Available online at www.ijournalse.org

Emerging Science Journal

Vol. 4, No. 5, October, 2020

An Efficient Decoding Algorithm for Block Codes Based on the Communication Channel Reliability Information

Yong-Geol Shim [a*]

[a] *Departement of Electronics and Electrical Eng., Dankook University, Gyeonggi, 16890, Korea*

Abstract

For channel codes in communication systems, an efficient algorithm that controls error is proposed. It is an algorithm for soft decision decoding of block codes. The sufficient conditions to obtain the optimum decoding are deduced so that the efficient method which explores candidate code words can be presented. The information vector of signal space codes has isomorphic coherence. The path metric in the coded demodulator is the selected components of scaled regions. The carrier decision is derived by the normalized metric of synchronized space. An efficient algorithm is proposed based on the method. The algorithm finds out a group of candidate code words, in which the most likely one is chosen as a decoding result. The algorithm reduces the complexity, which is the number of candidate code words. It also increases the probability that the correct code word is included in the candidate code words. It is shown that both the error probability and the complexity are reduced. The positions of the first hard-decision decoded errors and the positions of the unreliable bits are carefully examined. From this examination, the candidate codewords are efficiently searched for. The aim of this paper is to reduce the required number of hard-decision decoding and to lower the block error probability.

Keywords:

Soft Decision Decoding;

Communication Engineering;

Electronics;

Channel Codes.

Article History:

Received:	01	July	2020
Accepted:	27	September	2020
Published:	01	October	2020

1- Introduction

Modern communication systems are composed of multitudinous digital circuits. They transmit and receive digital data. The transmitted digital data suffer from noise which exists in communication channel. The noise causes errors at receivers. The receivers control errors with channel codes.

Decoding linear block codes by using channel measurement information (soft-decision) has received considerable attention [1, 2]. In channel coding systems, some binary block codes have arithmetical structures, with which the hard decision decoding procedure can be performed easily [3]. But in the soft decision decoding procedure, the arithmetic structures can't be fully helpful. There are some algorithms that use the channel reliability information [4].

There are two kinds of algorithms that provide the conceptual basis for soft-decision decoding. One is to select the code word which minimizes the distance from the received sequence in order to minimize the block error probability [5, 6]. The other is to decode each symbol in a code word in order to minimize the symbol error probability [7]. In the algorithms minimizing the average symbol error probability, the decoded sequence may not even be a code word. In this paper, we shall investigate the former approach. The conventional algorithms have excellence in either error probability or decoding complexity [1, 4-10]. Zhang et al. (2017) [11] proposed a feedback method combined with the low-density parity-check codes for building the wiretap channel. An algorithm for cyclic codes based on extended parity-check equations was proposed in Babalola and Versfeld (2018), which operates on transforming the systematic parity-check matrix using the soft reliability information matrix obtained from the received vector [12]. Wijekoon et al. (2019), an iterative approach for soft-decision decoding of Reed-Solomon codes employs symbol-level belief

[*] **CONTACT**: Ygshim@dankook.ac.kr

DOI: http://dx.doi.org/10.28991/esj-2020-01235

propagation on an alternative parity-check matrix representation of the code [13]. Choi and Jeong (2019) proposed an ordered statistics-based decoding [14]. A generalized parity-check matrix transformation algorithm for binary cyclic codes is developed in Babalola et al. (2020) [15]. Lin et al. (2020) presented a scheme for encoding and iterative soft-decision decoding of cyclic codes of prime lengths [16].

With the conventional algorithms, however, if you improve one, the other is deteriorated. The research purpose of this paper is solving the dilemma. With the proposed algorithms, both error probability and decoding complexity can be improved. In this paper, the sufficient conditions to obtain the optimum decoding are deduced so that the efficient method which explores candidate code words can be presented. An efficient algorithm is proposed based on the method. The proposed algorithm aims to achieve two targets. The first target is that the transmitted code word should be included in the set of explored candidate words. The second target is that the complexity of the algorithm should be reduced. The number of candidate code words should be reduced, too.

The positions of the first hard-decision decoded errors and the positions of the unreliable bits are carefully examined. From this examination, the candidate codewords are efficiently search for. The aim of this paper is to reduce the required number of hard-decision decoding and to lower the block error probability.

2- Soft Decision Decoding

A binary antipodal signal associated with code word is transmitted. An error control system uses linear code which has minimum distance d [9]. From the communication channel, two vectors are received. The hard decision and the reliability information are received vectors. The receiver decoder determines the code word which has been transmitted.

Let C be an (n , k) code. The rate of the code is $R=k/n$. A code word of C is denoted by $\mathbf{c}=(c_1,c_2,\cdots,c_n)$, where $c_i \in GF(2)$. The code symbol c_i is transformed into an antipodal signal $s_i=\sqrt{E_s}(1-2c_i)$, where E_s is the energy per symbol entering the channel. The signal vector $\mathbf{s}=(s_1,s_2,\cdots,s_n)$ is transmitted over a memoryless channel, which adds noise and produces the output $\mathbf{r}=(r_1,r_2,\cdots,r_n)$. The symbol r_i is given by $r_i=s_i+z_i$, where z_i represents noise. The noise has zero mean and $N_o/2$ variance.

The channel output $\mathbf{r}$ produces two vectors $\mathbf{y}=(y_1,y_2,\cdots,y_n)$ and $\mathbf{a}=(a_1,a_2,\cdots,a_n)$. The vector $\mathbf{y}$ is the hard-decision, where y_i is 0 if $r_i \geq 0$ and y_i is 1 otherwise. The vector $\mathbf{a}$ is the confidence value vector. For the antipodal signal through the additive white Gaussian noise channel, a_i is equivalent to r_i .

