Synopsis of the Ph.D. Thesis

# SOME INVESTIGATIONS ON A CLASS OF RELIABILITY BASED SOFT DECISION DECODING ALGORITHMS FOR BLOCK CODES

By

**B.YAMUNA**

Department of Electronics and Communication Engineering

Amrita School of Engineering

Coimbatore 641 112, Tamil Nadu, India.

**June, 2012**

# 1. Introduction

Since Shannon's seminal work [1] the main challenge in the field of error control coding is to find (useful) codes and efficient decoding schemes with the objective of achieving low error probability. Block codes and convolution codes constitute two broad classes of coding schemes. The focus of the research work here being decoding of block codes, the same is discussed henceforth. A well established approach to decode block codes is to do Hard Decision Decoding (HDD) with the received bit sequence. As long as the number of errors in the received sequence is restricted to $\lfloor d_{\min}/2 \rfloor$ – $d_{\min}$ is the minimum Hamming distance of the code – the HDD (if successful) leads to a unique codeword directly.

The fact that HDD discards part of the information regarding the reliability of the received bit has been its bane. Two questions naturally arise here. If the number of errors exceeds $\lfloor d_{\min}/2 \rfloor$, the decoding is not unique. How best the information regarding the reliability referred to above can be used to select the 'best codeword' ? Further can the use of such reliability information lead to better results than HDD itself ? Approaches where we choose reliability information in the received bit sequence to go beyond HDD and identify codewords in a more meaningful manner comprehensively, constitute Soft Decision Decoding (SDD).

Two types of SDD algorithms – Code structure based and Reliability based – have been open problems for researchers [2]. Ideally with SDD we may aim at identifying a codeword such that the probability of decoding to an incorrect codeword is minimized; this is called Maximum Likelihood Decoding (MLD). ML decoding being computationally complex with larger block lengths, decoding methods for reducing the complexity of MLD have been suggested [3]. Techniques of reducing the decoding complexity by trading the ML performance [4-6] have also been proposed.

## 2. Motivation

Chase and Forney are the forerunners of a class of reliability based SDD algorithms that provide methods of generating a set of codewords that will contain the most likely codeword. These provide suboptimal ML performance at low SNR and reasonable block lengths [4, 5]. Marc P. C. Fossorier and Shu Lin [7] proposed an ordered statistics based most reliable independent positions (MRIPs) processing algorithm which was modified later as ordered statistics based near-optimum low complexity soft output decoding algorithm [8]. Chase algorithms have been of great interest to many researchers; their adaptations are available for binary block codes [9-11].

Correlation decoding which minimizes block error probability constitutes an optimal SDD scheme [3]. The decoding complexity makes it difficult to apply the scheme to a linear ($n$, $k$) block code when $k$ is large. A simplified correlation decoding scheme is available by which any desired block-error probability between the error probabilities of correlation and HDD can be realized by setting up a threshold value for erasure decision [6]. An ML decoding algorithm due to [12] uses algebraic decoder to generate candidate codewords and compares these candidate codewords with the received sequence using a likelihood measure. Since the decoding algorithm generates sets of different candidate codewords corresponding to the received sequence, its decoding complexity depends on the received sequence. The algorithm generates a larger set of candidates when a noisy sequence is received but a smaller set when a clean sequence is received; thus it reduces the average decoding complexity without loss of performance for MLD. An MLD algorithm due to [13] claims lower decoding complexity compared to others; the algorithm uses exact probability as a metric and selects the codeword from a short list identified. Subsequently the scheme was improved [14] by generating a minimum set of candidate code words through efficient use of the algebraic decoder.

In essence, these SDD algorithms generally aim at generation of a set of codewords with the most likely codeword being present in it with high probability; then the same is selected based on a suitable likelihood measure. The complexity and performance of the techniques are influenced by the number of candidate code words in the set.

