Reed-Solomon 부호의 성능분석

Performance Analysis of the Reed-Solomon Codes

鄭 濟 洪*, 朴 鎭 秀**
(Je Hong Jeong, Jin Soo Park)

요 약

본 논문은 Reed-Solomon부호의 복호가능어 가중치 분포에 대한 명시적 식과 근사식을 구하여 이를 복호기 오류확률 $P_E(u)$에 적용하고, 복호기 오류확률의 상한식을 구하고 분석하였다.

t+1개 이상의 오류가 발생했을때 복호기 오류확률의 추정치 Q와 Q'를 개선하여 식 Q^*를 제안하고, 컴퓨터 시뮬레이션을 수행한 결과 가중치 u가 커질때 복호기 오류확률은 추정치 Q와 Q'에는 접근하였으나, 본 논문에서 제안한 식 Q^*와는 일치됨을 확인하였다.

그리고, 가중치 u가 부호의 길이 n에 접근할때, 복호가능어의 명시적 식 D_u와 근사식 D_u'가 서로 일치하고, 복호기 오류확률 $P_e(u)$와 근사오류확률 $P_e(u')$가 일치함을 보였다. 또한 t+1개 이상의 오류가 발생했을때 복호기 오류확률은 $1/t!$보다 작으며, 가중치분포 A_u에 $V_n(t)$를 곱한 결과는 근사복호가능어 D_u'와 일치함도 확인하였다.

Abstract

This paper derived the explicit formula and approximation formula for the weight distribution of decodable word of a Reed-Solomon code, the upper bound of the decoder error probability was derived and analyzed.

If more than or equal to t errors accur, this paper proposed the expression Q^* which is the improved expression of Q and Q'. To show the validity of analysis, computer simulations were performed. The results showed that the decoder error probability approached to the estimate Q and Q' as u becomes large and coincided with the improved expression Q^* which was proposed in this paper.

And this paper showed that the explicit formula D_u of decodable word coincided with the approximation formula D_u' as weight u approaches to the code length n. Also it were showed that if more than t errors occur, then the probability of decoder error is less than $1/t!$, and that the weight distribution A_u multiplied by $V_n(t)$ coincided with the decodable word D_u.

I. 서 론

부호의 오류정정이론은 통신및 컴퓨터시스템에서 채널상의 잡음으로 인하여 발생하는 오류의 검출과 정정에 이용되며, 디지탈 자료의 전송과 자료저장 시스템에서는 고속의 신뢰성 있는 정보의 송수신이 요구되고 있다. 신뢰성 있는 정보의 송수신을 위하여 가장 널리 사용되고 있는 오류정정부호에는 Reed-Solomon(이하 RS부호라 함)와 길쌈부호가 있다.

RS부호는 비이원 부호로서 연집오류가 발생하는 채널인 CD, DAT, VCR등과 임의 오류의 정정에 이용되고 있으며, RS부호의 성능을 평가하는 중요한 요소중의 하나인 복호기 오류확률이다.

부호 C의 길이를 n, 정보의 길이를 k, 최소거리를 d, q를 솟수의 양수 멱승이라 하면, GF(q)상에서 t개의

* 건양대학교 전자계산학과
** 충북 청주시 청주대학교 전자공학과
접수일자 : 1992년 10월 17일

오류를 정정할수 있는 (n,k,t) RS부호의 매개변수는 다음과 같다.

$n=2^m-1$
$n-k=2t$
$d_{min}=2t+1$

특히 $d=n-k+1$일때 MDS(maximum distance separable)부호라 하며, MDS부호의 가중치분포에 대하여 Assmus와 Mattson, Turyn과 Forney, 그리고 Kasami등의 세 연구 그룹이 서로 독립적으로 연구하였다.[7]

만일 전송된 부호어가 t개 이하의 오류를 가지면 성공적으로 그 오류를 정정할수 있으나 t개보다 많은 수의 오류가 발생하면 복호기가 부호어를 찾는데 실패하든지, 또는 전송된 부호어와는 다른 부호어를 발견한다. 이때 전자를 복호기 실패라 부르며 기호로 P_F라 표시하고, 후자의 경우를 복호기 오류라 하며 기호로 P_E라 표시한다.

