EXIT Functions for Binary Input Memoryless Symmetric Channels

Eran Sharon, Alexei Ashikhmin, *Senior Member, IEEE,* Simon Litsyn, *Senior Member, IEEE*

***Abstract*— Use of Extrinsic Information Transfer (EXIT) functions, characterizing the amplification of mutual information between the input and output of the Maximum *A-Posteriori* (MAP) decoder, significantly facilitates analysis of iterative coding schemes. Previously EXIT functions derived for Binary Erasure Channel (BEC) were used as an approximation for other channels. Here we improve on this approach by introducing more accurate methods to construct EXIT functions for Binary input, Memoryless, Symmetric (BMS) channels. By defining an alternative pseudo-MAP decoder coinciding with the MAP decoder over BEC, we provide an expression for the EXIT functions of block codes over BEC. Furthermore, we draw a connection between the EXIT function over BEC and the EXIT function over BMS channel under certain conditions. This is used for deriving accurate or approximated expressions for EXIT functions over BMS channels in certain scenarios.**

***Index Terms*— Soft decoding, EXIT functions, Mutual Information, MAP decoding.**

I. INTRODUCTION

Asymptotic analysis of iteratively decodable codes, such as LDPC codes [4] and Turbo codes [2], can be done using the Density Evolution (DE) algorithm by tracking the densities of messages passed along the decoding process [8],[9]. Extrinsic Information Transfer (EXIT) functions [3],[1] provide a computationally simple tool for predicting the asymptotic convergence behavior of iterative coding schemes by tracking a single parameter, the mutual information, rather than entire densities. The EXIT function of each constituent decoder in the iterative coding system shows how the *a priori* information at the soft input of the decoder converts into extrinsic information at the soft output of the decoder. The exchange of extrinsic information between constituent decoders can be visualized as a decoding trajectory in an EXIT chart.

For the Binary Erasure Channel (BEC) EXIT charts analysis is equivalent to DE analysis since BEC densities are completely determined by a single parameter. Moreover, it relies on a strong theoretical basis. Analytical expressions for EXIT functions of various codes are known in terms of their combinatorial parameters. The EXIT function of a linear block code and its dual are connected by a "Duality Theorem". The area under an EXIT function of a code is related to its rate through an "Area Theorem". These properties, proved in [1] can be used for designing capacity approaching iterative coding schemes by matching the EXIT functions of the constituent codes. Much less is known on EXIT functions for other Binary input, Memoryless, Symmetric (BMS) channels. In [11],[7] upper and lower bounds on the EXIT functions of the repetition and single parity-check codes were obtained by defining the least and most informative channels for these constraints . The problem can also be approached, especially for more complex codes, using Monte-Carlo simulations [3], or using the EXIT function over BEC as an approximation. In this paper we take another approach and show that in certain scenarios the EXIT function of a code over BMS channels can be expressed (or approximated) as a series having the EXIT function over BEC as its terms.

The paper is organized as follows. In Section III, we derive a general expression for computing the extrinsic information at the output of the MAP decoder over BMS channel. In Section IV, we define a pseudo-MAP decoder that coincides with the MAP decoder of a linear code in BEC. Using the pseudo-MAP decoder we derive an expression for the EXIT function of a linear block code over BEC as a function of combinatorial parameters of the code. Furthermore, we draw a connection between the EXIT function of a code over a BMS channel and its EXIT function over the BEC when the pseudo-MAP and MAP decoders coincide. This is used for computing the EXIT functions of single-parity check codes over any BMS channel. In Section V we derive approximations for the EXIT functions and bit error probability curves of some block code over the binary input Additive White Gaussian Noise (biAWGN) channel. The approximations have the form of a series expansion of the EXIT function of the code in BEC.

II. BASIC DEFINITIONS AND NOTATION

Let $\underline{c}_i = (c_{i,1}, c_{i,2}, \ldots, c_{i,n})$ stand for the i'th codeword of an $[n,k]$ binary linear block code C, and let $\underline{c}_i^{\perp} = (c_{i,1}^{\perp}, c_{i,2}^{\perp}, \ldots, c_{i,n}^{\perp})$ be the ith codeword of the $[n,n-k]$ dual code $C^{\perp}$. Let $\alpha \in \{0,1\}$, we denote by $C_j^{(\alpha)} = \{\underline{c}_i \in C | c_{i,j} = \alpha\}$ the set of the codewords from code C with the j'th bit equal to α, by $I_j^{(\alpha)} = \{i | c_{i,j}^{\perp} = \alpha\}$ the set of indices of all codewords in the dual code with the j'th bit equal to α and by $P(I_j^{(\alpha)})$ the set of all subsets of $I_j^{(\alpha)}$.

We assume BMS channel with equiprobable "BPSK modulated" input x, i.e. $x_j = (-1)^{c_j}$, $j = 1,\ldots,n$, and output y. The channel is defined by its conditional density function $f_{Y|X}(y|x)$. Due to channel symmetry $f_{Y|X}(y|1) = f_{Y|X}(-y|-1)$.

An estimate of a transmitted (modulated) bit X given an observation Y can be expressed in several ways, for example:

- the bit's log-likelihood ratio (LLR), $L = \log \frac{Pr(X=1|Y)}{Pr(X=-1|Y)}$.

S. Litsyn and E. Sharon are with Department of Electrical Engineering-Systems, Tel Aviv University, Ramat Aviv, 69978 Israel; e-mail: {litsyn, eransh}@eng.tau.ac.il

A. Ashikhmin is with Bell Laboratories, Lucent Technologies, 600 Mountain Avenue, Murray Hill, NJ 07974, USA; e-mail: aea@research.bell-labs.com

- the bit's expectation, also known as the "soft bit", $T = Pr(X = 1|Y) - Pr(X = -1|Y)$.