SDD of Reed-Solomon (RS) codes – a well established family of nonbinary codes – has also been studied. The Chase (Chase-2) and GMD approaches can be extended also to nonbinary codes formed from GF ($q$). For large values of $q$ and $d_{\min}$ the complexity of decoding becomes unduly high with the Chase extension. However GMD does not entail such increase in complexity but sacrifices performance. A class of reduced-complexity algorithms combining the two – referred to as Chase-GMD algorithms – is also available [15]. Alexander Vardy and Yair Be'ery have proposed a soft-decision ML decoding algorithm for RS codes using the structure of the generator matrix [16]. A computationally efficient ML-SDD algorithm was proposed by V.Ponnampalam and B.Vucetic [17]. A class of algorithms called List decoding algorithms decode beyond the half-the-distance bound by producing a small list of codewords as the output. List decoding algorithm – originally due to Sudan [18] and refined subsequently by Guruswami and Sudan (GS) [19] – extended the decoding radius of RS codes beyond the conventional $\lfloor d_{\min}/2 \rfloor$ limit. It uses a multiplicity factor $m$, builds an interpolated polynomial passing through all points representing the received word, and leads to the identification of a set of polynomials representing a list of corresponding codewords [20]. The decoded codeword is identified from this list. As an extension of the method for SDD, the soft information available from the demodulator is used to decide the values of *m* at each point separately; the list of codewords identified from the factors of the corresponding interpolated polynomial is the basis to decide the decoded codeword here [21]. However RS codes with multilevel modulation schemes essentially remain unexplored.

If the received word $r(x)$ has a codeword within the Hamming sphere of radius $\lfloor d_{\min}/2 \rfloor$ around it, HDD decodes to the same; else HDD is a failure. The GS algorithm extends the decoding range beyond this zone for RS codes. The magnitudes representing the individual bits – $|r_i|$ – though they carry definite information regarding the reliability of the bit value – are ignored in HDD as well as GS algorithm. All reliability based SDDs cash in on this additional information to identify the most likely 'decoded codeword'. *These lead us to the following inferences which constitute the motivation for the present work:*

- The $|r_i|$ value is taken to represent the reliability of the $i^{th}$ bit and it decides the quantitative importance given to the index *i* in the whole algorithmic search.
- A limited zone around $r(x)$ is identified initially; the decoded codeword is culled out of this zone subsequently – either in one search or through a succession of such zonal reductions culminating in the decoded codeword.

- The extent of shrinkage of the zone spread around $r(x)$ determines a trade-off between computational effort called for and the confidence level attached to the identified codeword being the most likely one.

- If $r(x)$ has a codeword within the Hamming sphere of radius $\lfloor d_{\min}/2 \rfloor$ around it and all the deviations are in the least reliable $\lfloor d_{\min}/2 \rfloor$ set, the same is uniquely identified as the decoded codeword in all these SDD methods; else – that is if the codeword has deviations at bit positions outside the least reliable $\lfloor d_{\min}/2 \rfloor$ set or if a codeword does not exist within the Hamming sphere of radius $\lfloor d_{\min}/2 \rfloor$ around $r(x)$ – the results can differ.

## 3. Objective

On the whole SDD schemes have been a subject of great interest to researchers in the recent years and the problem of finding an efficient SDD scheme is still open, with the focus on *performance enhancement and reduction of decoding complexity*. Obviously these issues are directly associated with the efficient and meaningful exploitation of the soft information from the channel. Based on these the following implicit questions can be posed:

1) How best to use the soft information from the channel ?
2) Can the decoded codeword be identified directly without having to select from a set of candidate words ?
3) Can the decoded codeword so identified be the best in terms of soft decision ?
4) What would be the decoding radius of such a scheme ?

5) Is there a room for a comprehensive SDD for any block code with any multilevel modulation scheme ?

The thesis addresses the above issues and takes a fresh look at SDD and presents an alternate and relatively simpler reliability based SDD algorithm for binary and non binary block codes. The algorithm evolved uses the actual reliabilities of the received symbols and determines their reliability order. It leads to the direct identification of the most reliable codeword – termed the Target Codeword (TCW) here since it is the most reliable amongst all the possible codewords. The decoding radius has been redefined in terms of the evaluated reliabilities.

## 4. Methodology of the research work

Based on the objective as detailed above, the problem can be stated as:

Instead of specifying a zone around $r(x)$ and doing a full-fledged search within, can we identify a most likely path for the search around $r(x)$ which can lead to the decoded codeword with an obvious reduction in computational effort – again using the reliability information provided by $r_i$ ?