발생된 오류의 수가 t개 이하이면 $P_E=P_F=0$이고, t 초과 t+1 미만이면 $P_F=1$, $P_E=0$가 되며, t+1개 이상이면 일반적으로 P_F나 P_E를 계산하거나 추정하는 것이 매우 어렵다.

채널상에서 u개의 오류가 발생했을때 $u\le t$이면 $P_E(u)=P_F(u)=0$이고, $t<u<t+1$이면 $P_E(u)=0$, $P_F(u)=1$이며, $t+1\le u$이면 $P_E(u)=P_F(u)=1$인 관계가 성립하기 때문에 $P_E(u)$를 구하면 $P_F(u)$를 계산할수 있다.[11]

t+1개 이상의 오류가 발생했을때 완전확률 오류형태에서 자기발견적 추정 (heuristic estimate)은 다음과 같다.

$$Q=(q^k-1)*V_n(t)/q^n$$
$$=(q^{-r}-q^{-n})*V_n(t) \quad (1)$$

여기서, $r=n-k$ 이고

$$V_n(t)=\sum_{s=0}^{t}\binom{n}{s}(q-1)^s \quad (2)$$

이다. 식(1)과 복호기 오류 P_E는 다음과 같은 추정할 수 있다.

$$P_E\approx Q\cdot Pr\{\ge t+1\text{개의 오류}\}$$

이러한 추정을 일반화하기 위한 많은 연구가 있었는데, R.J.McEliece와 L.Swanson은 Q값을 증가하여 다음과 같이 Q'를 취하였다.[1]

$$Q'=(q-1)^{-r}V_n(t) \quad (3)$$

그 결과, Reed-Solomon부호에 대하여

$$P_E\le Q'\cdot P_r\{\ge d-t\text{ 오류}\}$$

임을 확인하였다.

Kasami와 Lin은 RS부호의 복호기 오류문제를 연구하였는데, q-ary대칭 채널상에서 e를 채널기호 오류확률이라할때 다음과 같은 관계가 성립함을 나타내고 있다.

$$\sum_{u=t+1}^{n}P_e(u)\binom{n}{u}e^u(1-e)^{n-u}\le Q \quad (4)$$

본 논문에서는 Q값을

$$Q^*=q^{-r}V_n(t) \quad (5)$$

와 같이 간단한 식으로 표현하여 가중치 u가 n에 접근할때 그 값이 Q, Q'값보다 복호기의 오류확률 $P_E(u)$에 더 일치함을 보인다.

특히 n,k,t가 (7,5,1), (7,3,2), (7,1,3) 인 경우와 (15,7,5), (15,7,4), (15,5,5), 그리고 (31,17,7), (31,15,8), (31,15,9), (31,15,10)인 경우에 Q^*값이 Q, Q'값보다 $P_E(u)$에 더 일치함을 확인한다.

Du를 가중치 u의 복호가능어의 수라 하자. 복호가능어란 단어가 부호어로부터 거리 t 이내에 있음으로 정의되는데, 만일 복호기 거리내에 있으면 복호가능어의 가중치 분포는 복호기 오류확률을 구하는데 이용될수 있다.[4]

가중치 u의 오류형태가 발생했을때 복호기 오류확률을 $P_E(u)$라 하면, 다음 식과 같다.[2]

$$P_E(u)=D_u/(\binom{n}{u}(q-1)^u),\ t+1\le u\le n \quad (6)$$

즉, $P_E(u)$는 복호가능어 수에 대한 전체벡터공간에서 가중치 u의 단어수 비와같다.

본 논문에서는 복호 가능어의 가중치분포에 대한 명시적 식(explicit formula)과 근사식(approximation formula)을 구하고, 이를 식(6)에 적용하여

가중치 u가 커질때 복호기 오류확률 $P_E(u)$값이 본 논문에서 제시한 식(5)에 접근함을 보인다. 특히 근사 복호확률 $P_E(u')$는 u가 부호장 n에 접근함에 따라 McEliece가 제안했던 Q값이나 K.M.Cheung이 제안했던 Q'값보다 본 논문에서 재안한 Q*에 더 근사적으로 일치함을 보인다.

또한 상한, 가중치분포, 오류확률등에 컴퓨터 시뮬레이션을 수행하여 그 결과를 분석한다.

