Some Properties of Bit Decoding Algorithms for Binary Linear Block Codes

Ali Abedi and Amir K. Khandani

Coding & Signal Transmission Laboratory

Department of Electrical & Computer Engineering

University of Waterloo

Waterloo, Ontario, Canada, N2L 3G1

Technical Report UW-E&CE#2003-5

May 8, 2003

Some Properties of Bit Decoding Algorithms for Binary Linear Block Codes

Ali Abedi and Amir K. Khandani

Coding & Signal Transmission Laboratory(www.cst.uwaterloo.ca)

Dept. of Elec. and Comp. Eng., University of Waterloo, Waterloo, ON, Canada, N2L 3G1

e-mail: ali, khandani@cst.uwaterloo.ca, Tel: 519-8848552, Fax: 519-8884338

Abstract

In this paper, we study certain properties of the bit decoding algorithms for the case of binary linear block codes. Our focus is on the Probability Density Function (pdf) of the bit Log-Likelihood-Ratio (LLR). A general channel model with discrete input and discrete or continuous output is considered. We prove that under a set of mild conditions on the channel, the pdf of the bit LLR of a specific bit position is independent of the transmitted code-word. It is also shown that the pdf of a given bit LLR when the corresponding bit takes the values of zero and one are symmetric with respect to each other (reflection of one another with respect to the origin). For the case of channels with binary input, a sufficient condition for two bit positions to have the same pdf is presented.

Index Terms

Bit Decoding, Block Codes, Geometrically Uniform, Log-Likelihood Ratio, Probability Density Function, Regular Channel, Symmetric Channel.

I. Introduction

In the application of channel codes, one of the most important problems is to develop an efficient decoding algorithm for a given code. The class of Maximum Likelihood (ML)

decoding algorithms are designed to find a valid code-word with the maximum likelihood value. The ML algorithms are known to minimise the probability of the Frame Error Rate (FER) under the mild condition that the code-words occur with equal probability.

Another class of decoding algorithms, known as bit decoding, compute the probability of the individual bits and decide on the corresponding bit values independent of each other. The straightforward approach to bit decoding is based on summing up the probabilities of different code-words according to the value of their component in a given bit position of interest. Reference [2] provides an efficient method (known as BCJR) to compute the bit probabilities of a given code using its trellis diagram. The main simplification of BCJR has been the SOVA (Soft Output Viterbi Algorithm) [3], which is a sub-optimum solution. A reduced-search BCJR algorithm is also proposed in [4]. There are some special methods for bit decoding based on coset decomposition principle [5], sectionalised trellis diagrams [6], and using the dual code [7], [8].

Maximum Likelihood decoding algorithms have been the subject of numerous research activities, while bit decoding algorithms have received much less attention in the past. More recently, bit decoding algorithms have received increasing attention, mainly due to the fact that they deliver bit reliability information. This reliability information has been effectively used in a variety of applications including Turbo decoding.

Probability density function (pdf) of the bit Log-Likelihood-Ratio (LLR) can be used as a tool for analysis of bit decoding algorithms. A recent work [9] on analysis of Sum-Product decoding of Low-Density-Parity-Check (LDPC) codes takes advantage of certain symmetry properties for pdf of bit LLR over binary input channels with Additive White Gaussian Noise (AWGN) interference. It is shown in [10] that for a binary input, $output-symmetric$ channel defined in [11] (assuming that the all zero code-word is transmitted), the bit LLR at each node of the code graph posses a symmetric pdf (refer to [10] for the definition of symmetry) and this symmetry is preserved under belief propagation decoding. Note that the definition of "symmetry" in the current article is different from [10]. In [11], it is shown that for a binary input, $output-symmetric$

channel, the conditional probability of error is independent of the transmitted code-word. We prove a more general result concerning the invariance property of the pdf of the bit LLR in theorem 1 (note that we also use a more general channel model as compared to [11]).

This paper is organised as follows. In section II, the model used to analyse the problem is presented. All notations and assumptions are given in this section. Some theorems are proved on bit decoding algorithms in section III. We conclude in section IV. This work is a continuation of [12], in which the case of AWGN channel with Binary Phase Shift Keying (BPSK) modulation is considered.

II. MODELLING

Assume that a binary linear code $\mathcal{C}$ with code-words of length N is given. Notation $\mathbf{c}^i = (c_1^i, c_2^i, \ldots, c_N^i)$ is used to refer to the i^{th} code-word and its elements. We partition the code into a sub-code C_k^0 and its coset C_k^1 according to the value of the k^{th} bit position of its code-words. i.e.,

$$\forall \mathbf{c}^i \in \mathcal{C} : \begin{cases} c_k^i = 0 \Longrightarrow \mathbf{c}^i \in C_k^0, \\ c_k^i = 1 \Longrightarrow \mathbf{c}^i \in C_k^1, \end{cases} \tag{1}$$

$$C_k^0 \cup C_k^1 = \mathcal{C}, \qquad C_k^0 \cap C_k^1 = \varnothing. \tag{2}$$