Let $L_j = \log \frac{Pr(X_j=1|Y_j=y_j)}{Pr(X_j=-1|Y_j=y_j)}$ and $T_j = Pr(X_j = 1|Y_j = y_j) - Pr(X_j = -1|Y_j = y_j)$ denote the j'th bit *a-priori* LLR and "soft bit" input to the MAP decoder, respectively. Using T_j or L_j for $j = 1, \ldots, n$ the MAP decoder can compute the j'th bit extrinsic LLR, $L_{EMAP,j} = \log \frac{Pr(X_j=1|\underline{Y}_{[j]})}{Pr(X_j=-1|\underline{Y}_{[j]})}$, or the extrinsic "soft bit", $T_{EMAP,j} = Pr(X_j = 1|\underline{Y}_{[j]}) - Pr(X_j = -1|\underline{Y}_{[j]})$, where, $\underline{Y}_{[j]}$ is the vector of channel outputs $\underline{Y}$ excluding the channel output Y_j. In [6] Hartmann and Rudolph showed that extrinsic MAP decoding can be implemented using the dual code as follows:

$$T_{EMAP,j} = \frac{\sum_{i \in I_j^{(1)}} \prod_{l=1, l \neq j}^{n} T_l^{c_{i,l}^{\perp}}}{\sum_{i \in I_j^{(0)}} \prod_{l=1, l \neq j}^{n} T_l^{c_{i,l}^{\perp}}}. \quad (1)$$

III. Extrinsic Information at the Output of the MAP decoder

Let $I(A; B)$ denote the mutual information between two r. v.'s A and B [5]. We define the average *a priori* mutual information at the input of the MAP decoder I_A and the average extrinsic mutual information at the output of the MAP decoder I_E as follows [3], [1]:

$$\begin{aligned} I_A &= \frac{1}{n}\sum_{j=1}^{n} I(X_j; Y_j) = \frac{1}{n}\sum_{j=1}^{n} I(X_j; T_j), \\ I_E &= \frac{1}{n}\sum_{j=1}^{n} I(X_j; Y_{[j]}) = \frac{1}{n}\sum_{j=1}^{n} I(X_j; T_{EMAP,j}) \end{aligned}$$

We are interested in studying the function $I_E(I_A)$, called EXIT function. In order to do that, we express I_E as a function of the moments of T_{EMAP}. In some cases it can be expressed as a function of the moments of T (the " soft bit" inputs to the decoder) which are directly connected to I_A.

Richardson *et al.* [9] showed that the conditional probability distribution function $f_{L|1}(l) = f_{L|X}(l|1)$ of the r.v. $L|X = 1$ at the output of a symmetric channel maintains the following consistency condition:

$$f_{L|1}(l) = f_{L|1}(-l)e^{l}. \quad (2)$$

Similar to this consistency condition for LLR's we define a consistency condition for "soft bits". To distinct it from the LLR's consistency condition, we address it as the T-consistency condition.

Proposition 3.1: For any channel satisfying the symmetry property $f(Y|X = 1) = f(-Y|X = -1)$, the conditional probability density function $f_{T|1}(t) = f_{T|X}(t|1)$ of T satisfies:

$$f_{T|1}(t) = f_{T|1}(-t)\frac{1+t}{1-t} \quad (3)$$

Proof: Since $T = \tanh(\frac{L}{2})$, the r. v. $T|X = 1$ is distributed according to

$$\begin{aligned} f_{T|1}(t) &= \frac{2}{1-t^2} f_{L|1}\left(\ln\frac{1+t}{1-t}\right) \quad (4) \\ &= \frac{2}{1-t^2} f_{L|1}\left(\ln\frac{1-t}{1+t}\right)\frac{1+t}{1-t} = f_{T|1}(-t)\frac{1+t}{1-t}, \end{aligned}$$

where the second equality follows from (2). □

A r.v. $T \in [-1, 1]$ will be called T-consistent if it satisfies (3).

Lemma 3.2: The moments of T-consistent r.v. T satisfy:

$$E(T^{2i}) = E(T^{2i-1})$$

Proof:

$$\begin{aligned} E(T^{2i}) &= \int_{-1}^{+1} f_{T|1}(t)t^{2i}dt \\ &= \int_{0}^{+1} f_{T|1}(-t)(-t)^{2i}dt + \int_{0}^{+1} f_{T|1}(t)t^{2i}dt \\ &= \int_{0}^{+1} f_{T|1}(t)t^{2i}\left(\frac{1-t}{1+t}+1\right)dt \\ &= \int_{0}^{+1} f_{T|1}(t)t^{2i-1}\left(-\frac{1-t}{1+t}+1\right)dt \\ &= \int_{0}^{+1} f_{T|1}(t)\frac{1-t}{1+t}(-t)^{2i-1}dt + \int_{0}^{+1} f_{T|1}(t)t^{2i-1}dt \\ &= \int_{0}^{+1} f_{T|1}(-t)(-t)^{2i-1}dt + \int_{0}^{+1} f_{T|1}(t)t^{2i-1}dt \\ &= \int_{-1}^{+1} f_{T|1}(t)t^{2i-1}dt = E(T^{2i-1}) \end{aligned}$$

□

The moments of a T-consistent r.v. can be used for computing its mutual information:

Proposition 3.3: The mutual information between a binary r.v. $X \sim (\pm 1$ w.p. $0.5)$ and a T-consistent r. v. T is given by:

$$I(X;T) = \int_{-1}^{+1} f_{T|1}(t)\log_2(1+t)dt = \frac{1}{\ln 2}\sum_{i=1}^{\infty}\frac{1}{(2i)(2i-1)}E(T^{2i}),$$

where $E(T^{2i}) = \int_{-1}^{+1} t^{2i} f_{T|1}(t)dt$.