Ⅱ. 복호가능어의 명시적 식과 근사식

N개의 객체(object)와 u개의 특성(property)집합 P(1), P(2),...,P(u)을 생각하자. 그리고 $N(i_1, i_2, \ldots, i_r)$이 특성 $P(i_1), P(i_2), \ldots, P(i_r)$을 갖는 객체의 수라 하면, 특성을 갖지 않는 객체의 수 N(0)는 다음과 같다.[4]

$$N(0)=N-\sum_{i}N(i)+\sum_{i_1<i_2}N(i_1,i_2)+\cdots+(-1)^r\sum_{i_1<i_2<\cdots i_r}N(i_1,i_2,\ldots,i_r)+\cdots+(-1)^u N(1,2,3,\ldots,u) \qquad (7)$$

D를 C의 복호가능어 집합이라 하자. d가 $u \geq n-l$인 해밍 가중치 u를 갖는 복호가능어이고, 그 좌표를 {0,1,...,n}이라 표시하면, d는 v=n−u일때 v개의 영원소를 갖는다. ($v \leq 1$)

V를 v=n−u인 v개의 좌표집합, 즉 |V|=v이고 $\{i_1,i_2,\ldots,i_j\} \subseteq \{0,1,2,\ldots,n-1\}-V$가 j개의 좌표집합이라 하면, 복호가능어 $d \in S_V(i_1,i_2,\ldots,i_j)$는 항상 적어도 u+j개의 영원소를 갖는다.

$$T_{v,j}=\sum_{|V|=v}\sum_{i_1<i_2<\cdots<i_j}|S_V(i_1,i_2,\ldots,i_j)|$$

이라 하자. 즉 $T_{v,j}$가 포함과 배제의 식에서 j번째 항이라면, $0 \leq j \leq 1-v$에 대하여 $S_V(i_1,i_2,\ldots,i_j)$의 복호가능어에서 영의 갯수는 l이하이다.

해밍영역내에 위치한 모든 단어에 대하여 복호가능어를 포함하는 서로 소인 coset Vn(t)가 존재한다. 각각의 coset 는 C내에 있는 각 부호어에 coset leader a를 더하여 구성한다. 서로 다른 coset leader에 대하여 q^{k-v-j}개의 부호어가 존재한다면, $S_V(i_1,i_2,\ldots,i_j)$에 있는 복호가능어의 갯수는 다음식과 같다.

$$|S_V(i_1,i_2,\ldots,i_j)|=q^{k-v-j}\,V_n(t),\quad 0 \leq j \leq 1-v \qquad (8)$$

0,1,2,...,n−1으로부터 V를 선택하는데는 $\binom{n}{v}$의 경우가 존재하고, V의 각 선택에 대하여 나머지 u−n−v좌표로부터 $i_1,i_2,\ldots,i_j$를 선택하는데는 $\binom{u}{j}$개의 경우가 존재하므로,

$$T_{v,j}=\binom{n}{v}\binom{u}{j}q^{k-v-j},\quad 0 \leq j \leq l-v \qquad (9)$$

$l-v+1 \leq j \leq n-d-v+t$에 대하여 영의 갯수가 l을 초과하기 때문에 $T_{v,j}$는 식(9)로 표현될수 없다. 이 경우 $T_{i,j}$는 $S_V(i_1,i_2,\ldots,i_j)$의 수를 나열하여 계산한다.

영 부호어에 대하여 V를 선택하는데 $\binom{n}{v}$의 경우가 존재하고, 나머지 j개의 영좌표를 선택하는데는 $\binom{u}{j}$개의 방법이 있다. $u+j \leq m \leq n-d+t$일때 가중치 n−m의 복호가능어에 대하여 V를 택하는데 $\binom{m}{v}$경우가 존재하고, 나머지 j개의 영좌표를 선택하는데는 $\binom{m-v}{j}$경우가 존재한다.