We denote bit wise binary addition of two code-words on the code book as, $\mathbf{c}^i \oplus \mathbf{c}^j$. Note that the sub-code C_k^0 is closed under binary addition. Each code-word will be partitioned into L blocks of m bits, assuming $N = mL$, to be transmitted over a channel with a discrete input alphabet set composed of 2^m elements. Notation $\mathbf{I}_j^i$, $i = 1, \ldots, |\mathcal{C}|$, $j = 1, \ldots, L$, is used for these blocks, which will be called m-blocks hereafter. For example, code-word $\mathbf{c}^i$ is composed of $(\mathbf{I}_1^i, \mathbf{I}_2^i, \ldots, \mathbf{I}_L^i)$. We assume that there exists a one to one correspondence between the 2^m possible m-blocks and the input symbols of the channel. The set of m-blocks referred as $\mathcal{I}$ forms a group under binary addition.

The channel has 2^m discrete input and discrete or continuous output as shown in Figure 1. For channels with discrete output, $\mathcal{O}$ is a set of discrete alphabets and $p(.)$ stands for the probability mass function (pmf). For the continuous output channels, $\mathcal{O} \subset \Re^n$, where $\Re$ is the set of real numbers and $p(.)$ stands for pdf.

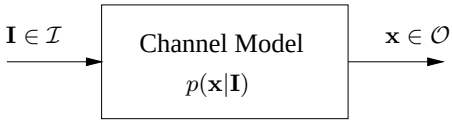

Fig. 1. Channel Model

Consider the situation of sending a code-word $\tilde{\mathbf{c}} = (\tilde{\mathbf{I}}_1, \ldots, \tilde{\mathbf{I}}_L)$ through the channel. Each m-block, $\tilde{\mathbf{I}}_j$, $j = 1 \ldots L$, will be transmitted and a symbol $\mathbf{x}_j$, $j = 1 \ldots L$, will be received at the channel output. A common tool to express the bit probabilities in bit decoding algorithms is based on using the so-called Log-Likelihood-Ratio (LLR). The LLR of the k^{th} bit position is defined by the following equation,

$$LLR_{\tilde{\mathbf{c}}}(k) = \log \frac{P(\tilde{c}_k = 1|\mathbf{x}_1 \ldots \mathbf{x}_L)}{P(\tilde{c}_k = 0|\mathbf{x}_1 \ldots \mathbf{x}_L)}, \tag{3}$$

where $\tilde{c}_k$ is the value of the k^{th} bit in the transmitted code-word and $\log$ stands for natural logarithm. Assuming,

$$P(\tilde{c}_k = 0) = P(\tilde{c}_k = 1) = \frac{1}{2}, \tag{4}$$

for a memoryless channel we have,

$$LLR_{\tilde{\mathbf{c}}}(k) = \log \frac{\sum\limits_{\mathbf{c}^i \epsilon C_k^1} p(\mathbf{x}_1 \ldots \mathbf{x}_L|\mathbf{c}^i)}{\sum\limits_{\mathbf{c}^i \epsilon C_k^0} p(\mathbf{x}_1 \ldots \mathbf{x}_L|\mathbf{c}^i)} = \log \frac{\sum\limits_{\mathbf{c}^i \epsilon C_k^1} \prod\limits_{j=1}^{L} p(\mathbf{x}_j|\mathbf{I}_j^i)}{\sum\limits_{\mathbf{c}^i \epsilon C_k^0} \prod\limits_{j=1}^{L} p(\mathbf{x}_j|\mathbf{I}_j^i)}. \tag{5}$$

We are interested in studying the probabilistic behaviour of the LLR.

Assuming a linear code, we derive a set of conditions on the channel for which the choice of $\tilde{\mathbf{c}}$ does not have any impact on the pdf of $LLR(k)$ as long as the value of the

k^{th} bit remains unchanged. This is a generalisation of the distance invariance property at the bit level. It will be also shown that, under the same set of conditions, the pdf of a given bit LLR when the corresponding bit takes the values of zero and one are symmetric with respect to each other (reflection of one another with respect to the origin). For the case of channels with binary input a sufficient condition for the LLR of two bit positions to have the same pdf is presented.

The following sufficient condition is required to carry out the proofs.

$$\forall \tilde{\mathbf{I}} \in \mathcal{I},\ \forall \mathbf{x} \in \mathcal{O},\ \exists \mathbf{y} \in \mathcal{O} : p(\mathbf{x}|\mathbf{I} \oplus \tilde{\mathbf{I}}) = p(\mathbf{y}|\mathbf{I}),\quad \forall \mathbf{I} \in \mathcal{I}. \tag{6}$$

This is obviously equivalent to,

$$\forall \tilde{\mathbf{I}}^1, \tilde{\mathbf{I}}^2 \in \mathcal{I},\ \forall \mathbf{x} \in \mathcal{O},\ \exists \mathbf{y} \in \mathcal{O} : p(\mathbf{x}|\mathbf{I} \oplus \tilde{\mathbf{I}}^1 \oplus \tilde{\mathbf{I}}^2) = p(\mathbf{y}|\mathbf{I}),\quad \forall \mathbf{I} \in \mathcal{I}, \tag{7}$$

however, as we will see later the form given in (7) is more convenient to use in the proof of the theorems.

