

An Optimal Two-Stage Decoding Algorithm for Linear Block Codes

Xianren Wu

Department of ECE
Michigan Technological University
Houghton, MI 49931

Hamid R. Sadjadpour

Department of EE
University of California, Santa Cruz
Santa Cruz, CA 95064

Abstract

A new optimal two stages decoding algorithm for linear block codes is presented. At first stage, the minimum sufficient test set \hat{S} is estimated. With the minimum sufficient test set, decoding complexity can be greatly reduced while maintaining the optimal performance. At the second stage, ordered processing is performed over the estimated minimum sufficient test set \hat{S} to find the optimal solution. Ordered processing helps to find the optimal solution quickly and in the meanwhile enables complexity-reduced sub-optimal solution with bounded block error rate. Simulation result shows that this algorithm achieves the optimal performance with low average computational complexity.

1 Introduction

During the past decades, various algorithms [2]-[11] have been proposed to address the optimal decoding problem for linear block codes. This problem has been proven to be NP-hard [1] and its complexity grows exponentially with increase in the code length. All these proposed algorithms attempt to achieve optimal or near-optimal performance with high to moderate complexity. Generally, these algorithms can be classified into three main categories. The first group [2, 3, 4] solve this problem through usage of an algebraic decoder with list decoding. The decision on the list of test codes is based on maximizing the probability of the optimal codeword included within the set of output codewords. Also its size determines decoding complexity and is heavily connected to the achievable performance. Realizing that the optimal decoding problem can be viewed as finding the shortest path in a graph, the second category of algorithms [7, 8, 9] first convert this to a graph problem and then solve it with existing graph-searching algorithms to obtain optimal or near-optimal performance.

Based on ordered statistics of the received data, the third set of algorithms [5, 6] eliminates the need of al-

gebraic decoder while achieving near optimum decoding performance. Ordered statistics decoding (OSD) was first introduced in [5] and the improved version of this algorithm presented in [6] utilizing iterative reprocessing to further decrease complexity. Since decoding complexity of ordered processing grows exponentially with the order, ordered statistics suffers from high decoding complexity when higher order processing is required to achieve acceptable performance. Besides its complexity depends on the information length and for codewords with large information length, its decoding can be very complex.

An optimal decoding algorithm was introduced in [10] with a strong optimality testing criterion and the decoding of this algorithm is dynamically updated to converge to the optimal solution. The optimality testing criterion helps to stop decoding and hence reduces the complexity whenever the optimal solution is found. However, the convergence speed can be slow and the decoding complexity increases quickly. In [11] a similar algorithm is proposed to reduce the decoding complexity further.

Similar to [10], our proposed algorithm fully utilizes the strong optimality test criterion with a new two-stage processing scheme to improve the convergence speed. The first stage of processing estimates a minimum sufficient set for optimal decoding. This minimum sufficient set is usually fairly small compared to the list required by the first group of algorithms. Then in the second stage, ordered processing is performed on the confined minimum sufficient set to result in a fast and bounded error performance decoding. Also the strong optimality test criterion helps to stop decoding whenever the optimal codeword is found.

The rest of this paper is organized as follows. The preliminary results related to the optimal decoding and basic properties of linear block codes are given in section 2. Section 3 is dedicated to detail description and analysis of the proposed two-stage processing algorithm. Simulation results are presented in section

4 and final remarks conclude the paper in section 5.

2 Preliminaries

2.1 System Model

Suppose $C(n, k, d, t)$ is the binary error correction code used in the system, where n, k, d, t denote the code length, information length, minimum Hamming distance and error correction capability of the code respectively. The encoded bits are mapping of $f : \{0, 1\} \rightarrow \{-1, +1\}$. Then these bits are modulated by antipodal signals transmitted over an additive white Gaussian noise (AWGN) channel where the noise is expressed as a Gaussian random variable with zero mean and σ^2 variance, $\mathcal{N}(t, \sigma^\epsilon)$.