가중치 n−m에 대하여 D_{n-m}복호가능어가 존재하므로

$$T_{v,j}=\binom{n}{v}\binom{u}{j}+\sum_{m=v+1}^{n-d}\binom{m}{v}\binom{m-v}{j}D_{n-m}, \qquad (10)$$
$$l-v+1 \leq j \leq n-d-v.$$

이 성립한다. $n-v-d+t+1 \leq j \leq n-d-t$에 대하여 복호가능어 내에서 영의 갯수는 n−d+t−1 이상 n−t 이하이므로 $S_V(i_1,i_2,\ldots,i_j)$는 좌표 $\{0,1,2,\ldots,n-1\}-(V \cup \{i_1,i_2,\ldots,i_j\})$에서 t개 이하 가중치의 모든 단어를 포함한다. 따라서,

$$|S_V(i_1,i_2,\ldots,i_j)|=\sum_{i=0}^{t}\binom{u-j}{i}(q-1)^i, \qquad (11)$$
$$n-v-d+t+1 \leq j \leq n-v-t$$

$$T_{v,j}=\binom{n}{v}\binom{u}{j}+\sum_{m=v+j}^{n-d}\binom{u-j}{i}(q-1)^i, \qquad (12)$$
$$n-v-d+t+1 \leq j \leq n-v-t$$

이 성립한다. $n-v-t+1 \leq j \leq n-v$에 대하여 j가 n−v−t+1이상이므로 영의 갯수 v+j는 n−t+1 보다 크거나 같다. 따라서, 영이 아닌 원소의 갯수는 t보다 작으며, $(V \cup \{i_1,i_2,\ldots,i_j\})$에서 영인 모든 단어는 복호가능하므로,

$$|S_V(i_1,i_2,\ldots,i_j)|\,q^{u-j},\quad n-v-t+1 \leq j \leq n-v \qquad (13)$$

그리고

$$T_{v,j}=\binom{n}{v}\binom{u}{j}q^{u-j},$$

이 성립한다. 포함과 배제의 원리에 의하여 가중치 u 의 복호가능어의 수 D_u는 다음식과 같다.

$$D_u=\sum_{j=0}^{u}(-1)^j T_{v,j} \tag{14}$$

식(14)에서 $l-v-1$개 이하의 모든 항이 무시된다면 식(15)이 성립한다.

$$D_u=\binom{n}{u}\sum_{j=0}^{l-v-1}(-1)^j\binom{u}{j}q^{k-v-j}Vn(t)+E_1 \tag{15}$$

단, $E_1=\binom{n}{u}(-1)^{l-v}\binom{u}{l-v}q^{k-1}Vn(t)+\sum_{j=l-v+1}^{n-v}T_{v,j}$

$|E_1|$은 $l-v$항에 의하여 나타내어 질수 있다. 즉, $|E_1|\le\binom{n}{u}\binom{u}{l-v}q^{k-1}Vn(t)$이다. 만일,

$|E_2|=\binom{n}{u}\sum_{j=l-v}^{u}(-1)^j\binom{u}{j}q^{k-v-j}Vn(t)$을 더하고 식(14)로부터 빼면

$$D_u=\binom{n}{u}((q-1)^u/q^{n-k})\cdot E_1+E_2 \tag{16}$$

가 성립한다. 만약,

$\binom{u}{l-v}q\ge\binom{u}{l-v+1}$ 즉, $u\ge\{(q+1)/q\}\cdot(n-1)-1$

이면, E_2는 교대부호와 감소하는 양의 합이므로,

$$D_u=\binom{n}{u}\{(q-1)^u/q^{(n-k)}\}\cdot Vn(t)+E \tag{17}$$

가 된다. 여기서 $E=E_1+E_2$이고, $|E|\le 2\binom{n}{u}\binom{u}{l-v}q^{k-1}Vn(t)$이다. 따라서 D_u는 $\binom{n}{u}\{(q-1)^u/q^{n-k}\}*Vn(t)$로 근사화될수 있으며, 근사화의 유용성은 비율 $R=E/[\binom{n}{u}(q-1)^u q^{-(n-k)})*Vn(t)]$이 얼마나 작아지는지에 의존한다. $|E|$에 상한을 이용하면 이 비율에 대한 상한은 다음과 같다.

$$R\le 2\binom{u}{n-1}q^{k-1}(q-1)^{-U} \tag{18}$$

따라서 $u\ge MAX\{n-1,(q-1)/q(n-1)-1\}$에 대하여 D_u는 다음과 같이 근사화될 수 있다.

$$D_u\approx q^{-(n-k)}\binom{n}{u}(q-1)^u Vn(t) \tag{19}$$

Ⅲ. 컴퓨터 시뮬레이션과 고찰

(31,15,8) RS부호에 복호가능어의 명시적 값 D_u를 구하기 위하여 식(16)을 적용하고, 근사값 D_u를 구하기 위하여 식(19)를 적용한 결과는 그림1과 같다. 그림에서 가중치 u가 n에 접근할때 D_u와 D_u'는 그 값이 일치해 가는데, 특히 u가 17이후에는 명시적 값과 근사값이 일치함을 알수 있다. 또한 가중치 u가 부호의 길이 n에 접근할때 10^{41}값으로 일치함을 나타내고 있다.