The decoder uses $\mathbf{y}$ and $\mathbf{a}$ to determine which code word has been transmitted. A decoding rule is a strategy for determining an estimate of the transmitted information. The decoder selects the estimated code word $\mathbf{c}$ which minimizes the distance from the received vector $\mathbf{r}$. The error pattern for the estimated code word $\mathbf{c}$ is given by $\mathbf{e}=\mathbf{y}\oplus\mathbf{c}$, where $\oplus$ between two binary symbols is modulo-2 addition. $W_a(\mathbf{e})$ is the analog weight defined as:

$$W_a(\mathbf{e})=\sum_i a_i e_i \tag{1}$$

The maximum likelihood decoder is equivalent to the decoder which selects the estimated code word $\mathbf{c}$ minimizing $W_a(\mathbf{e})=W_a(\mathbf{y}\oplus\mathbf{c})$. To determine $\mathbf{c}$, we should search for a few candidate codewords.

2-1- Sufficient Condition

Let the first candidate code word be $\mathbf{c}_1=(c_{11},c_{12},\cdots,c_{1n})$, which is obtained by hard-decision decoding of $\mathbf{y}$. However, uncorrectable but detectable errors may occur, for some codes which is not perfect. If uncorrectable errors are detected, the least confident bit of $\mathbf{y}$ is complemented (i.e., if a_i is the smallest, complement y_i) and a hard-decision decoding is performed again to obtain $\mathbf{c}_1$. But, if uncorrectable errors are detected again, we finish the entire decoding procedure reporting the detection of errors. The path metric represents the quantized components in the demodulator [6]. The optimum decision is based on normalized metric of the synchronized space [8]. The scaled regions are designed to achieve the uniform phase [7, 8]. The symmetry properties of signal space codes are isomorphic to the signal set in the demodulator [9]. The carrier decision is derived by the normalized metric of synchronized space [4, 6]. The adjacent measure has constant weight with the symbol code which gives zeros in the synchronized space. The maximum likelihood unrestricted decision of redundant bits determines the decision threshold [4].

The code point that is nearest to the decoding result generates the candidate code words [10]. The subsets of the prefix length matching parameters provide optimum gain. The coding gain is obtained by symmetric search. The carrier phase should be considered. When the PLL synchronizer is used, the symbol parameters are efficiently estimated. If we can obtain $\mathbf{c}_1$, the error pattern for $\mathbf{c}_1$ is given by $\mathbf{e}_1=\mathbf{y}\oplus\mathbf{c}_1=(e_{11},e_{12},\cdots,e_{1n})$.

If $\mathbf{e}_1=\mathbf{0}$ (the zero vector), $W_a(\mathbf{e}_1)=0$ and it is the minimum analog weight. Therefore, $\mathbf{c}_1$ is the maximum likelihood decoding result. In this case, we set $\mathbf{c}=\mathbf{c}_1$ and finish the entire decoding procedure.

If $\mathbf{e}_1 \neq \mathbf{0}$, we search for the other candidate code words. Let $\mathbf{c}_m = (c_{m1}, c_{m2}, \cdots, c_{mn})$ be a candidate code word. Since C is a linear code, we can denote $\mathbf{c}_m$ as $\mathbf{c}_1 \oplus \mathbf{u}_m$, where $\mathbf{u}_m = (u_{m1}, u_{m2}, \cdots, u_{mn})$ is another code word. Of course, $\mathbf{c}_m \neq \mathbf{c}_1$, and $\mathbf{u}_m \neq \mathbf{0}$. The error pattern for $\mathbf{c}_m$ is given by $\mathbf{e}_m = \mathbf{y} \oplus \mathbf{c}_m = \mathbf{y} \oplus \mathbf{c}_1 \oplus \mathbf{u}_m = \mathbf{e}_1 \oplus \mathbf{u}_m$. Thus, we should find the code word $\mathbf{u}_m$, which minimizes:

$$W_a(\mathbf{e}_m) = W_a(\mathbf{e}_1 \oplus \mathbf{u}_m) = \sum_i a_i (e_{1i} \oplus u_{mi}) \tag{2}$$

In order to minimize (2), the vector, $\mathbf{b}$ has at least $[d - W_H(\mathbf{e})]$ 1's for positions i where $e_i = 0$. So we set $b_i = 1$, for least reliable $[d - W_H(\mathbf{e})]$ positions i where $e_i = 0$. The position i has small value of r_i. For the code word $\mathbf{b}$, $\mathbf{e} \oplus \mathbf{b}$ has the minimum analog weight among all error patterns except $\mathbf{e}$. Therefore, the sufficient condition of optimality is that $W_a(\mathbf{e}) \leq W_a(\mathbf{e} \oplus \mathbf{b})$.

2-2- Locating the Error Positions

Starting from a code word $\mathbf{c}$ and its error pattern $\mathbf{e}$, we explore other candidate code words. Let $\mathbf{b}^w = (b_1^w, b_2^w, \cdots, b_n^w)$ be a vector whose Hamming weight is integer w. We set $b_i^w = 1$, for all positions i where $e_i = 1$ and least reliable $[w - W_H(\mathbf{e})]$ positions i where $e_i = 0$.