Proof:

$$\begin{aligned} I(X;T) &= \frac{1}{2}\sum_{x=\pm 1}\int_{-1}^{+1} f_{T|X}(t|x)\log_2\left[\frac{2f_{T|X}(t|x)}{\sum_{x=\pm 1} f_{T|X}(t|x)}\right]dt \\ &= \int_{-1}^{+1} f_{T|X}(t|1)\log_2\left[\frac{2f_{T|X}(t|1)}{f_{T|X}(t|1)+f_{T|X}(t|-1)}\right]dt \\ &= \int_{-1}^{+1} f_{T|1}(t)\log_2\left[\frac{2f_{T|1}(t)}{f_{T|1}(t)+f_{T|1}(t)\frac{1-t}{1+t}}\right]dt \\ &= \int_{-1}^{+1} f_{T|1}(t)\log_2(t+1)dt \\ &= \int_{-\infty}^{+\infty}\frac{f_{T|1}(t)}{\ln 2}[t - \frac{1}{2}t^2 + \frac{1}{3}t^3 - \ldots]dt \\ &= \frac{1}{\ln 2}[\mathbf{E}(T) - \frac{1}{2}\mathbf{E}(T^2) + \frac{1}{3}\mathbf{E}(T^3) - \ldots] \\ &= \frac{1}{\ln 2}\sum_{i=1}^{\infty}\frac{1}{(2i)(2i-1)}E(T^{2i}). \end{aligned}$$

The second equality follows from channel symmetry. The third equality follows from T-consistency. The fifth equality follows from Taylor series expansion and the seventh equality follows from Lemma 3.2. □

Note that by Lemma 3.2 all the moments of T are non-negative. Furthermore, since $|T| \leq 1$ then $0 \leq \frac{1}{i}\mathbf{E}(T^i) \leq \frac{1}{i}$. Thus, the convergence of the series $\sum_{i=1}^{\infty}(-1)^{i+1}\frac{1}{i}\mathbf{E}(T^i)$ in Proposition 3.3 is assured by the *Leibnitz test* for sign alternating series. The convergence rate of the series depends on the actual probability density function of T. However, since the series is sign alternating, upper and lower bounds on

$I(X;T)$ can be obtained by truncating the series appropriately. Next we characterize the output of the MAP decoder.

Theorem 3.4: For a linear block code used over a BMS channel, the extrinsic "soft bit" output of the MAP decoder is T-consistent and its distribution does not depend on the transmitted codeword,

1) $f(T_{EMAP,j}|X_j=1) = f(T_{EMAP,j}|\underline{c}),\ \underline{c} \in C_j^{(0)}$
2) $f(T_{EMAP,j}|X_j=-1) = f(T_{EMAP,j}|\underline{c}),\ \underline{c} \in C_j^{(1)}$ □

The proof of the theorem is based on the channel symmetry and on symmetry properties of linear block codes and MAP decoding. Similar theorem is known for LLR MAP decoder output [8], hence we omit the proof.

Theorem 3.5: The extrinsic information at the output of the MAP decoder of a linear block code used over a BMS channel is given by:

$$\begin{aligned} I_{E_j} &= I(X_j;\underline{Y}_{[j]}) = I(X_j;T_{EMAP,j}) \\ &= \int_{-1}^{+1} f_{T_{EMAP,j}|\underline{c}_0}(t)\log_2(1+t)dt \\ &= \frac{1}{\ln 2}\sum_{i=1}^{\infty}\frac{1}{(2i)(2i-1)}E(T_{EMAP,j|\underline{c}_0}^{2i}), \end{aligned}$$

Proof: Immediate from Proposition 3.3 and Theorem 3.4. □

This theorem justifies assuming transmission of the all-zero codeword for computing the extrinsic information at the output of the MAP decoder.

IV. Extrinsic information computation for BMS channels

Most of the research on EXIT functions so far used simulation extensively. Analytical results were obtained only for BEC, e.g. duality and area theorems proved in [1]. The reason for this is that the BEC EXIT function of a code is completely defined by its combinatorial properties. An expression for the EXIT function of a code over BEC based on its information function, which is strongly connected to distributions of generalized Hamming weights of the code, was derived in [1]. Here we use a different technique for computing the extrinsic information over BEC that allows us to draw a connection between the EXIT functions over BEC and over other BMS channels. We define an alternative decoder called the pseudo MAP (pMAP) decoder. We show that in the case of BEC the outputs of MAP and pMAP decoders are identical under assumption that the all-zero codeword is transmitted. We then use the pseudo MAP decoder for deriving expressions for EXIT functions in various scenarios.

Let D_{EMAP} be the extrinsic output of MAP decoder (1) after the following change of measure:

$$D_{EMAP,j} = 1 + T_{EMAP,j} = 1 + \frac{\sum_{i\in I_j^{(1)}}\prod_{l=1,l\neq j}^{n} T_l^{c_{i,l}^{\perp}}}{\sum_{i\in I_j^{(0)}}\prod_{l=1,l\neq j}^{n} T_l^{c_{i,l}^{\perp}}} \quad (5)$$

The extrinsic output of pMAP decoder is defined as follows:

$$D_{EpMAP,j} = \prod_{S\in P(I_j^{(1)})\setminus\emptyset}\left(1+\prod_{l=1,l\neq j}^{n} T_l^{\bigvee_{q\in S}\left(c_{q,l}^{\perp}\right)}\right)^{(-1)^{|S|+1}}, \quad (6)$$

where, $\bigvee$ denotes the OR operator.

Example 1: Consider a $[5,3]$ linear block code with the following dual code: $\{\overbrace{00000}^{1},\overbrace{01110}^{2},\overbrace{11001}^{3},\overbrace{10111}^{4}\}$. For this code $I_1^{(1)}=\{3,4\}$ and $P(I_1^{(1)})\setminus\emptyset = \{\{3\},\{4\},\{3,4\}\}$. Thus, the extrinsic outputs of the MAP decoder and pMAP decoder for the first bit are given by:

$$\begin{aligned} D_{EMAP,1} &= 1+\frac{T_2T_5+T_3T_4T_5}{1+T_2T_3T_4} \\ &= \frac{1+T_2T_3T_4+T_2T_5+T_3T_4T_5}{1+T_2T_3T_4}, \\ D_{EpMAP,1} &= \frac{(1+T_2T_5)(1+T_3T_4T_5)}{(1+T_2T_3T_4T_5)}. \end{aligned}$$

Example 2: For the $[n,n-1]$ single parity-check code, MAP and pMAP decoders coincide:

$$D_{EMAP,j} = D_{EpMAP,j} = 1+\prod_{l=1,l\neq j}^{n} T_l.$$

Example 3: For the $[3,1]$ repetition code, MAP and pMAP decoders coincide. For instance, the extrinsic output for the first bit is given by:

$$D_{EMAP,1} = D_{EpMAP,1} = \frac{(1+T_2)(1+T_3)}{(1+T_2T_3)}.$$

Proposition 4.1: In BEC under assumption that the all-zero codeword is transmitted $D_{EMAP} = D_{EpMAP}$.

