L. Urbanke, "Finite-length analysis of low-density parity-check codes on the binary erasure channel," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1570–1579, Jun. 2002.
[23] R. Koetter and P. O. Vontobel, "Graph covers and iterative decoding of finite-length codes," in *Proc. 3rd Int. Conf. Turbo Codes and Related Topics*, Brest, France, Sep. 1–5, 2003, pp. 75–82.

Consta-Abelian Polyadic Codes

Chong Jie Lim

***Abstract*—In this correspondence, the class of polyadic codes is generalized to the class of consta-Abelian polyadic codes, which, in particular, includes the class of constacyclic polyadic codes. Properties such as the equivalence of polyadic codes and the mth-root lower bound for the minimum weight of a subcode of certain types of polyadic codes are preserved in the consta-Abelian case. Sufficient conditions for the existence of this class of codes are established. For the special case of constacyclic codes, the characterization of negacyclic self-dual codes of length coprime to the characteristic of the field in terms of negacyclic duadic codes is also given.**

***Index Terms*—Consta-Abelian codes, constacyclic codes, minimum weight, m-splitting, polyadic codes, self-dual codes, twisted discrete Fourier transform.**

I. Introduction

The class of binary cyclic duadic codes generalizing quadratic residue codes was first introduced by Leon, Masley, and Pless in [9], and a different approach was given in [15]. Generalizations of binary cyclic duadic codes to other base fields were given by Smid [17]. Subsequently, Pless and Rushanan moved on to investigate cyclic triadic codes [16], and the class of cyclic polyadic codes (or m-adic codes) was later introduced by Brualdi and Pless [4].

Following the growing interest in Abelian group codes, the class of cyclic duadic codes was generalized in another direction to the class of split group codes, or Abelian duadic codes, where in this case, the "cyclic" property was, in some sense, removed [6]. Only recently, Ling and Xing unified the two directions of generalizations of duadic codes to Abelian polyadic codes [12]. In that correspondence, necessary and sufficient conditions for the existence of nondegenerate polyadic codes (see [12]) were studied, and an mth-root lower bound for a subcode of certain types of polyadic codes was established.

In this correspondence, following the idea in [12], we extend the class of polyadic codes to the class of consta-Abelian polyadic codes, which, in particular, include constacyclic polyadic codes. We extend various results established in [4] and [12] for this new class of codes. For the special case of constacyclic codes, we also give a characterization of negacyclic self-dual codes of lengths coprime to the characteristic of the finite field in terms of negacyclic duadic codes.

The organization of this correspondence is as follows. We first discuss in detail the generalization to the class of constacyclic polyadic codes (Sections II–VI), before moving on to generalize to consta-Abelian polyadic codes (Section VII). In Section II, the main definitions are given. Section III gives some basic results, while Section IV gives lower bounds on the minimum weight of a subcode. Section V establishes sufficient conditions for the existence of the class of constacyclic polyadic codes, and Section VI deals with the characterization of negacyclic self-dual codes of lengths coprime to the characteristic of the finite field. Section VII, as mentioned, is devoted to the generalization to consta-Abelian polyadic codes. The results from Sections III–V will be restated in the new setting without proofs since the proofs are very much similar to the constacyclic case. The reader who is not interested in this section can skip it without causing

Manuscript received May 26, 2004; revised December 8, 2004. This work was supported in part by the National University of Singapore Academic Research Fund (NUS-ARF) under Research Grant R146-000-029-112.

The author is with the Department of Mathematics, National University of Singapore, Singapore 117543, Republic of Singapore.

Communicated by C. Carlet, Associate Editor for Coding Theory.
Digital Object Identifier 10.1109/TIT.2005.847734