A closer examination of bit reliabilities and most likely erroneous bit sets does lead to such an interesting 'most likely path based' decoding algorithm. This approach is called the Reliability Level List (RLL) based approach. Use of the actual reliability value, the RLL concept for SDD, and the more direct TCW identification that it leads to, together constitute the main contributions of this thesis.

The salient features of the proposed algorithm are:

(i) The algorithm for binary codes is evolved as a two step procedure of identifying the possible error positions using 'Reliability Level List' (RLL) as the frame work followed by identification of the most likely codeword called the TCW. The first of the steps in the proposed algorithm is general enough to be applicable to any block code; the proof provided for the algorithm puts it on a firm footing and establishes its applicability to any block code. A simplified approach to the second step of TCW identification is presented by exploiting the cyclic property of block codes.

(ii) The algorithm evolved uses the actual reliability itself (and not a representative measure) to identify the TCW here. TCW is identified directly obviating the need for forming an intermediate set of candidate codewords and then selecting the decoded codeword from the set. The TCW so identified is *the best* in terms of reliability.

(iii) The algorithm has the flexibility of fixing the decoding radius as a threshold suiting to the channel noise conditions and hence reducing the complexity of computation when possible.

(iv) The algorithm evolved for binary codes is generalized subsequently. With this generalization the concept of RLL and identification of TCW are given a fresh look and extended to symbol level. This symbol level decoding of RS codes, again uses reliability as the pivot.

(v) The unique decoding radius for RS codes is established as ($d_{\min} - 1$) symbol errors from the least reliable end.

(vi) The TCW identification method with suitable modifications can be used to extract a list of the most reliable RS codewords in the lines of [21].

(vii) Though only Binary Phase-Shift Keying (BPSK) mapping scheme had been used through out, the concept of RLL based decoding is more general and applicable to codes mapped using other multilevel modulation schemes as well. The adaptability of the proposed algorithm to transmission schemes other than BPSK is presented.

Fig.1. is a schematic representation of the work carried out and its context vis-à-vis decoding of block codes.