A. Channels with a Geometrical Representation

We use the notation $\mathbf{P}_{\mathbf{I}^i} \in \Re^n$ to refer to the channel input symbols representing $\mathbf{I}^i$. In this case, the m-blocks are just labels of the points in an Euclidean space. We assume that the signal set at the channel input is geometrically uniform [13]. This means that for any given pair of signal points, say $\mathbf{P}_{\tilde{\mathbf{I}}^1}$ and $\mathbf{P}_{\tilde{\mathbf{I}}^2}$, there exists an isometry which transforms $\mathbf{P}_{\tilde{\mathbf{I}}^1}$ to $\mathbf{P}_{\tilde{\mathbf{I}}^2}$ while leaving the signal set unchanged. In addition, we assume that the scenario shown in Figure 2 is valid for the corresponding labels.

It is easy to see that under the following conditions,
(i) $\mathbf{y}$ is selected as the image of $\mathbf{x}$ under the isometry $\mathbf{P}_{\tilde{\mathbf{I}}^1} \Longrightarrow \mathbf{P}_{\tilde{\mathbf{I}}^2}$
(ii) $p(\mathbf{x}|\mathbf{P}_{\tilde{\mathbf{I}}^1})$ is a function of $\|\mathbf{x} - \mathbf{P}_{\tilde{\mathbf{I}}^1}\|,\ \forall \mathbf{x},\ \forall \mathbf{P}_{\tilde{\mathbf{I}}^1}$
the condition given in (7) will be satisfied. A well known example for a channel satisfying condition (ii), is the AWGN channel.

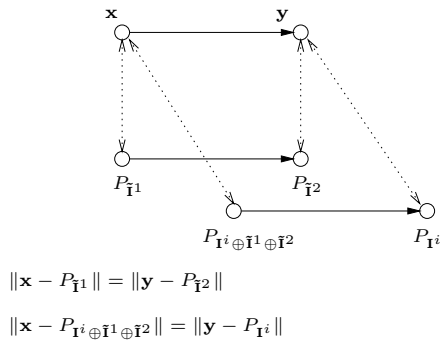

Fig. 2. Mapping of points with an isometry

B. Channels without Geometrical Representation

In this section, we assume that the channel output set is a discrete set composed of elements $\mathbf{x}^j \in \mathcal{O}$. The Channel is characterised by matrix of transition probabilities, $\mathbf{A}$.

$$\mathbf{A}_{u\times v} = [a_{ij}], \quad a_{ij} = p(\mathbf{x}^j|\mathbf{I}^i), \quad u = 2^m = |\mathcal{I}|,\ v = |\mathcal{O}|. \tag{8}$$

We can satisfy the condition given in (7), if after permuting all input symbols by adding an arbitrary m-block $\mathbf{I}$ to them, for each column in $\mathbf{A}_{u\times v}$, there exists another column for which the probability values are shuffled in the same order as the corresponding m-blocks. It appears that our channel model is a $Regular$ channel [1]. Reference [14] defines the concept of the $Regular$ channel as follows. Assume that permutation $\psi_{\mathbf{I}}$ acts on the set $\mathcal{O}$ with the property,

$$\forall\ \mathbf{I}^1, \mathbf{I}^2 \in \mathcal{I},\ \forall\ \mathbf{x}^j \in \mathcal{O}\ \ \psi_{\mathbf{I}^1}(\psi_{\mathbf{I}^2}(\mathbf{x}^j)) = \psi_{\mathbf{I}^1 \oplus \mathbf{I}^2}(\mathbf{x}^j). \tag{9}$$

The channel is called a $Regular$ channel, if the probability $p(\mathbf{x}^j|\mathbf{I}^i)$ only depends on $\psi_{\mathbf{I}^i}(\mathbf{x}^j)$. It can be verified easily that a $Regular$ channels is always $Symmetric$ in sense of Gallager [15], where in [15] the symmetry condition only involves the channel symbols and not the underlying labelling. For a recent introduction to the $Regular$ channels refer to [16].

[1]The authors would like to thank G. D. Forney for his invaluable comments on an earlier version of this article, including pointing out references [9], [14], [16].

Here are some examples for the discrete case.