The vector $\mathbf{b}^w$ may not be a code word. We hard decision decode $\mathbf{b}^w$ to obtain a code word $\mathbf{c}^w$. We obtain a candidate code word $\mathbf{c} \oplus \mathbf{c}^w$ and its error pattern $\mathbf{e} \oplus \mathbf{c}^w$. When $w < (d-1)/2$, $\mathbf{c}^w$ becomes $\mathbf{0}$. Thus, there is no need to do for $w < (d-1)/2$. The set of the representation of integers by specific binary forms can be associated with $W_a(\mathbf{e} \oplus \mathbf{b})$. One can properly select scaled transformation to be applied to these lattices in order to produce the required number of representatives in which $W_a(\mathbf{e} \oplus \mathbf{b})$ will be partitioned. Let (x, y) be a prime solution to $A(x, y) = q$ for any integer q. Let $A(x, y)$ be defined as the sum of two squares, that is, $A(x, y) = x^2 + y^2$. The solution is connected to the problem of realizing the partitioning of a lattice into sublattices. This interest is basically due to the richness of the algebraic structure available and the possibilities to explore new ways of constructing complex lattices as well as of partitioning them. However, we also need a method for constructing irreducible decomposable forms in order not to be too restrictive.

In this direction, let Ω be any algebraic number field of degree n, and let θ be a primitive element for Ω over Q, such that $\Omega = Q(\theta)$. The minimum monic polynomial $p(x)$ of the number θ over the field Q has degree n. An extension L over Ω can be constructed for $p(x)$ factoring completely,

$$p(x) = (x - \theta_1) \cdot (x - \theta_2) \cdot \cdots \cdot (x - \theta_n), \quad \theta_1 = \theta. \tag{3}$$

The coefficients of the field are rational numbers such that the norm $N(\alpha)$ satisfies

$$N(\alpha) = \alpha_1 \cdot \alpha_2 \cdot \cdots \cdot \alpha_n \quad .$$
(4)

Let $x_1, x_2, \cdots, x_m$ be elements of Q, then the norm of the number $x_1\mu_1 + x_2\mu_2 + \cdots + x_m\mu_m$ with respect to the extension Ω / Q is

$$N(x_1\mu_1 + x_2\mu_2 + \cdots + x_m\mu_m) = A(x_1, x_2, \cdots, x_m). \tag{5}$$

Some caution should be taken regarding this equality for not always it is possible to have an irreducible form. However, if $\mu_2, \mu_3, \cdots, \mu_m$ generate the field $\Omega = Q(\mu_2, \mu_3, \cdots, \mu_m)$, then the form

$$A(x_1, x_2, \cdots, x_m) = N(x_1 + x_2\mu_2 + \cdots + x_m\mu_m) \tag{6}$$

Is irreducible over Q. The integral solutions to $A(x_1, x_2, \cdots, x_m) = N(x_1 + x_2\mu_2 + \cdots + x_m\mu_m) = q$ reduces to the determination of all numbers ξ in Ω such that $\xi = x_1 + x_2\mu_2 + \cdots + x_m\mu_m$ with x_i rational integers and $N(\xi) = q$.

Let $\{\mu_1, \mu_2, \cdots, \mu_m\}$ be an arbitrary finite set of elements of an algebraic number field. Let M be a module in Ω. Then, $\mu_1, \mu_2, \cdots, \mu_m$ are generators for the module M. Now, if Ω is an algebraic number field of degree m and M is a module in Ω with m linearly independent elements, then M is a full module.

If the set of generators $\{1, \mu_2, \mu_3, \cdots, \mu_m\}$ is a full module of Ω, then $\Omega = Q(\mu_2, \mu_3, \cdots, \mu_m)$ and it follows from (6) that any full form is irreducible. Let the numbers $\mu_1, \mu_2, \cdots, \mu_m$ be the generators of the module M. Hence, they form a basis for M.

Let the set D_M be the coefficients ring of the module M. Since the element l is in D_M, D_M is a ring with unit. The ring of integers of the field Ω is a full module in the field of algebraic number which contains the number l and is a ring. Consequently, the ring of the algebraic number field Q is the ring of integers of the field. Recalling the problem of integral representation by decomposable forms, we see that it reduces to the determination in a full module of all numbers μ for which $N(\mu) = q$. Now, for any element ν of D such that $N(\nu) = l$, the product $\nu \cdot \mu$ is in M. Thus, the coefficients provide new solutions of $N(\mu) = q$ from one solution.

The coefficients belong to the set of elements which are the ring D. If α is an element of Ω, the units of D satisfy the sufficient condition. Consequently, if α is an element of Ω, the polynomial has integer coefficients. Since there are various orders of a number field Ω, there is a maximal order containing the previous ones because there are various orders of a number field Ω.

There is a geometric representation of the algebraic numbers as points in n-dimensional space. Let Ω be a number field. The set { $\mu_1,\mu_2,\cdots,\mu_n$ } is the basis of the full module. The numbers of M are represented by the linear combinations of the n linearly independent $x(\mu_1),x(\mu_2),\cdots,x(\mu_n)$ with:

$$x(\alpha)=(\sigma_1(\alpha),\sigma_2(\alpha),\cdots,\sigma_s(\alpha),\sigma_{s+1}(\alpha),\cdots cr2(a),\cdots,\sigma_{s+t}(\alpha)) \tag{7}$$

