논문 2005-42TC-11-2

디지털 오디오/비디오, 통신용 전자기기를 위한 Reed Solomon 복부호기 설계에 대해

(Reed Solomon CODEC Design For Digital Audio/Video,Communication Electronic Devices)

안 형 근*

(Hyeong-Keon An)

요 약

현대의 디지털통신기기나 ,오디오/비데오 전자기기엔 항상 비바이나리 에러정정복부호기가 사용되는데 그중 필수적으로 사용되는 Reed-Solomon 복부호화기기의 설계에 대해 기술했다. 2,3 symbol RS 복호기설계법을 설명 후, 새로운 RS 부호화기의 설계법을 제시한다. 각각의 복부호화기기의 동작여부를 예를들어 test해보고 잘 동작함을 확인했다.

Abstract

For Modern Consumer and Communication Elecronic Devices, Always Error Protecting HW and SW is used. The Core is RS(Reed Solomon) Codec in Galois Field GF(2^8). Here New 2 to 3 Symbol RS Decoder Design and Encoder design Method using Normalized error position Value is described. Examples are given to show the methods are working well.

Keywords: RS(Reed Solomon), Syndrome, Encoder, Decoder, Error Locator polynomial, Galois Field(GF)Digital Compact Cassette (DCC), Mini Disc(MD), Audio/Video(A/V)

I. Introduction

Reed Solomon coding theory is very famous well known nonbinary error correction method for Digital Electronic Devices (Consumer and Communication products.)[3].

In this paper, new RS(Reed Solomon) Decoder, which is correcting 2 and 3 symbol errors,and encoder design method is proposed using Normalized error position stored ROM[7]. Here New encoder is designed using Erasure correcting decoding algorithm so removing separate encoding hardware so saving total gate counts of the Codec. The New RS Codec is much simpler and faster than before, So More efficient RS CODEC SOC(System On Chip) design is Possible[1,2].

In chapter II, we briefly described RS(Reed Solomon) ECC algorithm[9]. For example we describe how to calculate syndromes, solve Newtonian identitiy equations. In chapter III, we describe the New RS Decoder algorithm which is correcting 2 symbol error in the codeword RS(32,28) in GF(2^8). This Decoder is used for CDP(Compact Disc Player). Example is showing the algorithm is working well. In MD(Mini Disc Player), DCC, HDTV, Main computer magnetic storage system, 3 symbol error correcting RS decoder is used. And 3 symbol Error

* 정회원, 동명정보대학교 정보통신과
(Dept. of Information and Telecommunication Engineering, Tong Myung University of Information Technology.)
접수일자: 2005년8월3일, 수정완료일: 2005년11월10일

Correcting New algorithm is described in Chapter Ⅳ. Here we also show the example to verify the algorithm.

In chapter V, the new RS encoder, in GF(2^8), design method is described. Here as we already mentioned, 4 Erasure correcting RS decoding algorithm is used for RS(32,28) encoder. For more clarity, we show Encoding example to describe the step of the algorithm and finally we find the syndromes of the output of Designed encoder is Zero so acknowledges that the New RS encoding process is working correctly[3].

In chapter Ⅵ conclusions are made. Future works on 4 symbol error correcting RS decoder is briefly mentioned. Also Divider in GF(2^8) design method is also discussed.

Ⅱ. Syndromes and Error Locator polynomial

An RS(Reed Solomon) codes are based on finite fields, often called Galois fields.

In CDP, RSC(32,28), on GF(2^8) field, codes is used and up to 2 symbol errors can be corrected[2].

An RS code with 8bit symbols will use a Galois field GF(2^8), consisting of 256 symbols. In decoding Reed-Solomon code, we should calculate the Syndromes as in equation 1.

Let

$$C(X)=\sum_{j=0}^{n-1} C_j X^j$$

Be the Transmitted polynomial, and let

$$r(X)=\sum_{j=0}^{n-1} r_j X^j$$

Be the received polynomial. Then error pattern of the channel is

$$E(X)=\sum_{j=0}^{n-1} E_j X^j$$

Where E_j(j=0 to n-1) are error values. Here Syndromes are defined as

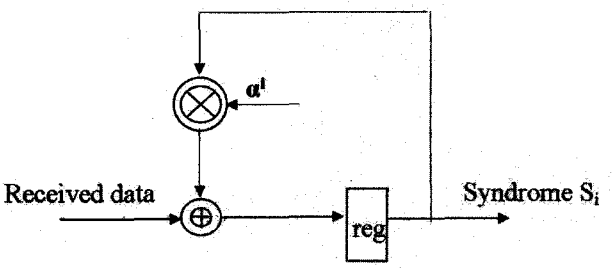


그림 1. RS 복부호기의 신드롬 계산기
Fig. 1. Syndrome calculator of RS codec.

$$S_i = E(\alpha^i)(i=0,1,\cdots,2t-1) \quad (1)$$

For t error correction coding.