Example 1: For the channel shown in Figure 3 we have,

$$\mathbf{A} = \left[\begin{array}{c|cccc} & \mathbf{x}^1 & \mathbf{x}^2 & \mathbf{x}^3 & \mathbf{x}^4 \\ \hline 0 & 1/2-\epsilon_1 & \epsilon_1 & 1/2-\epsilon_2 & \epsilon_2 \\ 1 & \epsilon_1 & 1/2-\epsilon_1 & \epsilon_2 & 1/2-\epsilon_2 \end{array}\right] \tag{10}$$

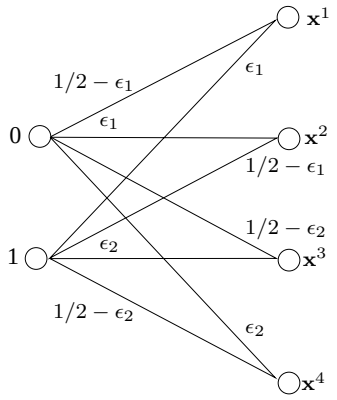

Fig. 3. Channel model for example 1.

Example 2: For the channel shown in Figure 4 we have,

$$\mathbf{A} = \left[\begin{array}{c|ccccc} & \mathbf{x}^1 & \mathbf{x}^2 & \mathbf{x}^3 & \mathbf{x}^4 & \mathbf{x}^5 \\ \hline 00 & e_0 & e_1 & \epsilon & 0 & 0 \\ 01 & e_1 & e_0 & \epsilon & 0 & 0 \\ 10 & 0 & 0 & \epsilon & e_0 & e_1 \\ 11 & 0 & 0 & \epsilon & e_1 & e_0 \end{array}\right] \tag{11}$$

where $e_0 + e_1 + \epsilon = 1$.

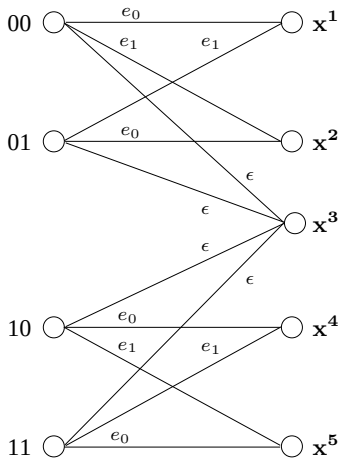

Fig. 4. Channel model for example 2.

Example 3: For the channel shown in Figure 5 we have,

$$\mathbf{A} = \left[\begin{array}{c|cccccccc} & \mathbf{x}^1 & \mathbf{x}^2 & \mathbf{x}^3 & \mathbf{x}^4 & \mathbf{x}^5 & \mathbf{x}^6 & \mathbf{x}^7 & \mathbf{x}^8 \\ \hline 00 & e_0 & e_1 & e_2 & e_3 & e_4 & e_3 & e_2 & e_1 \\ 01 & e_2 & e_1 & e_0 & e_1 & e_2 & e_3 & e_4 & e_3 \\ 10 & e_4 & e_3 & e_2 & e_1 & e_0 & e_1 & e_2 & e_3 \\ 11 & e_2 & e_3 & e_4 & e_3 & e_2 & e_1 & e_0 & e_1 \end{array}\right] \tag{12}$$

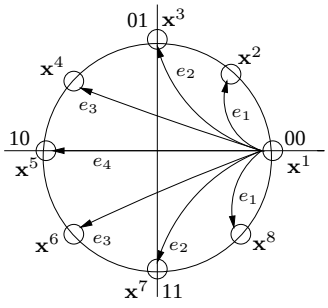

Fig. 5. Channel model for example 3: The values of error probabilities which are not shown follow the same pattern as the values specified on the figure.

where $e_0 + 2(e_1 + e_2 + e_3) + e_4 = 1$. It is easy to see that the required condition for the

columns of the probability matrix are satisfied in all of the above examples.

III. Main Results

Using the above definitions and notations, we have the following theorems.

Theorem 1: The pdf of $LLR(k)$ is not affected by the choice of the transmitted code-word $\tilde{\mathbf{c}}$, as long as the value of the k^{th} bit remains unchanged.

Proof: Consider two code-words, $\tilde{\mathbf{c}}^1, \tilde{\mathbf{c}}^2$ which have the same value in their k^{th} bit position. Let us assume that $\tilde{\mathbf{c}}^1$ is transmitted through the channel and $(\mathbf{x}_1 \dots \mathbf{x}_L)$ is received. This results in a realization of random variable $LLR_{\tilde{\mathbf{c}}^1}(k)$ with a value of,

$$LLR_{\tilde{\mathbf{c}}^1}(k) = \log \frac{\sum\limits_{\mathbf{c}^i \epsilon C_k^1} p(\mathbf{x}_1 \dots \mathbf{x}_L | \mathbf{c}^i)}{\sum\limits_{\mathbf{c}^i \epsilon C_k^0} p(\mathbf{x}_1 \dots \mathbf{x}_L | \mathbf{c}^i)} = \log \frac{\sum\limits_{\mathbf{c}^i \epsilon C_k^1} \prod\limits_{j=1}^{L} p(\mathbf{x}_j | \mathbf{I}_j^i)}{\sum\limits_{\mathbf{c}^i \epsilon C_k^0} \prod\limits_{j=1}^{L} p(\mathbf{x}_j | \mathbf{I}_j^i)}, \tag{13}$$