Being a point of the space $L^{s,t}$. The binary quadratic forms $A(x,y)=ax^2+bxy+cy^2$, with $a=c=l$ and $b=0$; and $a=b=c=1$, are irreducible rational forms. Which decomposes into linear factors in some quadratic field (extension of the rational field of degree 2). Therefore, the full modules in quadratic fields is the connection with the problem of representation of integers by the binary quadratic forms. Being more specific, let Ω be a field, $p(x)$ be a polynomial in $\Omega[x]$ of degree 2. Let $f(x)$ and $g(x)$ be polynomials in $\Omega[x]$. Let us represent the collection of all congruence classes be defined by addition and multiplication of representatives. A typical element of $\Omega[x]/p(x)$ is:

$$[a_0+a_1x+\cdots+a_nx^n]=[a_0]+[a_1][x]+\cdots+[a_n][x]^n \tag{8}$$

Since a_i and $[a_i]$ are congruent, (8) becomes $a_0+a_1[x]+\cdots+a_n[x]^n$. If the polynomial is represented by α, then $a_0+a_1\alpha+\cdots+a_n\alpha^n$ is a polynomial of $\Omega[x]/p(x)$ with coefficients in Ω. Consequently, $\Omega[x]/p(x)$ is a simple extension field of Ω and it is isomorphic to $\Omega[\alpha]$.

For instance, take an integer $\alpha=\sqrt{d}$ ($d\neq 1$). Clearly, $\sqrt{d}$ is a root of $x^2-d=0$, and so it is an algebraic number. By the division algorithm, there is some $g(x)$ in $Q[x]$ and some remainder $r(x)=a+bx$ in $Q[x]$ such that for any polynomial $f(x)$ in $Q[x]$. We have that:

$$f(x)=(x^2-d)\cdot g(x)+r(x)=(x^2-d)\cdot g(x)+(a+bx) \tag{9}$$

Evaluating (9) at $x=\sqrt{d}$, it follows that $f(\sqrt{d})=a+b\sqrt{d}$. Thus, $Q[\sqrt{d}]$ is a ring where each element has the form $(a+b\sqrt{d})$. The nonzero elements of $Q[\sqrt{d}]$ have an inverse and $Q[\sqrt{d}]$ is a field. Since any number of the field $Q[\sqrt{d}]$ has the form $\alpha=a+b\sqrt{d}$, the characteristic polynomial of α is $x^2-2ax+a^2-db^2$. Then α lies in the maximal order of the field $Q[\sqrt{d}]$ if and only if $Tr(\alpha)=2a$ and $N(\alpha)=a^2-db^2$ are integers where $Tr(\cdot)$ is the trace. The most general quadratic integer has the form $(a+b\omega_0)$. If d is 1 mod 4, ω_0 is $(1+b\sqrt{d})/2$. If d is not 1 mod 4, ω_0 is $\sqrt{d}$. The module has as basis {l, ω_0 } and all numbers in the module have the form $(a+b\omega_0)$. Note that the module is an integral domain. The units of the maximal order are determined by $N(a+b\omega_0)=\pm 1$. For $d=1$ mod 4, this norm is given by $a^2+ab^2=\pm 1$. For $d\neq 1$ mod 4, the norm is given by $a^2+ab+((1-d)/4)b^2=\pm 1$.

For imaginary quadratic fields, d is less than 0, we have the following cases.

i) For $d=-1$, the solutions are $a=\pm 1$, $b=0$ and $a=0$, $b=\pm 1$, and so the units are ± 1 and $\pm i$.

ii) For $d=-3$, the solutions are $a=\pm 1$, $b=0$; $a=0$, $b=-1$; $a=1$, $b=-1$; $a=-1$, $b=1$, and so the units are ± 1 and $\pm(1/2)\pm i(\sqrt{3}/2)$.

iii) For all remaining values of negative d, the solutions are $a=\pm 1$, $b=0$, and so the units are ± 1.

If δ is an irrational number of $Q[\sqrt{d}]$ with $p(x)=a_1x^2+a_2x+a_3$ then the coefficient ring of the module {l, δ } is the order {l, $a_l\delta$ } with discriminant $a_2^2-4a_1a_3$. Note that for each basis { δ_1, δ_2 } of the full module M, there is a binary quadratic form $N(x\delta_1+y\delta_2)$. However, a module M with basis { δ_1, δ_2 } leads to:

$$A(x,y)=ax^2+bxy+cy^2=N(x\delta_1+y\delta_2)/N(M). \tag{10}$$

If some classes of modules have coefficient ring, the corresponding forms also have the same discriminant. The representation of integers by binary quadratic forms reduces to the problem of similarity of modules in quadratic fields. If $A(x,y)=q$ where $A(x,y)$ is a primitive form, then $A(x,y)=N(x\delta_1+y\delta_2)/N(M)$ with a basis { δ_1, δ_2 } for M. The mapping corresponds the solution and the number ξ with norm $N(\xi)=q\cdot N(M)$.

The information vector $\mathbf{y}$ is a binary quantization of $\mathbf{r}$. The Hamming distance between vector $\mathbf{x}$ and vector $\mathbf{y}$ is denoted by $d_H(\mathbf{x},\mathbf{y})$. The metric $d_E(S(\mathbf{x}_m),\mathbf{r})$ is the extended Euclidean distance between $S(\mathbf{x}_m)$ and $\mathbf{r}$. A test code pattern $\mathbf{T}$ is a binary vector of length n. The distance profile S_T is a set of test signals [7]. For each $\mathbf{T}\in S_T$, decode $\mathbf{y}\oplus\mathbf{T}$ by the t hard decision binary decoder and construct the determinant set D containing the code words $\mathbf{x}$ such that for $\mathbf{T}\in S_T$, $d_H(\mathbf{x},\mathbf{y}\oplus\mathbf{T})\leq t$. If D is empty set, then the decoding procedure fails to decode.