Let $\vec{c} = (c_1, c_2, \dots, c_n)$ be the output codeword of the encoder, $\vec{x} = (x_1, x_2, \dots, x_n)$ the modulated vector signal, $\vec{r} = (r_1, r_2, \dots, r_n)$ the received vector signal and $\vec{n} = (n_1, n_2, \dots, n_n)$ the noise vector. Then, the modulated and the received vector signals can be described as:

$$\vec{x} = 2 \times \vec{c} - \vec{1} \quad (1)$$

and

$$\vec{r} = \vec{x} + \vec{n}. \quad (2)$$

Let $\vec{\gamma} = (\gamma_1, \gamma_2, \dots, \gamma_n)$ be the log-likelihood vector, $\vec{y} = (y_1, y_2, \dots, y_n)$ the hard-decision vector and $\vec{\beta} = (\beta_1, \beta_2, \dots, \beta_n)$ be the reliability measurement vector of the hard decision \vec{y} . The i th log-likelihood can be calculated from:

$$\begin{aligned} \gamma_i &= \log \frac{\Pr(r_i | c_i = 1)}{\Pr(r_i | c_i = 0)} \\ &= \frac{1}{2 \times \sigma^2} [(r_i + 1)^2 - (r_i - 1)^2] \\ &= L \cdot r_i, i = 1, 2, \dots, N \end{aligned} \quad (3)$$

where L is a positive constant.

$$\beta_i = |\gamma_i| \quad (4)$$

The hard-decision on the i th received data is given by:

$$y_i = \begin{cases} 1 & r_i \geq 0 \\ 0 & r_i < 0 \end{cases}$$

2.2 Maximum Likelihood Decoding Criterion

Let P be the codebook of C and the maximum likelihood decoding formula for linear block codes over AWGN channel can be formulated as:

$$\vec{c}_{opt} = \arg \min_{\forall \vec{c}^j \in P} \|2 \times \vec{c}^j - \vec{1} - \vec{r}\| \quad (5)$$

where $\|\cdot\|$ is the norm operation applied to vectors. This formula can be further simplified [10] as:

$$\vec{c}_{opt} = \arg \min_{\forall \vec{c}^j \in P} L(\vec{c}^j, \vec{r}) \quad (6)$$

$$L(\vec{c}^j, \vec{r}) = \sum_{\forall i, c_i^j \neq r_i} \beta_i \quad (7)$$

Clearly, without any specific method to decide whether a codeword is the optimal one, then the only solution is to compare all possible codewords and select the one that has the minimum Euclidean distance to the received vector \vec{r} . This exhaustive search requires extensive computational resources which is not practical for large values of n .

2.3 Basic Properties of Linear Block Codes with Algebraic Decoder

In this section, the basic properties of linear block codes to find the optimal codeword are described. The proof of Theorems and Lemmas are omitted due to space limitation and details can be found in [14]. Let $|\cdot|$ be the operation to calculate the cardinality of a set and also the absolute value of a scalar, i.e., $U = \{i | i = 1, 2, \dots, n\}, |U| = n$. For any two binary vectors of length n , define two sets $S_{diff}(\vec{a}, \vec{b}) = \{i | a_i \neq b_i, \forall i \in U\}$ and $S_{equal}(\vec{a}, \vec{b}) = \{i | a_i = b_i, \forall i \in U\}$. Clearly, $U = S_{equal}(\vec{a}, \vec{b}) + S_{diff}(\vec{a}, \vec{b})$.

Lemma 1 For any two binary codewords $\vec{C}^i, \vec{C}^j \in P, i \neq j$, and arbitrary binary vector \vec{Z} , one has $|S_{diff}(\vec{C}^i, \vec{Z})| + |S_{equal}(\vec{C}^j, \vec{Z})| \geq d$, where d is the minimum hamming distance of the code.