that occurs with probability $p(\mathbf{x}_1 \dots \mathbf{x}_L | \tilde{\mathbf{c}}^1)$. Noting the $\tilde{\mathbf{c}}^1 \oplus \tilde{\mathbf{c}}^2 \in C_k^0$, it is easy to show that,

$$LLR_{\tilde{\mathbf{c}}^1}(k) = \log \frac{\sum\limits_{\mathbf{c}^i \epsilon C_k^1} p(\mathbf{x}_1 \dots \mathbf{x}_L | \mathbf{c}^i \oplus \tilde{\mathbf{c}}^1 \oplus \tilde{\mathbf{c}}^2)}{\sum\limits_{\mathbf{c}^i \epsilon C_k^0} p(\mathbf{x}_1 \dots \mathbf{x}_L | \mathbf{c}^i \oplus \tilde{\mathbf{c}}^1 \oplus \tilde{\mathbf{c}}^2)} = \log \frac{\sum\limits_{\mathbf{c}^i \epsilon C_k^1} \prod\limits_{j=1}^{L} p(\mathbf{x}_j | \mathbf{I}_j^i \oplus \tilde{\mathbf{I}}_j^1 \oplus \tilde{\mathbf{I}}_j^2)}{\sum\limits_{\mathbf{c}^i \epsilon C_k^0} \prod\limits_{j=1}^{L} p(\mathbf{x}_j | \mathbf{I}_j^i \oplus \tilde{\mathbf{I}}_j^1 \oplus \tilde{\mathbf{I}}_j^2)}, \tag{14}$$

where $\tilde{\mathbf{I}}_j^1, \tilde{\mathbf{I}}_j^2, \mathbf{I}_j^i$ are the j^{th} m-blocks of the code-words $\tilde{\mathbf{c}}^1, \tilde{\mathbf{c}}^2, \mathbf{c}^i$, respectively.

If $\tilde{\mathbf{c}}^2$ is transmitted, assuming condition (7) is satisfied, there exists a $\mathbf{y} = (\mathbf{y}_1 \dots \mathbf{y}_L) \in \mathcal{O}$ such that,

$$p(\mathbf{y}_j | \tilde{\mathbf{I}}_j^2) = p(\mathbf{x}_j | \tilde{\mathbf{I}}_j^1). \tag{15}$$

Noting that the channel is memoryless, from (15), we conclude that,

$$\prod_{j=1}^{L} p(\mathbf{y}_j | \tilde{\mathbf{I}}_j^2) = \prod_{j=1}^{L} p(\mathbf{x}_j | \tilde{\mathbf{I}}_j^1), \tag{16}$$

$$p(\mathbf{y}_1 \dots \mathbf{y}_L | \tilde{\mathbf{c}}^2) = p(\mathbf{x}_1 \dots \mathbf{x}_L | \tilde{\mathbf{c}}^1). \tag{17}$$

This $(\mathbf{y}_1 \dots \mathbf{y}_L)$ results in a realization of random variable $LLR_{\tilde{\mathbf{c}}^2}(k)$ with a value of,

$$LLR_{\tilde{\mathbf{c}}^2}(k) = \log \frac{\sum\limits_{\mathbf{c}^i \epsilon C_k^1} p(\mathbf{y}_1 \dots \mathbf{y}_L | \mathbf{c}^i)}{\sum\limits_{\mathbf{c}^i \epsilon C_k^0} p(\mathbf{y}_1 \dots \mathbf{y}_L | \mathbf{c}^i)} = \log \frac{\sum\limits_{\mathbf{c}^i \epsilon C_k^1} \prod\limits_{j=1}^{L} p(\mathbf{y}_j | \mathbf{I}_j^i)}{\sum\limits_{\mathbf{c}^i \epsilon C_k^0} \prod\limits_{j=1}^{L} p(\mathbf{y}_j | \mathbf{I}_j^i)}. \tag{18}$$

Using condition (7), we conclude that (14) and (18) are equal to each other. This means for each realization of the random variable $LLR_{\tilde{\mathbf{c}}^1}(k)$, there exists a realization of the random variable $LLR_{\tilde{\mathbf{c}}^2}(k)$ with the same value and occurring with the same probability, i.e., $p(\mathbf{y}_1 \dots \mathbf{y}_L | \tilde{\mathbf{c}}^2) = p(\mathbf{x}_1 \dots \mathbf{x}_L | \tilde{\mathbf{c}}^1)$. This completes the proof that the random variables $LLR_{\tilde{\mathbf{c}}^1}(k)$ and $LLR_{\tilde{\mathbf{c}}^2}(k)$ have the same pdf. ■

Theorem 2: The pdf of $LLR(k)$ for value of bit $k = 0 \ \ or \ \ 1$ are the reflections of one another through the origin.