3- Decoding Algorithm

The information vector of signal space codes has isomorphic coherence. The path metric in the coded demodulator is the selected components of scaled regions. The optimum decision is based on normalized metric of synchronized space. The scaled regions are designed to achieve the uniform phase.

The positions of the first hard-decision decoded errors and the positions of the unreliable bits are carefully examined. From this examination, the candidate codewords are efficiently search for. The aim of the algorithm is to reduce the required number of hard-decision decoding and to lower the block error probability.

(Step 1) Decode $\mathbf{y}$ to obtain $\mathbf{c}$ with hard decision information.

(Step 2) If the sufficient condition of optimum decoding for $\mathbf{c}$ is satisfied, then $\mathbf{c}$ is the code word. Terminate decoding.

(Step 3) For each w, $\lfloor (d-1)/2 \rfloor \le w \le n$, execute sub steps.

(Sub step 3-1) Explore code word $\mathbf{c} \oplus \mathbf{c}^w$.

(Sub step 3-2) If the sufficient condition of optimum decoding for $\mathbf{c} \oplus \mathbf{c}^w$ is satisfied, then get $\mathbf{c} \oplus \mathbf{c}^w$ is the code word. Terminate decoding.

(Step 4) Among all the explored code words, the code word with error pattern of smallest analog weight is decoding result. Terminate decoding.

Figure 1 illustrates the flowchart. The optimum decision is designed to achieve the uniform phase.

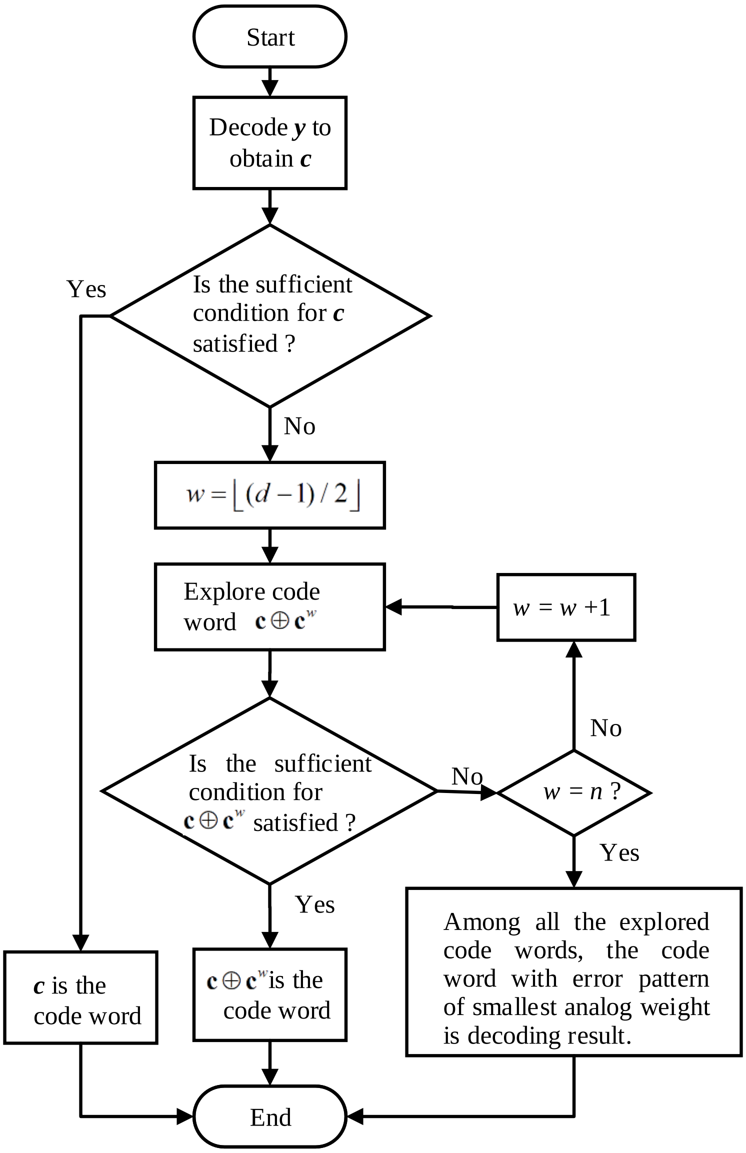
Start
Decode *y* to obtain *c*
Is the sufficient condition for *c* satisfied ?
Yes
No
$w = \lfloor (d-1)/2 \rfloor$
Explore code word $\mathbf{c} \oplus \mathbf{c}^w$
$w = w + 1$
No
Is the sufficient condition for $\mathbf{c} \oplus \mathbf{c}^w$ satisfied ?
No
$w = n$?
Yes
Yes
c is the code word
$\mathbf{c} \oplus \mathbf{c}^w$ is the code word
Among all the explored code words, the code word with error pattern of smallest analog weight is decoding result.
End

Figure 1. The flowchart of the algorithm.