In this paper, for finding Error values and positions, syndrome calculator shown in Fig.1 is used[5,6,8].

Now if there are t errors, error values are $E_n(n=0,2\cdots,t-1)$ and their positions are α^{jn} (n=0,1,⋯,t-1).

Then Let

$$\beta_j(j=0,1,\cdots,t-1)=\alpha^{jn}(n=0,1,\cdots,t-1)$$

and Error Locator polynomial is defined as

$$\delta(X)=(X-\beta_0)(X-\beta_1)\cdots(X-\beta_{t-1}) = \sum_{k=0}^{t} X^k \delta_{t-k} \quad (2)$$

Now Newton's identities are following set of equations.

$$\sum_{j=1}^{t} S_{t-j+v}\delta_j = S_{v+t}(v=0,1,2\cdots,t-1) \quad (3)$$

These equations are for t error correcting Reed-Solomon codec[4]. If we apply these equations to 3 symbol error correction case (t=3), all the δ_i (i=1,2,3) are got as described in the next section[8].

Ⅲ. Two Symbol Error Correcting Reed Solomon Decoder Design for CDP

This algorithm can be used for RS decoder of CDP. Now we describe the way briefly as follows.

Normalize first to derive the new method, the error

location polynomial for 2 errors[2,9].

$$\delta(x) = X^2 + \delta_1 X + \delta_2 \quad \text{by} X = \delta_1 x$$

we get

$$\delta(x) = X^2 + x + K, \text{ where } K = \delta_2/\delta_1^2 \tag{4}$$

$$T_2(K) = \sum_{i=0}^{m-1} K^{2^i} \text{ and } m = 8 \tag{5}$$

Hence

$$T_2(K) = \sum_{i=0}^{m-1} K^{2^i} = K + K^2 + K^4 + K^8 + K^{16} + K^{32} + K^{64} + K^{128} \tag{6}$$

(Theorem) If $\theta = \lambda - \lambda^2, \lambda \in GF(2^m)$, then $Tr(\theta) = T_2(\theta) = 0$.

$$\text{Here } Tr(K) = T_2(K) = \sum_{i=0}^{m-1} K^{2^i}$$

From the thorem, equation (4) has a solution when equation (5) $Tr(K) = T_2(K) = 0$[3].

In this case, if $K = (k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7)$, $k_i \in G^F(2)$, then $k_5 = 0$. And 2 solutions x_1, x_2 of equation (4) can be got as in equation (7).

$$x_1 = (k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7) \begin{pmatrix} 01101011 \\ 00010111 \\ 01010111 \\ 10110100 \\ 01110111 \\ 10000000 \\ 10100100 \\ 00001010 \end{pmatrix} \tag{7.a}$$

$$x_2 = 1 + x_1 \tag{7.b}$$

Now real solutions X_1, X_2 are

$$X_1 = \delta_1 x_1, \; X_2 = \delta_1 x_2 \tag{8}$$

Also two errors values are calculated as follows.

$$S_2 = e_1 X_1^2 + e_2 X_2^2$$
$$S_1 = e_1 X_1 + e_2 X_2 \tag{9}$$

Hence

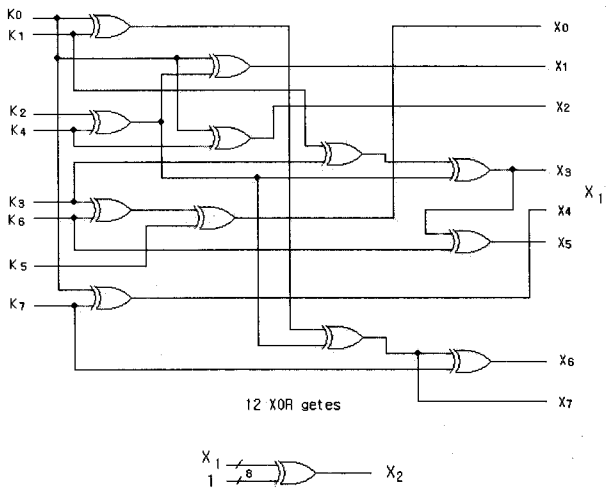


그림 2. K vector를 2개의 정규오류위치로 변환하는 논리회로

Fig. 2. Logic circuit which converts k to 2 normalized error locations.

$$E_1 = \frac{S_1 X_2 + S_2}{X_1 X_2 + X_1^2}$$
$$E_2 = \frac{S_1 X_1 + S_2}{X_1 X_2 + X_2^2} \tag{10}$$

In this way, 2 error locations and error values are all found. Equation (7) can be drawn as in Fig.2. Circuit. From K to 2 error locations, we use Fig.2 circuit.