Proof: Consider two code-words, $\tilde{\mathbf{c}}^1, \tilde{\mathbf{c}}^2$ which have different values in their k^{th} bit position. Let us assume that $\tilde{\mathbf{c}}^1$ is transmitted through the channel and $(\mathbf{x}_1 \dots \mathbf{x}_L)$ is received. This results in a realization of random variable $LLR_{\tilde{\mathbf{c}}^1}(k)$ with a value of,

$$LLR_{\tilde{\mathbf{c}}^1}(k) = \log \frac{\sum\limits_{\mathbf{c}^i \epsilon C_k^1} p(\mathbf{x}_1 \dots \mathbf{x}_L | \mathbf{c}^i)}{\sum\limits_{\mathbf{c}^i \epsilon C_k^0} p(\mathbf{x}_1 \dots \mathbf{x}_L | \mathbf{c}^i)} = \log \frac{\sum\limits_{\mathbf{c}^i \epsilon C_k^1} \prod\limits_{j=1}^{L} p(\mathbf{x}_j | \mathbf{I}_j^i)}{\sum\limits_{\mathbf{c}^i \epsilon C_k^0} \prod\limits_{j=1}^{L} p(\mathbf{x}_j | \mathbf{I}_j^i)}, \tag{19}$$

that occurs with probability $p(\mathbf{x}_1 \dots \mathbf{x}_L | \tilde{\mathbf{c}}^1)$. Noting the $\tilde{\mathbf{c}}^1 \oplus \tilde{\mathbf{c}}^2 \in C_k^1$, it is easy to show that,

$$LLR_{\tilde{\mathbf{c}}^1}(k) = \log \frac{\sum\limits_{\mathbf{c}^i \epsilon C_k^0} \prod\limits_{j=1}^{L} p(\mathbf{x}_j | \mathbf{I}_j^i \oplus \tilde{\mathbf{I}}_j^1 \oplus \tilde{\mathbf{I}}_j^2)}{\sum\limits_{\mathbf{c}^i \epsilon C_k^1} \prod\limits_{j=1}^{L} p(\mathbf{x}_j | \mathbf{I}_j^i \oplus \tilde{\mathbf{I}}_j^1 \oplus \tilde{\mathbf{I}}_j^2)} = -\log \frac{\sum\limits_{\mathbf{c}^i \epsilon C_k^1} \prod\limits_{j=1}^{L} p(\mathbf{x}_j | \mathbf{I}_j^i \oplus \tilde{\mathbf{I}}_j^1 \oplus \tilde{\mathbf{I}}_j^2)}{\sum\limits_{\mathbf{c}^i \epsilon C_k^0} \prod\limits_{j=1}^{L} p(\mathbf{x}_j | \mathbf{I}_j^i \oplus \tilde{\mathbf{I}}_j^1 \oplus \tilde{\mathbf{I}}_j^2)}, \tag{20}$$

where $\tilde{\mathbf{I}}_j^1, \tilde{\mathbf{I}}_j^2, \mathbf{I}_j^i$ are the j^{th} m-blocks of the code-words $\tilde{\mathbf{c}}^1, \tilde{\mathbf{c}}^2, \mathbf{c}^i$, respectively.

Assuming condition (7) is satisfied and noting that the channel is memoryless, using the same approach as theorem 1, it is easy to show that if $\tilde{\mathbf{c}}^2$ is transmitted, there exists

a $\mathbf{y} = (\mathbf{y}_1 \dots \mathbf{y}_L) \in \mathcal{O}$ occurring with probability $p(\mathbf{y}_1 \dots \mathbf{y}_L|\tilde{\mathbf{c}}^2) = p(\mathbf{x}_1 \dots \mathbf{x}_L|\tilde{\mathbf{c}}^1)$, and resulting in a realization of random variable $LLR_{\tilde{\mathbf{c}}^2}(k)$ with a value of,

$$LLR_{\tilde{\mathbf{c}}^2}(k) = \log \frac{\sum\limits_{\mathbf{c}^i \epsilon C_k^1} p(\mathbf{y}_1 \dots \mathbf{y}_L|\mathbf{c}^i)}{\sum\limits_{\mathbf{c}^i \epsilon C_k^0} p(\mathbf{y}_1 \dots \mathbf{y}_L|\mathbf{c}^i)} = \log \frac{\sum\limits_{\mathbf{c}^i \epsilon C_k^1} \prod\limits_{j=1}^{L} p(\mathbf{y}_j|\mathbf{I}_j^i)}{\sum\limits_{\mathbf{c}^i \epsilon C_k^0} \prod\limits_{j=1}^{L} p(\mathbf{y}_j|\mathbf{I}_j^i)}. \tag{21}$$

Using condition (7), we conclude that (20) and (21) are only different in their signs. This means for each realization of the random variable $LLR_{\tilde{\mathbf{c}}^1}(k)$, there exists a realization of the random variable $LLR_{\tilde{\mathbf{c}}^2}(k)$ with the same magnitude and different sign which occurs with the same probability, i.e., $p(\mathbf{y}_1 \dots \mathbf{y}_L|\tilde{\mathbf{c}}^2) = p(\mathbf{x}_1 \dots \mathbf{x}_L|\tilde{\mathbf{c}}^1)$. This completes the proof that the pdf of random variables $LLR_{\tilde{\mathbf{c}}^1}(k)$ and $LLR_{\tilde{\mathbf{c}}^2}(k)$ are the reflections of one another through the origin. ■

Note that for the above two theorems, it is not necessary to partition the code-words into blocks of equal length. In other words, channels with different number of inputs can be used in subsequent block transmissions. The only condition is that the channels in different transmissions should be independent of each other.