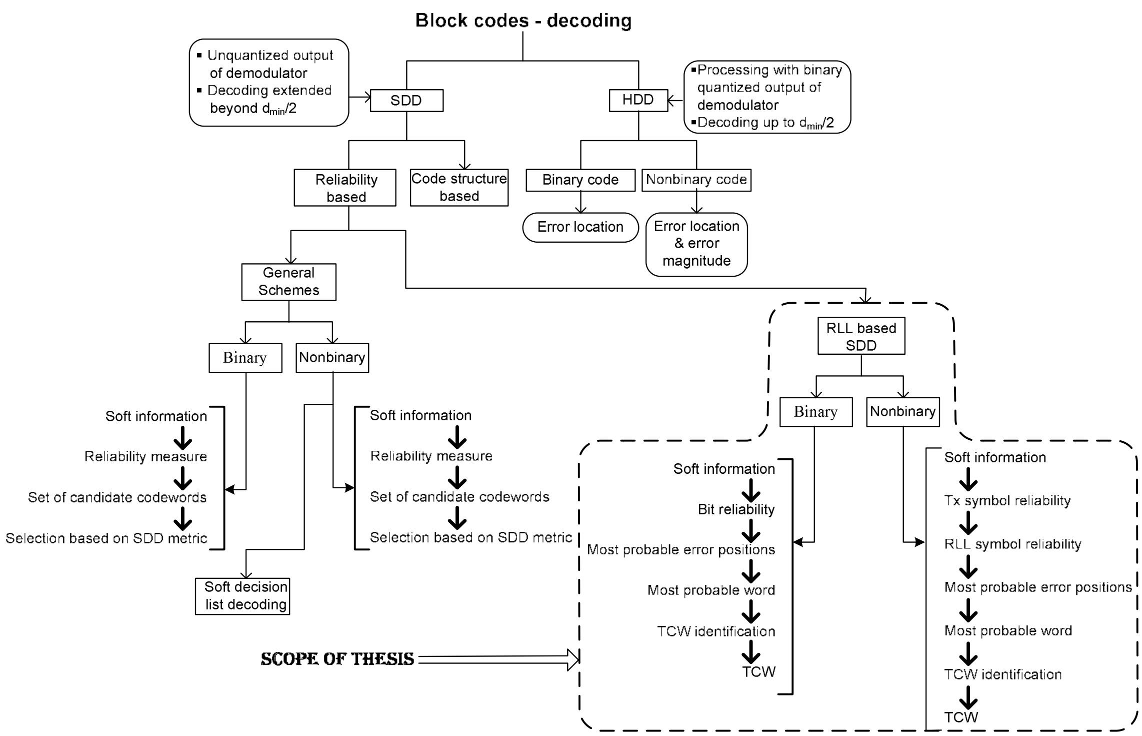


Fig.1. General overview of Block codes decoding and perspective of RLL based SDD in it.

## 5. Conclusion

In binary coded schemes the demodulator output magnitude represents the reliability of the output bit. All reliability based SDD approaches use it to refine the decoding procedure beyond what HDD can offer. Computing the actual reliability itself from this magnitude and using it for SDD can be more rewarding. With such an approach evolved here - the RLL based approach - the most likely codeword called the TCW can be identified through a shortest search starting with the received word itself. The proposed decoding scheme has been applied to different Bose, Chaudhuri, and Hocquenghem (BCH) codes to bring out its versatility.

The fact that reliability of a received bit can be directly identified as its probability was pivotal for the introduction of RLL concept and its use for SDD of binary codes. The concept has been extended to symbol reliability by combining corresponding bit reliabilities. This has directly led to the extension of RLL concept to RS codes. The RLL procedure has shown that the unique decodability with SDD extends to $d_{\min}-1$ (from the $d_{\min}/2$ limit of HDD). This is a noteworthy finding. The interesting foray beyond TCW – or the ($d_{\min}-1$) threshold – enables the identification of the most reliable list of codewords –the aim of approaches to extend the GS list decoding to SDD. The possibility of generalizing the RLL concept to block codes with any transmission scheme has been brought out.

## 6. Thesis organization

The thesis based on the above objective and methodology is organized as follows:

Introduction and problem formation are discussed in Chapter 1. In Chapter 2 an overview of cyclic codes and BCH codes is presented and a brief discussion of Chase, GMD, and OSD algorithms are taken up. The scope of RLL – central to the proposed decoding scheme – TCW identification, as applicable to binary codes, and extensive simulation establishing its effectiveness form the contents of Chapter 3.

In Chapter 4 a brief review of RS codes, their hard decoding approaches, and GS list decoding approach are presented. Extension of the proposed RLL based decoding scheme to RS codes forms the central theme of Chapter 5. A further contribution is the minimal search soft decision list decoding of RS codes using the RLL approach; the examples considered complement the same. Chapter 6 is an attempt for a comprehensive generalization of the RLL approach to block codes with multilevel transmission schemes. Chapter 7 is devoted to concluding remarks and possible directions for future work.

## 7. References


[1] C.E.Shannon (1948), 'A Mathematical Theory of Communication', *Bell Syst.Tech.Journal*, Vol 27, pp.379-423.

[2] Shu Lin, and D.J.Costello,Jr., (2004), *Error Control Coding*: *Fundamentals and Applications*, Englewood Cliffs, NJ: Prentice-Hall.

[3] Jack K. Wolf (1978), 'Efficient Maximum Likelihood Decoding of Linear Block Codes Using a Trellis', *IEEE Transactions on Information Theory*, vol. IT-24, no.1, pp. 76-80.

[4] G.D.ForneyJr., (1966), 'Generalized Minimum Distance Decoding', *IEEE Transactions on Information Theory*, vol. IT-12, pp.125-131.

[5] David Chase (1972), 'A Class of Algorithms for Decoding Block Codes with Channel Measurement Information', *IEEE Transactions on Information Theory*, vol. IT-18, pp.170-182.

[6] Hatsukazu Tanaka, and Koji Kakigahara (1983), 'Simplified Correlation Decoding by Selecting Possible Codewords Using Erasure Information', *IEEE Transactions on Information Theory*, vol. IT - 29, pp. 743-748.

[7] Marc P. C. Fossorier, and Shu Lin (1995), 'Soft-Decision Decoding of Linear Block Codes based on Ordered Statistics,' *IEEE Transactions on Information Theory*, vol. 41, pp. 1379-96.