(EXAMPLE) In $GF(2^8)$, when code polynomial $C(x) = 0$ is transmitted to the receiver, the received polynomial.

$$r(x) = \alpha^2 x + \alpha^3 x^4.$$

So two error values and locations are α^2 at and α^3 at α^4. Verify these values using the new method.

<sol>

$$S_1 = \alpha^3 + \alpha^7 = \alpha^{103}$$
$$S_2 = \alpha^4 + \alpha^{11} = \alpha^{116}$$
$$S_3 = \alpha^5 + \alpha^{15} = \alpha^{26}$$
$$S_4 = \alpha^6 + \alpha^{19} = \alpha^{105}$$

The error locator polynomial is $\delta(X) = X^2 + \delta_1 X + \delta_2$, where

$$\begin{pmatrix}\delta_2\\ \delta_1\end{pmatrix}=\begin{pmatrix}S_1S_2\\ S_2S_3\end{pmatrix}^{-1}\begin{pmatrix}S_3\\ S_4\end{pmatrix}=\begin{pmatrix}\alpha^5\\ \alpha^{224}\end{pmatrix}$$

hence

$$K=\delta_2/\delta_1{}^2=\alpha^{67}=(01000011)$$

So from equation (7).
We get 2 normalized error locations as follows.

$$x_1=(01000011)\begin{pmatrix}01101011\\ 00010111\\ 01010111\\ 10110100\\ 01110111\\ 10000000\\ 10100100\\ 00001010\end{pmatrix}=(10111001)$$

$$=\alpha^{32}$$

$$\therefore X_1=\delta_1x_1=\alpha^{32}\alpha^{224}=\alpha$$

$$X_2=\delta_1x_2=\delta_1(x_1+1)=\alpha^{224}\alpha^{35}$$

$$=\alpha^{259}=\alpha^4$$

These are correct 2 error locations.
Two error values are from equation (10),

$$Y_1=\frac{S_1X_2+S_2}{X_1X_2+X_1^2}=\frac{\alpha^{107}+\alpha^{116}}{\alpha^5+\alpha^2}=\frac{\alpha^{227}}{\alpha^{225}}=\alpha^2$$

$$Y_2=\frac{S_1X_1+S_2}{X_1X_2+X_2^2}=\frac{\alpha^{104}+\alpha^{116}}{\alpha^5+\alpha^8}=\frac{\alpha^{231}}{\alpha^{228}}=\alpha^3$$

These are correct 2 error values.

Ⅳ. Triple Symbol Error Correcting Reed Solomon Decoder Design for DCC,MD (Digital Compact Cassette, Mini Disc Player)

This 3 Symbol Error Correcting RS decoder can also be used for Digital Communicating Modem LSI. In GF(2^8), If there are 3 symbol errors in the received codeword, we can find 3 error positions and Error values as follows[4,7].

Here we use ROM tables as in 2 symbol error case [2]. In this case, Error Locator polynomial is

$$X^3+\delta_1X^2+\delta_2X+\delta_3=0 \qquad (11)$$

Here

< Zi ROM table >

Address(δ / $E^{3/2}$)	data (Z_i, i=1,2,3)
0	0,1,1
1	•
α	•
α^2	•
•	•
•	•
•	•
α^{239}	α^{157}, α^{181}, α^{156}
•	•
α^{254}	•

그림 3. 방정식 15에대한 ROM 테이블
Fig. 3. ROM table corresponding to equation 15. When Address = 0, Only 2 roots exist .