We will now concentrate on the conditions for two bit positions to have the same pdf for their bit LLR. These conditions are presented for a memoryless channel with binary input. Note that unlike in the previous two theorems, here, we require that the channel remains the same in subsequent transmissions.

Let $\mathcal{C}$ be a binary linear code of length N. We can define a permutation $\mathcal{P}$ which permutes the elements of each code-word. The set of permutations which map the code-book $\mathcal{C}$ onto itself forms a group called Auto-morphism group of code $\mathcal{C}$.

Theorem 3: Consider two bit positions of a code-word, a, b such that $1 \leq a, b \leq N$, $a \neq b$. The channel model is assumed to be memoryless and time invariant with binary input. If there exists a permutation $\mathcal{P}$ within Auto-morphism group of code $\mathcal{C}$ which transfers bit position a to b,

$$f_{\tilde{c}_a}(y) = f_{\tilde{c}_b}((-1)^{\tilde{c}_a \oplus \tilde{c}_b} y), \tag{22}$$

where $f_{\tilde{c}_j}(y)$, $j = 1, \ldots, N$, denotes the pdf of random variable Y corresponding to $LLR_{\tilde{\mathbf{c}}}(j)$.

Proof: From theorem 1, we know that pdf of the bit LLR is independent of the transmitted code-word. For simplicity, let us consider the situation of sending the all-zero code-word bit by bit and receiving $\mathbf{x}_j$ for bit $\tilde{\mathbf{I}}_j$ in the j^{th} transmission. This results in a realization of random variable $LLR_{\tilde{\mathbf{c}}=\mathbf{0}}(a)$ with a value of,

$$LLR_{\tilde{\mathbf{c}}=\mathbf{0}}(a) = \log \frac{\sum\limits_{\mathbf{c}^i \epsilon C_a^1} \prod\limits_{j=1}^{N} p(\mathbf{x}_j|\mathbf{I}_j^i)}{\sum\limits_{\mathbf{c}^i \epsilon C_a^0} \prod\limits_{j=1}^{N} p(\mathbf{x}_j|\mathbf{I}_j^i)}. \tag{23}$$

Permutation $\mathcal{P}$ acts on each code-word $\mathbf{c}^i$ as follows,

$$\mathcal{P} : C_a^0 \longrightarrow C_b^0, \tag{24}$$

$$\mathcal{P} : C_a^1 \longrightarrow C_b^1. \tag{25}$$

In memoryless time invariant channels for each $(\mathbf{x}_1 \ldots \mathbf{x}_L)$ there exists a $(\mathbf{y}_1 \ldots \mathbf{y}_L)$ with the conditional probability $P(\mathbf{y}_1 \ldots \mathbf{y}_L|\mathcal{P}(\tilde{\mathbf{c}})) = P(\mathbf{x}_1 \ldots \mathbf{x}_L|\tilde{\mathbf{c}})$, where $\mathcal{P}(\tilde{\mathbf{c}})$ is the code-word obtained by applying permutation $\mathcal{P}$ to $\tilde{\mathbf{c}}$ and vector $\mathbf{y}$ is obtained by applying permutation $\mathcal{P}$ to elements of vector $\mathbf{x}$. Noting this fact and applying the permutation $\mathcal{P}$ to the terms of summations in (23), reveals the one to one correspondence between terms within the summations in $LLR_{\tilde{\mathbf{c}}=\mathbf{0}}(a)$ and $LLR_{\tilde{\mathbf{c}}=\mathbf{0}}(b)$ as seen in (23) and (26),

$$LLR_{\tilde{\mathbf{c}}=\mathbf{0}}(b) = \log \frac{\sum\limits_{\mathbf{c}^i \epsilon C_b^1} \prod\limits_{j=1}^{N} p(\mathbf{y}_j|\mathbf{I}_j^i)}{\sum\limits_{\mathbf{c}^i \epsilon C_b^0} \prod\limits_{j=1}^{N} p(\mathbf{y}_j|\mathbf{I}_j^i)}. \tag{26}$$

The rest of the proof follows similar to the proof of theorem 1. This means for $\tilde{c}_a = \tilde{c}_b$, we have $f_{\tilde{c}_a}(y) = f_{\tilde{c}_b}(y)$. Using theorem 2, for the case of $\tilde{c}_a \neq \tilde{c}_b$, it easily follows that $f_{\tilde{c}_a}(y) = f_{\tilde{c}_b}(-y)$, which completes the proof. ■

We apply this result to the class of Cyclic codes as a good example for checking the existence of the desired permutation. Transferring bit position a to b ($a \leq b$) in a

Cyclic code is achievable by cyclic shifting elements of the code-words $b-a$ times to the right. It is the property of Cyclic codes that any such shift results in another code-word. Hence, this permutation in Auto-morphism group of the code $\mathcal{C}$ exists for the case of Cyclic codes.