Lemma 2 For any codewords $\vec{C}^i, \vec{C}^j, \vec{C}^k, i \neq k, j \neq k$, arbitrary binary vector \vec{Z} , let $m_0 = |S_{diff}(\vec{C}^i, \vec{Z})|$ and $m_1 = |S_{diff}(\vec{C}^j, \vec{Z})|$, one has

$$|S_{diff}(\vec{C}^k, \vec{Z})| \geq \begin{cases} d - \lfloor \frac{m_0 + m_1}{2} \rfloor, & m_0 < 2 \cdot d - m_1 \\ 0, & m_0 \geq 2 \cdot d - m_1 \end{cases}$$

Now we assume that an algebraic decoder capable of correcting up to τ ($\tau \leq t$) exists and codeword \vec{C}^0 is the output codeword when the hard-decision vector \vec{y} acts as the input of the algebraic decoder. For simplification, we use $S_{diff}(\vec{a}) = S_{diff}(\vec{a}, \vec{y})$ and $S_{equal}(\vec{a}) = S_{equal}(\vec{a}, \vec{y})$ in the following discussion. Let $m_0 = |S_{diff}(\vec{C}^0)| < d$ and we reorder the elements in set $S_{equal}(\vec{C}^0)$ according to their reliability value as: $\beta_{S_{equal}(\vec{C}^0)_1} \leq \beta_{S_{equal}(\vec{C}^0)_2} \leq \dots \leq \beta_{S_{equal}(\vec{C}^0)_{n-m_0}}$.

An efficient criterion to decide whether a codeword is the optimal one is presented in [12] and it can be expressed by the following theorem:

Theorem 1 For any codeword \vec{C}^j , if it satisfies $L(\vec{C}^j, \vec{r}) < \sum_{i=1}^{d-\lfloor \frac{m_0+S_{diff}(\vec{C}^j)}{2} \rfloor} \beta_{S_{equal}(\vec{C}^0)_i}$, then it is the optimal codeword.

Let's arrange elements in set U based on their reliability values to form a new vector $\vec{\alpha}$ with $\beta_{\alpha_1} \leq \beta_{\alpha_2} \leq \dots \leq \beta_{\alpha_n}$. Then by looking over the first m positions in $\vec{\alpha}$ and generating all possible error patterns in these m positions and applying those error patterns to hard-decision vector \vec{y} , one can generate a test set, say E_m . Let S_m be the set of output codewords when E_m is the input to the algebraic decoder. Obviously, $E_1 \subseteq E_2 \subseteq \dots \subseteq E_n$, $S_1 \subseteq S_2 \subseteq \dots \subseteq S_n$, and if $m \geq n - \tau$, then S_m will include the optimum solution. Kaneko shows [10] that if m is chosen to be sufficiently large, S_m will include the optimal codeword and is sufficient to perform the optimal decoding. We define such kind of set to be sufficient set and m to be the order of this sufficient set. Also Kaneko [10] presents a way to calculate m from any codeword \vec{C}^k , that is:

Theorem 2 For any codeword \vec{C}^k , if $m \in U$ satisfies

$$L(\vec{C}^k, \vec{r}) < \sum_{i=1}^{d-\lfloor \frac{m_0+S_{diff}(\vec{C}^k)}{2} \rfloor - \tau - 1} \beta_{S_{equal}(\vec{C}^0)_i} + \sum_{i=1}^{\tau+1} \beta_{\alpha_{(m+i)}}, \text{ then } S_m \text{ is a sufficient set to perform optimal decoding.}$$

3 Proposed Algorithm

3.1 Stage 1: Minimum Sufficient Set & Estimation

With above discussions, we already know that if S_m is a sufficient set, then we can restrict our decoding to S_m without sacrificing any performance. Since if S_m is a sufficient set, for any set $S_n (n \geq m)$ it is also a sufficient set. Obviously, there exists a smallest m that makes set S_m a sufficient set and we define this set to be the minimum sufficient set and it is denoted by S_{min} .

Theorem 3 The minimum sufficient set S_{min} is the set S_m , where one error happens at position α_m and there are exactly τ errors out of m least reliable positions.

Following from the properties of ordered statistics [5, 13], the probability for S_M to be the minimum sufficient set will be decreased quickly as M increases. In general, the average number for M is relatively a small number [14]. With the restriction of decoding into S_M , one can greatly reduce the decoding complexity.