4- Simulation Results

The algorithm is applied to some widely used block codes. The algorithm is compared with separate path equalization (SPA) algorithm [7]. Figures 2 and 3 show the decoding error probability. The signal-to-noise ratio is expressed as E_b / N_o. E_b and N_o are the energy per information bit and the single-sided noise spectral density, respectively [6]. Compared to the SPA algorithm, the proposed algorithm can increase the probability that the correct code word is included in the candidate words. The adaptive permutation of the proposed algorithm works efficiently. The proposed algorithm can reduce the decoding error probability. The proposed algorithm involves obtaining the most and least reliable bits by sorting the reliability vectors in ascending order. The normalized metric transformation stage of the algorithm takes a large component of the decoding complexity. The smallest analog weight requires more iterative steps, while the decoding procedure quickly arrives at the negative element stopping condition before the algorithm properly decodes the received vector. However, it is clear that the candidate error pattern is computationally efficient, since it yields a similar decoding performance with the smallest analog weight value and requires moderate number of iterations. The result in Figure 3 indicates that the proposed algorithm outperforms the SPA algorithm for the same input data. This is because the binary cyclic code of length 64 is designed to select scaled transformation. It can be applied to the lattices in order to produce the required number of representatives. The ring of integers of the field is a full module in the field of algebraic number which contains the number l and is a ring. The algorithm is suboptimal, but robust for decoding any class of linear block code and can be realized on a real-time coding scheme.

Figures 4 and 5 show that the proposed algorithm reduces the complexity of decoding [2]. The decoding complexity means the number of iterations of hard-decision decoding. A soft-decision decoding includes multiple hard decision decoding processes. When we perform a soft-decision decoding, the most computational process is hard-decision decoding. Therefore, it is common to indicate the complexity of soft-decision decoding as the number of iterations of hard-decision decoding [6]. In the searching process, if the analog weight of the error pattern is less than a predicted threshold value, then we can safely skip the search for remaining candidate code words. As can be observed from Figures 4 and 5, the computational complexity of the proposed algorithm is low. When E_b / N_o = 4.0dB, the number of iterations of hard-decision decoding is only 3.846 for (23,12) Golay code, which is considerably small. In addition, as can be gleaned from the figures, the number of iterations of hard-decision decoding, which requires the highest computational complexity, decreases steeply as the signal-to-noise ratio increases. Those of the other orders also decrease as the signal-to-noise ratio increases, making the proposed algorithm very fast. The algorithm increases the probability that the correct code word is included in the candidate words. The algorithm reduces the number of hard-decision decoding.

It has been shown that both the error probability and the complexity are reduced. The effect of exploring candidate code words with the proposed algorithm has been confirmed.

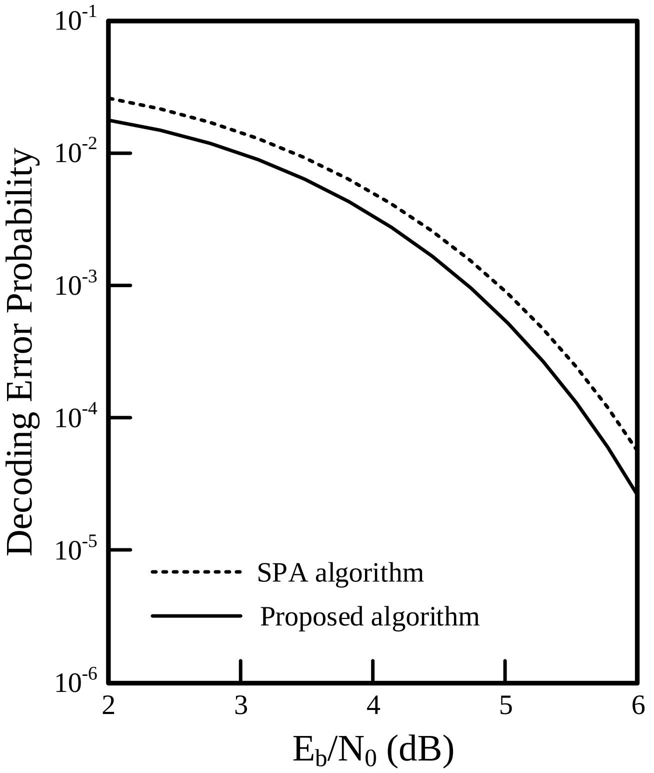

Figure 2. Error probability of Golay (23, 12).

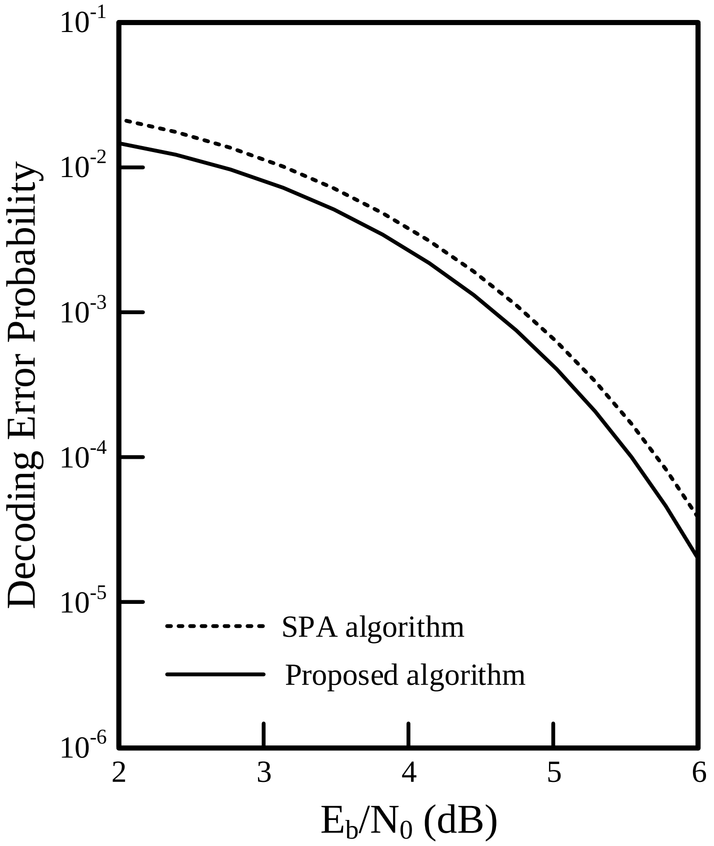

Figure 3. Error probability of Reed-Muller (64, 42).