IV. Summary

In this paper the probabilistic behaviour of the bit LLR has been investigated over a general channel model with discrete input and discrete or continuous output. We proved that under certain symmetry conditions on the channel, the pdf of the bit LLR for a specific bit position is independent of the transmitted code-word, if the value of that bit position remains unchanged. It is also shown that a change in the value of a bit position makes the pdf of that bit LLR reflect through the origin. Finally, a sufficient condition for two bit positions to have the same pdf for their bit LLR is presented.

References

[1] A. Abedi, A. K. Khandani, "Some Properties of Bit Decoding Algorithms Over A Generalised Channel Model," *Proceedings of Conference on Information Sciences and Systems (CISS 2002)*, Princeton, USA, pp. 112-117, March 2002.

[2] L. R. Bahl, J. Cocke, F. Jelinek, J. Raviv, "Optimal Decoding of Linear Codes for Minimising Symbol Error Rate," *IEEE Transactions on Information Theory*, vol. 20, pp. 284-287, March 1974.

[3] J. Hagenauer, P. Hoeher, "A Viterbi Algorithm With Soft Decision Outputs and Its Applications," *Proceedings of IEEE GLOBECOM*, Dallas, USA, pp. 47.1.1-47.1.6., November 1989.

[4] V. Franz, J. B. Anderson, "Concatenated Decoding With a Reduced-Search BCJR Algorithm," *IEEE Journal on Selected Areas in Communications*, Vol.16, No.2, pp. 186-195, February 1998.

[5] L. Ping, K. L. Yeung, "Symbol-by-Symbol Decoding of the Golay Code and Iterative Decoding of Concatenated Golay Codes," *IEEE Transactions on Information Theory*, vol. 45, no. 7, pp. 2558-2562, November 1999.

[6] Y. Liu, S. Lin, M. P. C. Fossorier, "MAP Algorithms for Decoding Linear Block Codes Based on Sectionalised Trellis Diagrams," *IEEE Transactions on Communications*, vol. 48, no. 4, pp. 577-586, April 2000.

[7] S. Riedel, "Symbol-by-Symbol MAP Decoding Algorithm For High-Rate Convolutional Codes That Use Reciprocal Dual Codes," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 2, pp. 175-185, February 1998.

[8] C. R. P. Hartmann, L. D. Rudolph, “An Optimum Symbol-by-Symbol Decoding Rule for Linear Codes,” *IEEE Transactions on Information Theory*, vol. 22, no. 5, pp. 514-517, September 1976.

[9] S. Y. Chung, T. J. Richardson, R. L. Urbanke, “Analysis of Sum-Product Decoding of Low-Density-Parity-Check Codes Using Gaussian Approximation,” *IEEE Transactions on Information Theory*, Vol.47, No.2, pp. 657-670, February 2001.

[10] T. J. Richardson, M. A. Shokrollahi, R. L. Urbanke, “Design of Capacity Approaching Low-Density-Parity-Check Codes,” *IEEE Transactions on Information Theory*, Vol.47, No.2, pp. 619-637, February 2001.

[11] T. J. Richardson, R. L. Urbanke, “The Capacity of Low-Density-Parity-Check Codes Under Message Passing Decoding,” *IEEE Transactions on Information Theory*, Vol.47, No.2, pp. 599-618, February 2001.

[12] A. Abedi, P. Chaudhari, A. K. Khandani, “On Some Properties of Bit Decoding Algorithms,” *Proceedings of the Canadian Workshop on Information Theory (CWIT 2001)*, Vancouver, Canada, pp. 106-109, June 2001. (available from www.cst.uwaterloo.ca)

[13] G. D. Forney Jr., “Geometrically Uniform Codes,” *IEEE Transactions on Information Theory*, Vol.37, No.5, pp. 1241-1260, September 1991.

[14] P. Delsarte, P. Piret, “Algebraic Constructions of Shannon Codes for Regular Channels,” *IEEE Transactions on Information Theory*, Vol.28, No.4, pp. 593-599, July 1982.

[15] R. G. Gallager, *Information Theory and Reliable Communication*, New York: Wiley, 1968.

[16] G. D. Forney Jr., M. D. Trott, S. Y. Chung, “Sphere-Bound-Achieving Coset Codes and Multilevel Coset Codes,” *IEEE Transactions on Information Theory*, Vol.46, No.2, pp. 820-850, May 2000.