However, without evaluating the whole codewords, one can not tell the exact value of M . But *Theorem 2* gives us an efficient way to estimate a sufficient set from a codeword. The closer is the codeword to the optimal one, the closer the estimation. We combine the power of algebraic decoder and ordered statistics to get a better estimate of the minimum sufficient set. Actually, Chase-III algorithm [3] and 1-OSD algorithm [5] are combined together to get a codeword near the optimal one and thus give a better estimate. This codeword is obtained by examining all codewords produced by these two algorithms and choosing the one that has the minimum Euclidean distance to the received vector \vec{r} . With the codeword in hand, then *Theorem 2* can be used to give an estimate of order of the minimum sufficient set. These two algorithms both have relative low computational complexity and there will not be much overhead in the whole decoding complexity.

3.2 Stage 2: Ordered Processing & Performance Analysis

After the first stage of processing, one already has an estimated minimum sufficient set \hat{S} , order \hat{M} and the corresponding test set \hat{E} . Also we know that the test set \hat{E} is generated by considering all possible error patterns in the \hat{M} least reliable positions. Similiar to the order- i processing in [5], we define the order- i processing as all possible error patterns with up to i errors. Specifically, Order- i processing applies those error patterns to get a subset \hat{E}_i of \hat{E} and an algebraic decoder is used to decode all test codes in \hat{E}_i . Among codewords produced by \hat{E}_i , the one that has the minimum Euclidean distance to the received vector \vec{r} is chosen as the output. Also in the Ordered processing, whenever the Euclidean distance between the estimated codeword and the received vector is computed, *Theorem 1* is used to stop the search if the optimal codeword is found.

Theorem 4 By examining test code in \hat{E} that are generated by error patterns of error number less or equal to i , Order- i processing can correct up to $(i + \tau)$ errors. In particular, Order- $(d - 1 - \tau)$ processing can correct up to $(d - 1)$ errors and achieve the performance of Chase-I [3] algorithm.

Using the union bound, the block error rate after Order- i processing can be bounded as:

$$P_{e,block}(i) \leq 1 - \sum_{m=0}^{\tau+i} \binom{n}{m} P_b^m \times (1 - P_b)^{(n-m)} \quad (8)$$

where P_b is the raw bit error rate. Under practical situation, the processing order i could be determined based on the desired block error performance and thus greatly reduces the decoding complexity with slight performance degradation. It enables a flexible design with the trade-off between decoding complexity and performance requirement.

4 Simulation Results

Figure 1 depicts the average complexity requirements of our proposed two-stage maximum likelihood (TS ML) decoding algorithm, Chase-II algorithm and Kaneko's algorithm for a BCH(31,16) code. In this figure, decoding complexity of Chase-II algorithm is normalized to 1 and decoding complexity of our proposed algorithm is drawn based on the normalized coordinates. For Chase-II algorithm, it has fixed complexity requirement irrespective of SNR value. Decoding complexity of our proposed algorithm continuously decreases with increase in SNR and its decoding complexity is well below Chase-II algorithm and Kaneko's algorithm at all simulated SNR regions.

Figure 2 demonstrates error performance of our Order-2 TS ML algorithm, Chase-II algorithm and 2-OSD algorithm for a BCH(31,16) code. Our algorithm achieves performance close to 2-OSD and Kaneko at all practical BER region. In all simulated SNR regions, our algorithm performs over Chase-II algorithm with much lower complexity.

5 Conclusion

In this paper, we present a new optimal decoding algorithm for linear block codes. The decoding is divided into two stages with distinct objectives. The first stage is aimed at minimizing the decoding complexity and the second stage is targeted to approach the optimal performance. Also the bounded sub-optimal performance with complexity reduction can be achieved in the second stage. Through the two-stage division, this algorithm can achieve optimal performance with low average complexity. Further investigation on this algorithm could be made on the development of efficient estimation algorithm for the minimum sufficient set and stronger criterion associated with the maximum likelihood decoding.