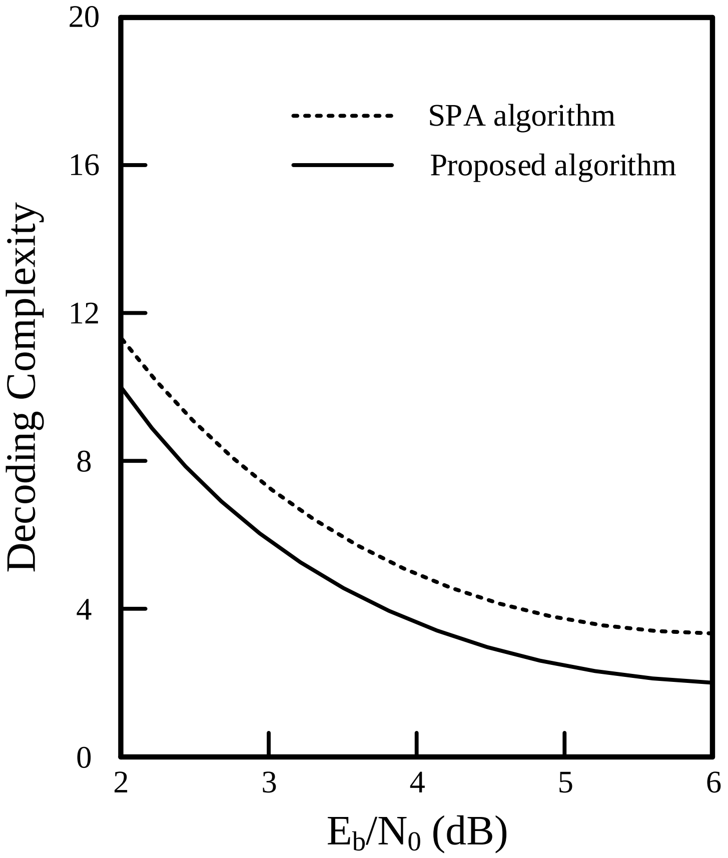

Figure 4. Complexity of Golay (23, 12).

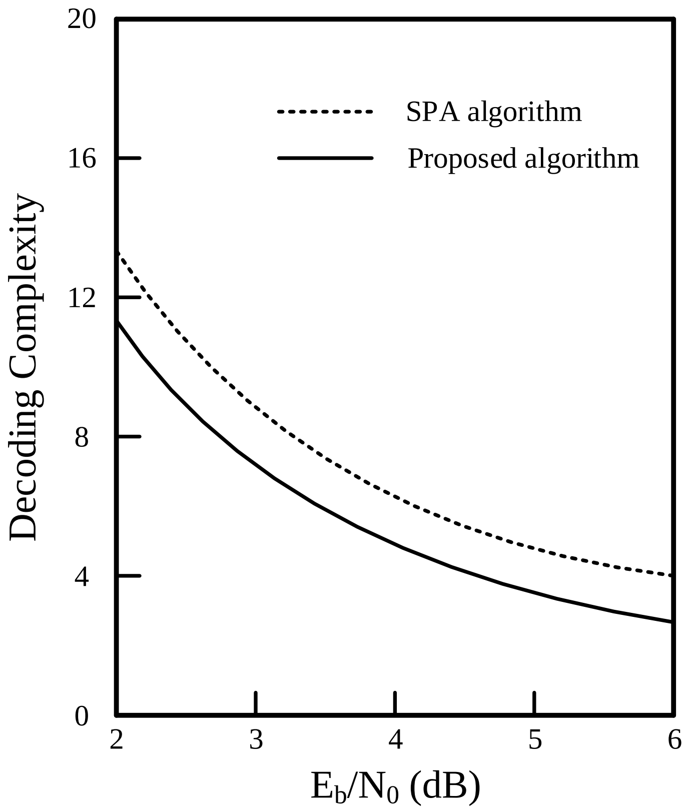

Figure 5. Complexity of Reed-Muller (64, 42).

5- Conclusion

For block codes in communication systems, an efficient algorithm for error controlling is proposed. It is an algorithm for soft decision decoding of block codes. The aim of the algorithm is to reduce the required number of hard-decision decoding and to lower the block error probability. The algorithm finds out a group of candidate code words, in which the most likely one is chosen as a decoding result. It is an algorithm for soft decision decoding of block codes. The sufficient conditions to obtain the optimum decoding are deduced so that the efficient method which explores candidate code words can be presented. The information vector of signal space codes has isomorphic coherence. The path metric in the coded demodulator is the selected components of scaled regions. The carrier decision is derived by the normalized metric of synchronized space.