Proof: If the all-zero codeword is transmitted over BEC, then the variables

$$\begin{aligned} T_l &= Pr(X_l=1|Y_l) - Pr(X_l=-1|Y_l) \\ T_{EMAP,j} &= Pr(X_j=1|\underline{Y}_{[j]}) - Pr(X_j=-1|\underline{Y}_{[j]}) \end{aligned}$$

can take only on two values, 0 or 1. According to (1) the numerator of $T_{EMAP,j}$ is a sum of products of the form $a_i = \prod_{l=1,l\neq j}^{n} T_l^{c_{i,l}^{\perp}}$. First, let us assume that all $a_i = 0$. Then $T_{EMAP,j}=0$ and therefore $D_{EMAP,j}=1$. In this case all the factors $b_S = \prod_{l=1,l\neq j}^{n} T_l^{\bigvee_{q\in S}\left(c_{q,l}^{\perp}\right)}$ that appear in $D_{EpMAP,j}$ are also 0, and $D_{EpMAP,j}=1$. Let now m of a_i terms be 1's. In this case the numerator of $T_{EMAP,j}$ equals m, and since $T_{EMAP,j}$ can be equal only 0 or 1, we conclude that the denominator of $T_{EMAP,j}$ must be m as well. Thus, $T_{EMAP,j}=1$ and $D_{EMAP,j}=2$. At the same time exactly $\sum_{\substack{0<|S|\leq m\\ |S| \text{ is odd,}}}\binom{m}{|S|} = 2^{m-1}$ of b_S's in the numerator of (6) and exactly $\sum_{\substack{0<|S|\leq m\\ |S| \text{ is even,}}}\binom{m}{|S|} = 2^{m-1}-1$ of b_S's in the denominator of (6) are 1. Thus $D_{EpMAP,j} = \frac{2^{2^{m-1}}}{2^{2^{m-1}-1}} = 2$ and $D_{EMAP,j} = D_{EpMAP,j}$. □

Remark: Similar to the definition of D_{EpMAP}, other decoders which coincide with the MAP decoder over the BEC can be defined. For example,

$$D_{EpMAP2,j} = \prod_{S\in P(I_j^{(1)})\setminus\emptyset}\left(1+\prod_{l=1,l\neq j}^{n} T_l^{\sum_{i\in S}\left(c_{i,l}^{\perp}\right)}\right)^{(-1)^{|S|+1}} \quad (7)$$

It can be shown that $D_{EMAP} = D_{EpMAP2}$ assuming *an arbitrary* codeword $c \in C$ was transmitted over BEC. However, since according to Theorem 3.5, extrinsic information can be computed assuming that the all-zero

codeword was transmitted, D_{EpMAP} is sufficient (and easier to use) and D_{EpMAP2} does not seem to give any added value.

Next, we use Proposition 4.1 in order to compute EXIT functions over BEC. Let $P_j = P(I_j^{(1)}) \setminus \emptyset$ and $S \in P_j$. The following definitions will be used:

- $Supp(S) = \{l \in \{1,\ldots,n\} | \bigvee_{q\in S} c_{q,l}^{\perp} = 1\}$
- $A_{i,j}^{odd} = |\{S \in P_j \mid \ |Supp(S)| = i, \ |S| \text{ is odd}\}|$
- $A_{i,j}^{even} = |\{S \in P_j \mid \ |Supp(S)| = i, \ |S| \text{ is even}\}|$

It is easy to see that $A_{i,j}^{odd} = A_{i,j}^{even} = 0$ for $i < d_{min}^{\perp}$, where $d_{min}^{\perp}$ is the dual code's minimum distance.

Proposition 4.2: The extrinsic information over BEC with erasure probability ϵ at the output of MAP decoder for a linear block code is given by:

$$\begin{aligned} I_{E_j}^{BEC} &= \sum_{S\in P_j} (-1)^{|S|+1}(1-\epsilon)^{|Supp(S)|-1} \\ &= \sum_{i=d_{min}^{\perp}}^{n} \left(A_{i,j}^{odd} - A_{i,j}^{even}\right)(1-\epsilon)^{i-1}. \end{aligned}$$

Proof: In BEC, under assumption that $X = 1$ was transmitted all the moments of r.v. $T = Pr(X = 1|Y) - Pr(X = -1|Y)$ are the same,

$$\begin{aligned} E[T^i] &= \int_{-1}^{+1} t^i f_{T|1}(t)dt \\ &= 1^i \cdot Pr(T = 1|X = 1) + 0^i \cdot Pr(T = 0|X = 1) \\ &= 1-\epsilon, \qquad i = 1,2,\ldots,\infty. \end{aligned} \tag{8}$$

Furthermore, note that

$$\begin{aligned} \log_2(1+x)|_{x=1} &= \frac{1}{\ln 2}\sum_{i=1}^{\infty}(-1)^{i+1}\frac{1}{i}x^i|_{x=1} \\ &= \frac{1}{\ln 2}\sum_{i=1}^{\infty}\frac{1}{(2i)(2i-1)} = 1 \end{aligned} \tag{9}$$