References

[1] S.G. Wilson, "Digital Modulation and Coding," NJ:Prentice-Hall, 1996

- [2] G.D. Forney, "Generalized minimum distance decoding," *IEEE Transactions on Information Theory*, vol.12, no.2, pp.125-131, April 1966.
- [3] D. Chase, "A class of algorithms for decoding block codes with channel measurement information," *IEEE Transactions on Information Theory*, vol.18, no.1, pp.170-182, January 1972.
- [4] H. Tanaka and K. Kakigahara, "Simplified correlation decoding by selecting codewords using erasure information," *IEEE Transactions on Information Theory*, vol.29, no.5, pp.743-748, September 1983.
- [5] M.P.C. Fossorier and S. Lin, "Soft-Decision decoding of linear block codes based on ordered statistics," *IEEE Transactions on Information Theory*, vol.41, no.5, pp.1379-1396, September 1995.
- [6] M.P.C. Fossorier, "Reliability-based soft-decision decoding with iterative information set reduction," *IEEE Transactions on Information Theory*, vol.48, no.12, pp.3101-3106, December 2002.
- [7] Y.S. Han, C.R.P. Hartmann and C.C. Chen, "Efficient priority-first search maximum-likelihood soft-decision decoding of linear block codes," *IEEE Transactions on Information Theory*, vol.39, no.5, pp.1514-1523, September 1993.
- [8] Y.S. Han, C.R.P. Hartmann and K.G. Mehrotra, "Decoding linear block codes using a priority-first search: performance analysis and suboptimal version," *IEEE Transactions on Information Theory*, vol.44, no.3, pp.1233-1246, May 1998.
- [9] M. Kokkonen and K. Kalliojärvi, "Soft-decision decoding of binary linear block codes using reduced breadth-first search algorithm," *IEEE Transactions on Information Theory*, vol.48, no.6, pp.905-907, June 2000.
- [10] T. Kaneko, T. Nishijima, H. Inazume and S. Hirasawa, "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, March 1994.
- [11] T. Kaneko, T. Nishijima and S. Hirasawa, "An improvement of soft-decision maximum-likelihood decoding algorithm using hard-decision bounded-distance decoding," *IEEE Transactions on Information Theory*, vol.43, no.4, pp.1314-1319, July 1997.

- [12] D.J. Taipale and M.B. Pursley, "An improvement to generalized-minimum distance decoding," *IEEE Transactions on Information Theory*, vol.37, no.1, pp.167-172, January 1991.
- [13] M.P.C. Fossorier and S. Lin, "First-order approximation of the ordered binary-symmetric channel," *IEEE Transactions on Information Theory*, vol.42, no.5, pp.1381-1387, September 1996.
- [14] X. Wu, H.R. Sadjadpour and Z. Tian, "A New Adaptive Two-Stage Maximum-Likelihood Decoding Algorithm for Linear Block Codes Suitable for Block Turbo Codes," submitted to *IEEE Transactions on Communications*, 2003.

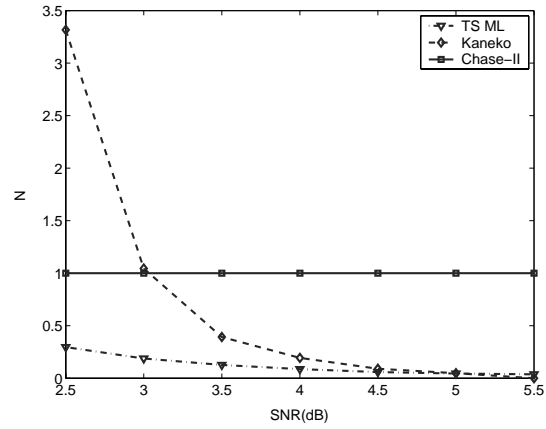


Figure 1: Complexity Comparison: Average number of decoded codewords

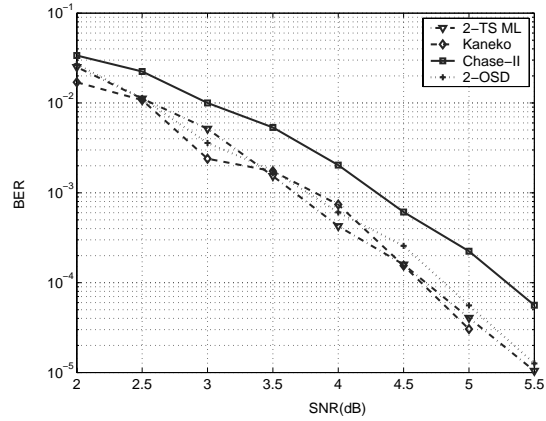


Figure 2: Performance Comparison for BCH(31,16)