The transmitted word is included in the set of explored candidate code words. The classes of modules have coefficient ring. The corresponding forms also have the same discriminant modules in quadratic fields. The representation of integers by binary quadratic forms reduces to the problem of similarity of modules in quadratic fields. The position tracking is achieved by the concepts of the theory algebraic numbers such as the ring of integers, integral basis, and decomposition of forms in finite extension field. The required number of hard-decision decoding and the complexity of the algorithm are reduced. The number of candidate code words is reduced, too. The proposed algorithm increases the probability that the correct code word is included in the candidate words. It is shown that both the error probability and the complexity are reduced. The positions of the first hard-decision decoded errors and the positions of the unreliable bits are carefully examined. From this examination, the candidate codewords are efficiently searched for. An efficient and systematic way of soft decision decoding of block codes is provided.

6- Conflict of Interest

The author declares that there is no conflict of interests regarding the publication of this manuscript. In addition, the ethical issues, including plagiarism, informed consent, misconduct, data fabrication and/or falsification, double publication and/or submission, and redundancies have been completely observed by the authors.

7- References

[1] Shim, Yong-Geol. “A Decoding Scheme for Error Control Codes in Communication Networks” Advanced Science and Technology Letters, Vol. 141, (December 23, 2016): 5-8. doi:10.14257/astl.2016.141.01.

[2] Varzakas, P. “Average Channel Capacity for Rayleigh Fading Spread Spectrum MIMO Systems.” International Journal of Communication Systems 19, no. 10 (2006): 1081–1087. doi:10.1002/dac.784.

[3] Garrammone, G. “On Decoding Complexity of Reed-Solomon Codes on the Packet Erasure Channel,” IEEE Communications Letters, vol. 17, no. 4, pp. 773-776, 2013.arzakas, P. “Average Channel Capacity for Rayleigh Fading Spread Spectrum MIMO Systems,” International Journal of Communication Systems, vol. 19, no. 10 (2006): 1081-1087.

[4] Shim, Yong-Geol. “Forward Error Correction Codes in Communication Channels.” International Journal of Control and Automation 10, no. 4 (April 30, 2017): 131–144. doi:10.14257/ijca.2017.10.4.12.

[5] Çalkavur, Selda. “A Study on Multisecret-Sharing Schemes Based on Linear Codes.” Emerging Science Journal 4, no. 4 (August 1, 2020): 263–271. doi:10.28991/esj-2020-01229.

[6] Shim, Yong-Geol. “An Improvement of Soft Decision Decoding Algorithm Using Linear Block Codes.” International Journal of Software Engineering and Its Applications 7, no. 6 (November 30, 2013): 319–324. doi:10.14257/ijseia.2013.7.6.26.

[7] Bossert, M. “An Iterative Hard and Soft Decision Decoding Algorithm for Cyclic Codes,” SCC 2019; 12th International ITG Conference on Systems, Communications and Coding, Rostock (2019): 263-268.

[8] Zhang, Mu, Kui Cai, Kees A. Schouhamer Immink, and Pingping Chen. “Soft-Decision Decoding for DNA-Based Data Storage.” 2018 International Symposium on Information Theory and Its Applications (ISITA) (October 2018): 16-20. doi:10.23919/isita.2018.8664305.

[9] Shim, Yong-Geol. “An Error Control Method with Linear Block Code in Sensor Networks.” International Journal of Distributed Sensor Networks 10, no. 4 (January 2014): 439231. doi:10.1155/2014/439231.

[10] Zarei, B., V. Muthukkumarasay, and Xin-Wen Wu. “A Residual Error Control Scheme in Single-Hop Wireless Sensor Networks.” 2013 IEEE 27th International Conference on Advanced Information Networking and Applications (AINA) (March 2013): 197-204. doi:10.1109/aina.2013.101.

[11] Zhang, Gaoyuan, Hong Wen, Jiexin Pu, and Jie Tang. “Build-in Wiretap Channel I with Feedback and LDPC Codes by Soft Decision Decoding.” IET Communications 11, no. 11 (August 3, 2017): 1808–1814. doi:10.1049/iet-com.2016.0880.

[12] Babalola, Oluwaseyi, and Jaco Versfeld. “Iterative Soft-Decision Decoding of Binary Cyclic Codes Based on Extended Parity-Check Transformation Algorithm.” 2018 IEEE Canadian Conference on Electrical & Computer Engineering (CCECE) (May 2018). doi:10.1109/ccece.2018.8447536.

[13] Wijekoon, V. B., Hoang Dau, and Emanuele Viterbo. “Iterative Decoding of Reed-Solomon Codes Based on Non-Binary Matrices.” 2019 IEEE International Symposium on Information Theory (ISIT) (July 2019): 1082-1086. doi:10.1109/isit.2019.8849566.

[14] Choi, Changryoul, and Jechang Jeong. “Fast and Scalable Soft Decision Decoding of Linear Block Codes.” IEEE Communications Letters 23, no. 10 (October 2019): 1753–1756. doi:10.1109/lcomm.2019.2927218.

[15] Babalola, O. P., O. O. Ogundile, and D. J. J. Versfeld. “A Generalized Parity-Check Transformation for Iterative Soft-Decision Decoding of Binary Cyclic Codes.” IEEE Communications Letters 24, no. 2 (February 2020): 316–320. doi:10.1109/lcomm.2019.2956935.

[16] Lin, Shu, Khaled Abdel-Ghaffar, Juane Li, and Keke Liu. “A Scheme for Collective Encoding and Iterative Soft-Decision Decoding of Cyclic Codes of Prime Lengths: Applications to Reed–Solomon, BCH, and Quadratic Residue Codes.” IEEE Transactions on Information Theory 66, No. 9 (September 2020): 5358–5378. doi:10.1109/tit.2020.2978383.