$$\delta_1=(S_1S_3^2+S_1^2S_5+S_2^2S_3+S_0S_2S_5+S_0S_3S_4+S_1S_2S_4)/\chi,$$

$$\delta_2=(S_0S_4^2+S_2S_3^2+S_2^2S_4+S_0S_3S_5+S_1S_2S_5+S_1S_3S_4)/\chi,$$

$$\delta_3=(S_3^3+S_1S_4^2+S_2^2S_5+S_1S_3S_4)/\chi \qquad (11\text{-}1)$$

where $\chi=S_2^3+S_0S_3^2+S_1^2S_4+S_0S_2S_4$ From equation 13, if $X=\delta_1+y$, also if

$E=\delta_1^2+\delta_2, \delta=\delta_1\delta_2+\delta_3$ then

We get

$$Y^3+EY+\delta=0 \qquad (12)$$

If $E=0, Y=(\delta)^{1/3}$, otherwise

Let's define $Z_i=E^{-1/2}Y_i\ (i=1,2,3)$

$$Z^3+Z+\delta/E^{3/2}=0 \qquad (13)$$

From Equation 6, corresponding to Add= $\delta/(E^{3/2})$ we can construct ROM table of root of equation (13) as in Fig.3 .

Once we find $Z_i(i=1,2,3), Y_i(i=1,2,3)=(E^{1/2}Z_i)$ So exact Error positions are

$$X_i=Y_i+\delta_1(i=1,2,3) \qquad (14)$$

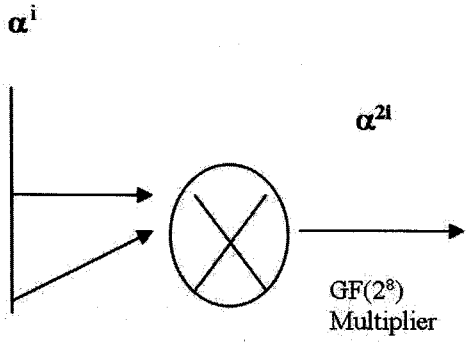
Also Error values are

$$E_i=(S_0\delta_3/X_i+S_1(\delta_1+X_i)+S_2)/(X_i^2+\delta_2) \quad (i=1,2,3) \qquad (15)$$

<Square ROM table>

Address α^i	Data α^{2i}
0	0
1	1
α	α^2
α^2	α^4
α^3	α^6
•	•
•	•
α^{254}	α^{253}

1) 자승을 계산하는 ROM표
1) Square calculation using ROM



2) 곱셈기를 이용한 자승계산기
2) Square calculation with Multiplier

그림 4. ROM을 사용 않는 자승계산기
Fig. 4. Square calculator with and without ROM.

As we see, there are many GF(2^8) Arithmatic operations to compute the Error values and positions. In Fig.4. we show how to compute square values. Other operations needed are $\alpha^{1/2}, \alpha^j/\alpha^j$. Allthese operations can be done using only Inverse calculator and Multiplier.

Next section, we show how to design Reed-Solomon Encoder using RS Erasure Decoder[4].

<Example> Triple Error correcting Reed Solomon Decoder example :

From the Transmitter, we send all 0 data so Code polynomial $C(x)=0$. In Receiver, Received polynomial $R(x)=\alpha+\alpha x+\alpha^2 x^2$.

In this case, find 3 error values and positions. All code symbols are 8 bits wise so GF(2^8) field elements are used.

<Solution>

We first find Syndromes :
$S_0=\alpha^2, S_1=\alpha+\alpha^2+\alpha^4=\alpha^{239}\ S_2=\alpha^{37}, S_3=\alpha^{75}$, $S_4=\alpha^{219}, S_5=\alpha^{24}$. From Equations (11-1), we find out $\delta_1=\alpha^{198}, \delta_2=\alpha^{199}, \delta_3=\alpha^3$. So from equations (12), $E=\alpha^{248}, \delta_2=\alpha^{101}$. Hence $\delta/E^{3/2}=\alpha^{239}$.

So from following equation,

$$Z^3+Z+\alpha^{239}=0.$$

So Using ROM table in fig.3, we find that

$$Z_i=\alpha^{157}, \alpha^{181}, \alpha^{156}$$

Therefore

$$Y_i=E^{1/2}Z_i=\alpha^{26}, \alpha^{50}, \alpha^{25}(i=1,2,3)$$

So from equation(14),

$$X_i=Y_i+\delta_1(i=1,2,3)=\alpha^0, \alpha^1, \alpha^2$$

These are 3 correct Error ositions and 3 error values are calculated from equation (15), as α, α, α^2. These are also correct 3 error values as we see from received polynomial $r(x)$.