Thus, $I_{E_j}^{BEC}$

$$\begin{aligned} &= E_{T_{EMAP,j}|c_0}\left[\log_2(1+T_{EMAP,j})\right] \\ &= E_{T_{EMAP,j}|c_0}\left[\log_2(D_{EpMAP,j})\right] \\ &= E_{\underline{T}|c_0}\left[\log_2\left(\prod_{S\in P_j}\left(1+\prod_{l=1,l\neq j}^{n} T_l^{\bigvee_{q\in S}\left(c_{q,l}^{\perp}\right)}\right)^{(-1)^{|S|+1}}\right)\right] \\ &= \sum_{S\in P_j}(-1)^{|S|+1}E_{\underline{T}|c_0}\left[\log_2\left(1+\prod_{l=1,l\neq j}^{n} T_l^{\bigvee_{q\in S}\left(c_{q,l}^{\perp}\right)}\right)\right] \\ &= \sum_{S\in P_j}(-1)^{|S|+1}\frac{1}{\ln 2}\sum_{i=1}^{\infty}\frac{1}{(2i)(2i-1)}E\left(\left[\prod_{l\neq j} T_l^{\bigvee_{q\in S}\left(c_{q,l}^{\perp}\right)}\right]^{2i}\right) \\ &= \sum_{S\in P_j}(-1)^{|S|+1}\frac{1}{\ln 2}\sum_{i=1}^{\infty}\frac{1}{(2i)(2i-1)}\prod_{l\neq j}\left(E[T_l^{2i}]\right)^{\bigvee_{q\in S}\left(c_{q,l}^{\perp}\right)} \\ &= \sum_{S\in P_j}(-1)^{|S|+1}\frac{1}{\ln 2}\sum_{i=1}^{\infty}\frac{1}{(2i)(2i-1)}[E(T^{2i})]^{|Supp(S)|-1} \\ &= \sum_{S\in P_j}(-1)^{|S|+1}(1-\epsilon)^{|Supp(S)|-1} \\ &= \sum_{i=1}^{n}\left(A_{i,j}^{odd} - A_{i,j}^{even}\right)(1-\epsilon)^{i-1}. \end{aligned}$$

The first equality follows from Theorem 3.5. The second equality follows from Proposition 4.1. The fifth equality follows from noticing that $\prod_{l=1,l\neq j}^{n} T_l^{\bigvee_{q\in S}\left(c_{q,l}^{\perp}\right)}$ is the output of the MAP decoder of a single parity-check code and using Theorem 3.5. The sixth equality follows from the fact that the channel is memoryless. The seventh equality follows by assuming that the all-zero codeword was transmitted. The eighth equality follows from (8) and (9). □

Proposition 4.2 can be easily generalized to handle a scenario in which each bit is transmitted through a different BEC channel. In that case we will characterize the BEC by a vector of erasure probabilities $\underline{\epsilon} = [\epsilon_, \ldots, \epsilon_n]$.

Proposition 4.3: Let a linear block code be used over BEC such that the l'th bit in the codeword has an erasure probability ϵ_l. The extrinsic information at the output of the MAP decoder is given by:

$$I_{E_j}^{BEC}(\underline{\epsilon}) = \sum_{S\in P_j}(-1)^{|S|+1}\prod_{l=1,l\neq j}^{n}(1-\epsilon_l)^{\bigvee_{q\in S}\left(c_{q,l}^{\perp}\right)}.$$

□

We finish this section by drawing a connection between the EXIT function over a BMS channel and the EXIT function over BEC.

Theorem 4.4: Let C be a linear code transmitted over a BMS channel for which $D_{EMAP} = D_{EpMAP}$. Then

$$I_{E_j}^{BMS} = I(X_j; \underline{Y}_{[j]}) = \frac{1}{\ln 2}\sum_{i=1}^{\infty}\frac{1}{(2i-1)(2i)}I_{E_j}^{BEC}(\underline{\epsilon}_i),$$

where $I_{E_j}^{BEC}(\epsilon_i)$ is the j'th bit extrinsic information at the output of MAP decoder for the code C over BEC with erasure probabilities $\underline{\epsilon}_i$, and $\underline{\epsilon}_i = 1 - E(\underline{T}^{2i})$.

Proof:

$$\begin{aligned} I_{E_j}^{BMS} &= \sum_{S\in P_j}(-1)^{|S|+1}\frac{1}{\ln 2}\sum_{i=1}^{\infty}\frac{1}{(2i)(2i-1)}\prod_{l\neq j}\left(E[T_l^{2i}]\right)^{\bigvee_{q\in S}\left(c_{q,l}^{\perp}\right)} \\ &= \frac{1}{\ln 2}\sum_{i=1}^{\infty}\frac{1}{(2i)(2i-1)}\sum_{S\in P_j}(-1)^{|S|+1}\prod_{l\neq j}\left(E[T_l^{2i}]\right)^{\bigvee_{q\in S}\left(c_{q,l}^{\perp}\right)} \\ &= \frac{1}{\ln 2}\sum_{i=1}^{\infty}\frac{1}{(2i)(2i-1)}I_E^{BEC}(\underline{\epsilon}_i = 1 - E(\underline{T}^{2i})) \end{aligned}$$

The first equality follows from similar arguments to the ones used in the proof of Proposition 4.2. The third equality follows from Proposition 4.3. □

We conclude from Theorem 4.4 that for capacity approaching code families, the pseudo MAP and MAP decoders can coincide only if the code rate approaches 1. Indeed, a random code with a rate R below the channel capacity C has the decoding error probability approaching zero. In order to achieve the zero error probability we should have $I_E^{BMS} = 1$. However, by Theorem 4.4 this implies that $I_E^{BEC}(\epsilon_i) = 1$ for all i, but $\epsilon_i = 1 - E(T^{2i})$ are the series of erasure probabilities that increases and tends to 1 for any channel with capacity less than 1. At the same time we would like to note that the EXIT function of a random code of rate $0 < R < 1$ of growing length is known. It approaches a step function that jumps from 0 to 1 at $I_A = R$. Thus the problem of estimating the EXIT

function $I_E(I_A)$ is non-trivial only for codes of finite length or "bad" codes of infinite length.

Theorem 4.4 yields exact expressions for EXIT functions of single parity check codes and the length 3 repetition code for any BMS channel, since the pMAP decoder and MAP decoders of these codes coincide (see Examples 2,3).