[8] Marc P. C. Fossorier, and Shu Lin (1998), 'Soft-input Soft-output Decoding of Linear Block Codes based on Ordered Statistics', *Global Telecommunications Conference,* (*GLOBECOM*)*,*IEEE,vol.5, pp.2828-2833.

[9] Jos H. Weber, and Marc P. C. Fossorier (2004), 'Limited-Trial Chase-Like Algorithms achieving Bounded-Distance Decoding', *IEEE Transactions on Information Theory*, vol. 50, no.12, pp. 3318-3323.

[10] Jos H.Weber (2003), 'Low Complexity Chase-Like Bounded-Distance Decoding Algorithms'*Global Telecommunications Conference,* (*GLOBECOM*)*,*IEEE,vol.3, pp.1608-1612.

[11] Marc P. C. Fossorier, and Shu Lin (2000), 'Chase-Type and GMD Coset Decodings', *IEEE Transactions on Communications*, vol. 48, no.3, pp.345-350.

[12] Toshimitsu Kaneko, Toshihisa Nishijima, Hiroshige Inazumi, and Shigeichi Hirasawa (1994), 'An Efficient Maximum-Likelihood-Decoding Algorithm for Linear Block Codes with Algebraic Decoder', *IEEE Transactions on Information Theory*, vol. 40, no. 2, pp.320-327.

[13] P.G. Babalis, P.T. Trakadas and C.N. Capsalis (2002), 'A Maximum Likelihood Decoding Algorithm for Wireless Channels', *Wireless Personal Communications* vol.23, no.2, pp. 283–295.

[14] P.G. Babalis, P.T. Trakadas, T. B. Zahariadis and C.N. Capsalis (2005), 'Improved Performance of Maximum Likelihood Decoding Algorithm with

Efficient use of Algebraic Decoder', *Wireless Personal Communications*, vol.32, no.1, pp. 1–7.

[15] Heng Tang, Ye Liu, Marc P. C. Fossorier and Shu Lin (2001), 'On Combining Chase-2 and GMD Decoding Algorithms for Nonbinary Block Codes', *IEEE Communications Letters*, vol. 5, no. 5, pp.209-211.

[16] Alexander Vardy, and Yair Be'ery (1991), 'Bit-Level Soft Decision Decoding of Reed-Solomon Codes', *IEEE Transactions on Communications*, vol. 39, no. 3**,** pp. 440-444.

[17] Vishakan Ponnampalam, and Branka Vucetic (1998), 'Maximum Likelihood Decoding of Reed Solomon Codes', *Proc.Int'l Symp.on Info.Th.,*(*ISIT*), pp. 368.

[18] M.Sudan,(1997) 'Decoding of Reed-Solomon Codes beyond the Error-Correction Bound', *J.Complexity*, vol.13, no.1, pp.180-193.

[19] V.Guruswami and M.Sudan (1999), 'Improved Decoding of Reed Solomon Codes and Algebraic Geometry Codes', *IEEE Transactions on Information Theory*, vol.45, no.6, pp.1757-1767.

[20] Robert J. McEliece (2003), 'The Guruswami-Sudan Decoding Algorithm for Reed-Solomon Codes', *Interplanetary Network Progress Report* (*NASA*), pp. 42–153.

[21] Ralf Koetter, and Alexander Vardy (2003), 'Algebraic Soft Decision Decoding of Reed Solomon Codes', *IEEE Transactions on Information Theory*, vol. 49, no.11, pp. 2809-2825.

**Publications based on the research work**

1. B. Yamuna, and T.R. Padmanabhan (2012), 'A Reliability Level List based SDD Algorithm for Binary Cyclic Block Codes' *International Journal of Computers, Communications & Control* , vol.7, no. 2, pp. 388-395.
2. B. Yamuna, and T.R. Padmanabhan , 'A minimal search soft decision list decoding algorithm for Reed Solomon codes' *International Journal of Electronics and Communications*, *Elsevier* (Communicated).
3. B. Yamuna, and T.R. Padmanabhan , 'Generalized reliability based soft decision decoding algorithm for *M*-ary transmitted binary and non binary cyclic block codes', *International Journal of Satellite Communications and Networking*, (Communicated).