V. New Reed Solomon Encoder Design For Digital A/V Devices

When we design a Reed Solomon Encoder, normally we use separate Encoderfor RS Codec. But VLSI H/W of this method becomes very complex, because there is separate RS Encoder and Decoder and Encoder itself is not so simple in HW wise also.

Here to save the Encoding HW(Hardware) we briefly describe the encoding hardware ,which is the

Erasure corrector of the RS Decoder. So Encoder is part of the RS decoder and we neednot design the separate Encoder saving the Encoder HW[4,5].

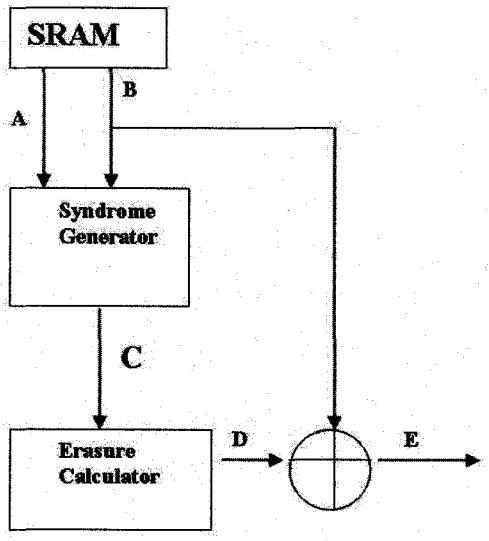
<Encoding Steps>

1. **Assume arbitrary parity values (Normally assume 0) : $P'_0, P'_1, P'_2, \cdots, P'_{k-1}$**
2. **Using K syndromes calculated by the cct in Fig. 3, Erasure Decoder get the K Erasure Values.**
3. **K Erasure values are added to the assumed Parities nd the result values Are True Parities.**

The New Encoder Block Diagram is shown in Fig. 5.

<Example>

In RS(32,28) code system of GF(2^8), let's assume all '0' parities. The \ codeword polynomial $C(x) = P_0 + P_1x + P_2x^2 + P_3x^3 + D_4x^4 + \cdots + D_{31}x^{31}$, where $P_i\,(i = 0,1,2,3)$ are parities and D_j $(j = 4,5,\cdots,31)$ are data bytes. If $D_j(j = 3,4,\cdots,30)$, $D_{31} = \alpha^0 = 1$, Find the Correct Parities $P_i\,(i = 0\,\text{to}\,3)$



A : $D_0, D_1, \ldots, D_M$ (Data)
B : $P'_0, P'_1, \ldots, P'_{k-1}$ (Error Parities)
C : $S_0, S_1, \ldots, S_{k-1}$
D : $E_0, E_1, \ldots, E_{k-1}$ (Erasure Values)
E : $P_0, P_1, \ldots, P_{k-1}$ (Correct Parities)

그림 5. 새로운 RS 부호화기의 블록그림
Fig. 5. Block Diagram of New RS Encoder.

<Sol>

Parity positions are known so this is the Erasure Correction case. Because all assumed Parities are 0 and using given data bytes, we calculate syndromes.

$$\begin{aligned} S_0 &= C(\alpha^0) = 1 \\ S_1 &= C(\alpha^1) = \alpha^{31} \\ S_2 &= C(\alpha^2) = \alpha^{62} \\ S_3 &= C(\alpha^3) = \alpha^{93} \end{aligned} \tag{16}$$

Now we setup following equations to find 4 erasure values E_0, E_1, E_2, E_3.

$$\begin{aligned} &E_0 + E_1 + E_2 + E_3 = S_0 \\ &E_0 + E_1\alpha + E_2\alpha^2, E_3\alpha^3 = S_1 \\ &E_0 + E_1\alpha^2 + E_2\alpha^4, E_3\alpha^6 = S_2 \\ &E_0 + E_1\alpha^3 + E_2\alpha^6, E_3\alpha^9 = S_3 \end{aligned} \tag{17}$$

From equations (1) and (2),

$$\begin{pmatrix} E_0 \\ E_1 \\ E_2 \\ E_3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 \end{pmatrix}^{-1} \begin{pmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{pmatrix} = \alpha^{108} \begin{pmatrix} \alpha^{110} & \alpha^{50} & \alpha^{48} & \alpha^{104} \\ \alpha^{50} & \alpha^{30} & \alpha^{149} & \alpha^{45} \\ \alpha^{48} & \alpha^{149} & \alpha^{27} & \alpha^{44} \\ \alpha^{104} & \alpha^{45} & \alpha^{44} & \alpha^{101} \end{pmatrix} \begin{pmatrix} \alpha^0 \\ \alpha^{31} \\ \alpha^{62} \\ \alpha^{93} \end{pmatrix} = \begin{pmatrix} \alpha^{148} \\ \alpha^{67} \\ \alpha^{205} \\ \alpha^{249} \end{pmatrix} \tag{18}$$