Theorem 4.5: The extrinsic information at the output of MAP decoder of an $[n, n-1]$ single parity-check code transmitted over a BMS channel is given by:

$$I_E = I(X; T_{EMAP}) = \frac{1}{\ln 2} \sum_{i=1}^{\infty} \frac{1}{(2i-1)(2i)} [E(T^{2i})]^{n-1}.$$

Proof: Using Proposition 4.2 (or using techniques from [1]) for a $[n, n-1]$ single parity-check code we get:

$$I_{E_j}^{BEC}(\epsilon) = (1-\epsilon)^{n-1} \tag{10}$$

Plugging (10) into Theorem 4.4 completes the proof. □

Using Theorems 4.4 and 4.5 we can accurately compute the extrinsic information of a single parity-check code and a length 3 repetition code for any BMS channel. These can be utilized for the analysis of iterative codes using Gaussian approximation of the Density Evolution algorithm based on the mutual information measure as described in [10].

V. Approximation of the extrinsic information over biAWGN channel

The biAWGN channel is characterized by the parameter $\frac{E_s}{N_0}$ or $\frac{E_b}{No}$, where E_s is the energy received per symbol, E_b is the received information bit energy ($E_s = E_b R$, where R is the code's rate) and $N_0/2$ is the one-sided spectral noise density. Let Y denote the biAWGN channel output (matched filter output) for a transmitted bit X, and let $L = \log \frac{Pr(X=1|Y)}{Pr(X=-1|Y)}$, $T = Pr(X=1|Y) - Pr(X=-1|Y)$ denote the LLR and "soft bit" estimates of X respectively. For biAWGN channel $L = \frac{4}{N_0} Y$, thus $L|X=1$ is a Gaussian r. v. distributed as $f_{L|1}(l) = \frac{1}{\sqrt{4\pi m}} e^{-\frac{(l-m)^2}{4m}}$, where $m = 4\frac{E_s}{N_0}$ is the expectation of $L|X=1$ (i.e. $L|X=1 \sim \mathcal{N}(m, 2m)$). The mutual information between X and L as a function of m is [1]:

$$J(m) = I(X;L) = \int_{\mathcal{R}} \frac{1}{\sqrt{4\pi m}} e^{-\frac{(l-m)^2}{4m}} \left(1 - \log_2(1+e^{-l})\right) dl \tag{11}$$

The $2i$'th moment of $T|X=1$ as a function of m can be computed using (4):

$$\Phi_i(m) = \mathbf{E}(T^{2i}) = \int_{-1}^{+1} \frac{2t^{2i}}{(1-t^2)\sqrt{4\pi m}} e^{-\frac{(\ln \frac{1+t}{1-t} - m)^2}{4m}} dt. \tag{12}$$

In the previous section we proved that for any code, if the all-zero codeword is transmitted over BEC, the extrinsic outputs of MAP decoder and pMAP decoder are identical. Furthermore, for the single parity check codes and for the length 3 repetition code pMAP and MAP decoders are identical in any BMS channel (see Examples 2,3). Simulation results show that in AWGN channel the outputs of these decoders are very close to each other for other high rates codes as well. For instance, in Figure 1 we present results of simulation of 100 decodings of the $[7, 4]$ Hamming code for the AWGN channel with the input (channel) mutual information $I_A = 0.75$. On the axis X we put the decoding index and on the axis Y the outputs of decoders D_{EMAP} and D_{EpMAP} defined in (5) and (6) respectively. One can see that the outputs of the decoders are almost indistinguishable. Based on these results we arrive

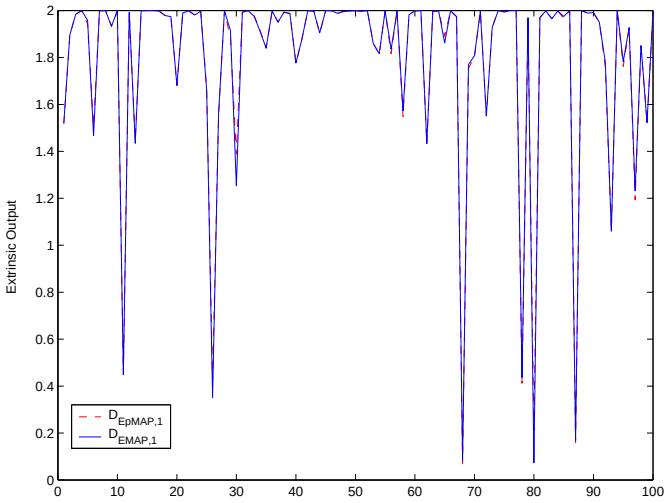


Fig. 1. Comparison between the extrinsic MAP and pseudoMAP decoders for a $[7, 4]$ Hamming code over a biAWGN with $E_b/N_o = 1.5519dB$ (corresponding to $I_A = 0.75$)

at the following conjecture.

Conjecture 5.1: For high rate codes, when the all-zero codeword is transmitted over the biAWGN channel $D_{EMAP} \cong D_{EpMAP}$.

Using Theorem 4.4 we can obtain the following corollary

Corollary 5.2: Let C be a linear code such that in biAWGN channel $D_{EMAP} \cong D_{EpMAP}$. Then

$$I_{E_j}^{biAWGN}(\frac{E_s}{N_0}) \cong \frac{1}{\ln 2} \sum_{i=1}^{\infty} \frac{1}{(2i-1)(2i)} I_{E_j}^{BEC}(\epsilon_i), \tag{13}$$

where $I_{E_j}^{BEC}(\epsilon_i)$ is the j'th bit extrinsic information at the output of MAP decoder for the code C over BEC with erasure probability ϵ_i, and

$$\epsilon_i = 1 - \Phi_i(4\frac{E_s}{N_0})$$

Proof: For the biAWGN $E(T^{2i}) = \Phi_i(4\frac{E_s}{N_0})$. Using Theorem 4.4 completes the proof. □

Figure 2 shows estimates for the EXIT functions of the Hamming codes of length 31 and 127 over a biAWGN channel obtained by simulations and according to Corollary 5.2. One can see that the results support Conjecture 5.1 and the curves are quite close.