So From Fig.5 and Equation (18), we find correct Pasrities as follows.

$$P_i, i=0 \text{ to } 3] = [\, E_i + \text{Initial } P_i \,] = \{i=0 \text{ to } 3\}$$

$$= [\, \alpha^{148}, \alpha^{67}, \alpha^{205}, \alpha^{249} \,]$$

$$\begin{pmatrix} \alpha^{148} \\ \alpha^{67} \\ \alpha^{205} \\ \alpha^{249} \end{pmatrix}^T + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}^T$$

Using this Correct Parities, we find all syndromes $S_j, j = 0$ to 3 are zeros and this is correct.

VI. Conclusions

In this Paper, we described how to implement 2 to 3 symbol error correcting RS ECC decoder. Here Tracing K vector and Normalized error position

stored ROM is used. We also study how to implement RS ECC encoder using Erasure correcting RS decoder. For DAT(Digital Audio Tape Recorder) case, 6 parities are used for the Encoder, and we use 6 Erasure correcting RS Decoder for the Encoder.

Later We will study how to implement 4 symbol error correcting RS decoder using GF(2^4) sub field, resulting in even further greately reducing RS codec HW circuitry

This Kind of RS Codec is used for most of the Current Digital Audio/Video and Communication devices, for example CDP, MP3, MD, HDTV, DMB, Digital Cellular phone, etc.

In Our future we will study how to implement Galois Field Arithmatic Operator in GF(2^8) field using Subfield GF(2^4) arithmetic operation, for example Divider. Here both direct divider and indirect divider can be used using Inverse calculator and Multiplier in GF(2^4) field [1].

References

[1] US patent number 5227992, "Operational Method and Apparatus over GF(2^m) using a Subfield GF($2^{m/2}$)", Man-young Lee, Hyeong-Keon An et al., 1993 Jul. 13

[2] Hyeong-Keon An, "2 Error Correcting RS Decoder design", IDEC Conference Paper, 2004.

[3] Hyeong-Keon An, TS Joo et al, "The New RS Ecc Codec For Digital Audio and Video", IEEE CES Conference paper, PP112-115, 1992.

[4] Lee Man Young, "BCH coding and Reed-Solomon Coding theory", 1990, Minumsa(Daewoo Academic Press).

[5] Sunghoon Kwon and Hyunchul Shin, "Anarea-efficient VLSI architecture of Reed-Solomon decoder/encoder for digital VCRs", IEEE Transactions on Consumer Electronics, Vol. 43, No.4, Nov. 1997.

[6] Kwang Y.Liu, "Architecture for VLSI design of Reed-Solomon Decoders", IEEE Transactions on Computers. Vol.33, No.2, Feb. 1984.

[7] 岡野博: "ROM used 2 to 3 error correcting BCH Decoder Improvement", 信學技報 ,AL 82-56 (1982).

[8] Hsu, I.K., I.S.Reed, "The VLSI Implementation of a Reed-Solomon Encoder Using Berlekamp's Bit-Serial Multiplier Algorithm", IEEE Trans. On Computer, Vol.C-33, No.10, pp.906-911(1984).

[9] Shu Lin, Daniel J. Costello,Jr., "Error Control Coding", Prentice-Hall, pp.240 -261(20044).

저 자 소 개

안 형 근(정회원)

- He received B. Engineering Degree in electrical engineering from Seoul National University, Seoul, KOREA, in 1979 and M.S degree in electrical science from Korea Advanced Institute of Science and Technology, Seoul, Korea in 1981, and the Ph.D. degree in electrical engineering from State University of New York at Stony Brook , NY, USA., in 1988.
- In 1988, he joined Samsung Electronics Co.Ltd as a Senior Researcher working for design ing System LSI for 10 years.
- From 1998 to 1999, He worked for Telson Electronics Corp. working for CDMA handphone design.
- In 2000, he joined Tong Myoung University in Busan as a Professor in Dept. Of Information and Telecommunication engineering.
- He has interests in designing CDMA and GSM hand phone and also in System LSI (Non Memory) design.
- He also operates Venture Comapany for Producing various Mobile phones and GPS/MP3Engines.