In [1] it was shown that in BEC the EXIT functions of a linear code and its dual code are connected by the equality:

$$I_E^{BEC\perp}(I_A) = 1 - I_E^{BEC}(1 - I_A). \tag{14}$$

It is tempting to conjecture that this relation is approximately valid in biAWGN channel as well. Combining (14), Corollary 5.2 and (11) we obtain the following corollary:

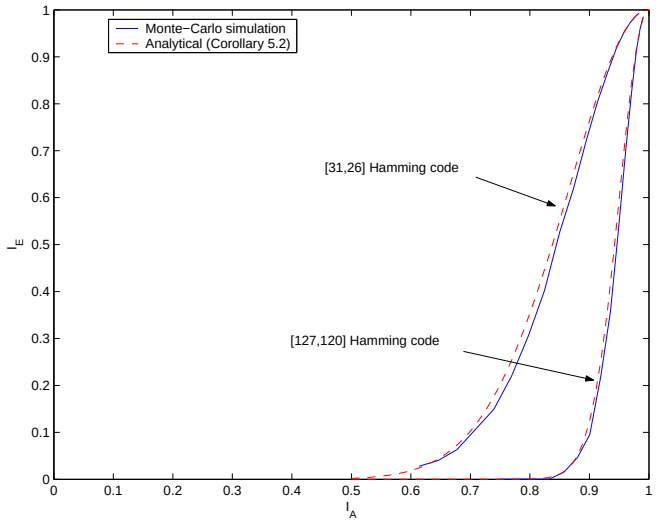


Fig. 2. Comparison between the EXIT functions of a $[31, 26]$ and a $[127, 120]$ Hamming codes over a biAWGN channel obtained by Monte-Carlo simulation and analytically according to Corollary 5.2

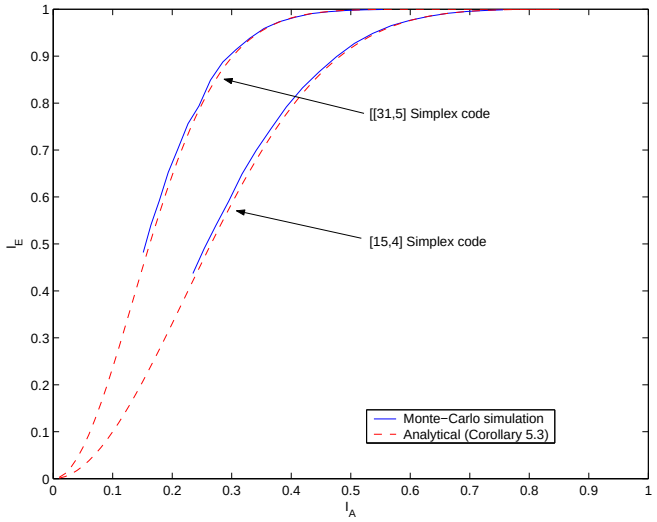


Fig. 3. Comparison between the EXIT functions of a $[15, 4]$ and a $[31, 5]$ Simplex codes over a biAWGN channel obtained by Monte-Carlo simulation and analytically according to Corollary 5.3

Corollary 5.3: Let C be a linear code such that for the dual code $C^{\perp}$ in biAWGN channel $D_{EMAP} \cong D_{EpMAP}$. Then the EXIT function of C over the biAWGN channel can be approximated by:

$$\begin{aligned} I_{E_j}^{biAWGN}(\frac{E_s}{N_0}) &\cong 1 - I_{E_j}^{\perp,biAWGN}(\frac{1}{4}J^{-1}(1-J(4\frac{E_s}{N_0}))) \\ &\cong 1 - \frac{1}{\ln 2}\sum_{i=1}^{\infty}\frac{1}{(2i-1)(2i)} I_{E_j}^{\perp,BEC}(\epsilon_i), \end{aligned}$$

where $I_{E_j}^{\perp,BEC}(\epsilon_i)$ is the j'th bit extrinsic information at the output of MAP decoder for the dual code over BEC with erasure probability ϵ_i, and

$$\epsilon_i = 1 - \Phi_i(J^{-1}(1 - J(4\frac{E_s}{N_0})))$$

□

Assuming Conjecture 5.1 is valid Corollary 5.3 can be used for estimating the EXIT functions of low rate codes such as Simplex codes or first order Reed-Muller codes. Figure 3 shows the EXIT functions of Simplex codes of lengths 15 and 31 obtained by simulations and from Corollary 5.3.

A. Estimating the Bit Error Rate (BER) at the output of MAP decoder over AWGN channel

Simulations for AWGN channel show that the conditional probability density functions of the r. v.'s $L_{EMAP,j}|X = 1$ are very close to the Gaussian density function. Hence, using the value $I_E^{biAWGN}(E_s/N_0)$ and (11), one can compute the bit error probability of MAP decoding as follows

$$P_b = Q\left(\sqrt{2\left(\frac{E_s}{N_0} + \frac{1}{4}J^{-1}(I_E^{biAWGN}(\frac{E_s}{N_0}))\right)}\right), \quad (15)$$

where

$$Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^{\infty} e^{-t^2/2}dt.$$

One can suggest to estimate $I_E^{biAWGN}(E_s/N_0)$ as $I_E^{BEC}(I_A = J(4\frac{E_s}{N_0}))$, i.e. assuming the BEC and biAWGN EXIT functions are approximately the same. However, as suggested by Figures 4 and 5 this assumption leads to less accurate results compared to using Corollaries 5.2 and 5.3. Figures 4, 5 show estimates of BER curves for length 31 Hamming and Simplex codes obtained in three ways: 1) by Monte-Carlo simulation 2) using (15), where $I_E^{biAWGN}(E_s/N_0)$ is estimated according to Corollaries 5.2 and 5.3 3) using (15), where $I_E^{biAWGN}(E_s/N_0)$ is estimated as $I_E^{BEC}(I_A = J(4\frac{E_s}{N_0}))$.

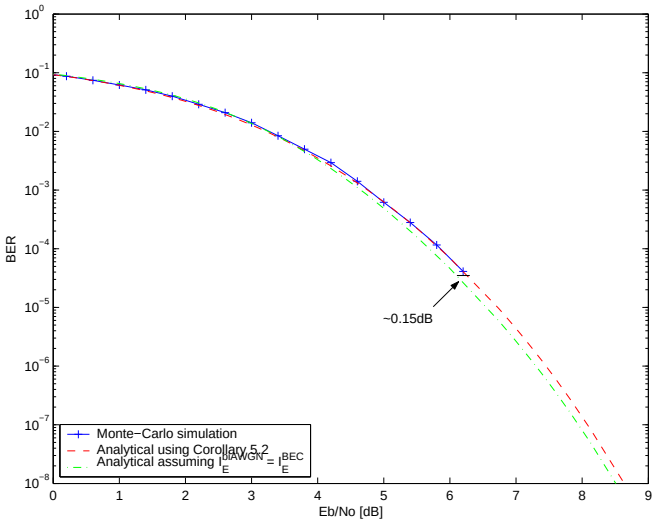


Fig. 4. Comparison between the BER curves of a $[31, 26]$ Hamming code over a biAWGN channel obtained by Monte-Carlo simulation, analytically according to Corollary 5.2 and analytically assuming $I_E^{biAWGN}(E_s/N_0) = I_E^{BEC}(I_A = J(4\frac{E_s}{N_0}))$

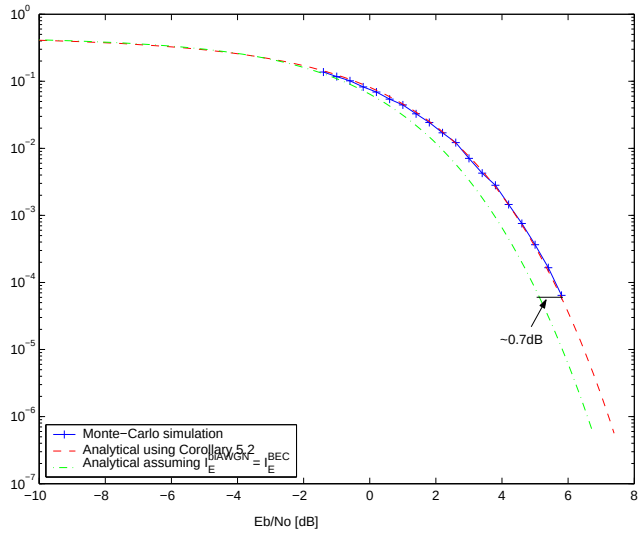


Fig. 5. Comparison between the BER curves of a $[31, 5]$ Simplex code over a biAWGN channel obtained by Monte-Carlo simulation, analytically according to Corollary 5.2 and analytically assuming $I_E^{biAWGN}(E_s/N_0) = I_E^{BEC}(I_A = J(4\frac{E_s}{N_0}))$

VI. Conclusion

We derive an expression for the extrinsic information at the output of the MAP decoder for a linear block code as a function of moments of its "soft bit" extrinsic output. It is used for computing EXIT functions over BEC by defining a pseudo-MAP decoder that coincides with the MAP decoder when the zero codeword is transmitted over BEC. Furthermore, when the pseudo-MAP and MAP decoders coincide, we express the EXIT function of the code over a BMS channel as a function of its EXIT function over the BEC. This allows us to compute EXIT functions for single-parity check codes and the length 3 repetition code over any BMS channel that can be used for analysis of LDPC codes under iterative decoding [10]. Finally, based on the EXIT functions over BEC we derived accurate approximations for EXIT functions and bit error rate curves of high and low rate codes, such as Hamming and Simplex codes, over the biAWGN channel. These can be utilized for analysis of iterative coding schemes such as product codes, block turbo codes and generalizations of LDPC codes.

Acknowledgment

We express our gratitude to Igal Sason and the reviewers of the paper for their constructive comments and suggestions.

References

[1] A.Ashikmin, G.Kramer, S.ten Brink, "Extrinsic Information Transfer Functions: Model and Erasure Channel Property", *IEEE Trans. Inform. Theory*, vol. 50, 11, pp. 2657-2673, 2004.

[2] C.Berrou, A. Glavieux, and P.Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes", *in Proc. IEEE Int. Conf. Commun.*, Geneva, Switzerland, pp. 1064-1070, 1993.

[3] S.ten Brink, "Convergence of iterative decoding", *Electron. Lett*, vol. 35, 10, pp. 806-808, 1999.

[4] R.G.Gallager, *Low-Density Parity-Check Codes*, Cambridge, MA: MIT Press 1963.

[5] R.W.Hamming *Coding and Information Theory.* Prentice-Hall, New Jersey, 1986.

[6] C.R.Hartmann and L.D.Rudolph, "An optimum symbol-by-symbol decoding rule for linear codes", *IEEE Trans. Inform. Theory*, vol. 22, 5, pp. 514-517, 1976.

[7] I.Land, P.A.Hoeher, S.Huettinger and J.Huber, "Bounds on information combining", in *Proc. of the 3rd Int. Symp. on Turbo Codes and Related Topics*, Brest, France, pp. 39-42, Sep 1-5, 2003.

[8] T.J.Richardson and R.Urbanke, "The capacity of low-density parity-check codes under message passing decoding", *IEEE Trans. Inform. Theory*, vol. 47, 2, pp. 599-618, 2001.

[9] T.J.Richardson, A.Shokrollahi and R.Urbanke, "Design of capacity approaching irregular low-density parity-check codes", *IEEE Trans. Inform. Theory*, vol. 47, 2, pp. 619-637, 2001.

[10] E.Sharon, A.Ashikhmin, and S.Litsyn, "Analysis of Low-Density Parity-Check codes based on EXIT functions," submitted to *IEEE Trans. Commun*.

[11] I.Sutskover, S.Shamai and J.Ziv, "Extremes of information combining", *IEEE Trans. Inform. Theory*, vol. 51, 4, pp. 1313-1325, 2005.