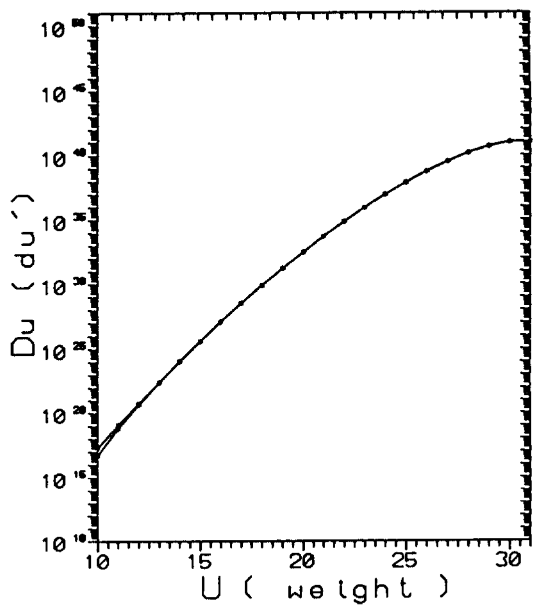

그림 1. (31,15,8) Reed-Solomon 부호의 D_u와 근사값
Figure 1. D_u and its approximation for the (31,15,8)

표1은 GF(2^5)상에서 (31,15,8)RS부호의 상한값 분포를 나타내며, 표2는 GF(2^5)상에서 (31,21,5)RS 부호에 대한 가중치분포를 나타내고있다. $D=n-k+1$에서 d값이 11이므로 11에서 31까지의 u값에 대하여 A_u값을 구할수 있다.

가중치 분포는 가중치가 부호의 길이 n에 접근함에 따라 증가함을 알수 있으며, 특히 가중치 분포에 식(2)의 Vn(t)값을 곱한 결과는 부호가능어 D_u와 일치함을 확인할수 있다.

식(19)을 식(6)에 대입하여 간단히 하면 $P_E(u)=q^{-(n-k)}Vn(t)$로 되는데 이는 상수값이 되어 가중

표 1. (31,15,8) RS부호에 대한 상한
Table 1. Upper bound on R for the (31,15,8) RS code.

u	R
16	4.399091E-23
17	1.206202E-23
18	2.334586E-24
19	3.577187E-25
20	4.615726E-26
21	5.211303E-27
22	5.283348E-28
23	4.89988E-29
24	4.21495E-30
25	3.399153E-31
26	9.082061E-32
27	2.043463E-33
28	4.401307E-34
29	9.116988E-35
30	1.823398E-37
31	1.823398E-38

치 u에 관계없이 복호기 오류확률이 일치함을 알수 있다. 또한 그 값은 서론에서 제시했던 Q* 값과 일치함을 알수 있다.

표2의 상한값은 t개의 오류정정가능 부호에서 그 값이 1/t!보다 작음을 나타내고 있다.

표 2. (31,21,5) RS부호에 대한 가중치 분포
Table 2. Weight distribution for the (31,21,5) RS code.

u	A(u)
11	2.624841E+09
12	9.624419E+10
13	4.654719E+12
14	1.840943E-14
15	6.472856E+15
16	2.006449E+17
17	5.488258E+18
18	1.323279E+20
19	2.806746E+21
20	5.220545E+22
21	8.477173E+23
22	1.194511E+25
23	1.448993E+26
24	1.497294E+27
25	1.299652E+28
26	9.297492E+28
27	5.337457E+29
28	2.363727E+30
29	7.580243E+30
30	1.566581E+31
31	1.566583E+31

표 3. n이 7,15,31인 경우 RS부호의 Q, Q', Q*
Table 3. Q, Q', Q* values of the RS codes on n=7,15,31

(n,k,t)	McEliece의 Q값	K.M.Cheung의 Q' 값	본 논문의 Q* 값	복호기오류확률 PE(u)
(7,5,1)	0.7812261	0.7804081	0.78125	0.78125
(7,3,2)	0.2629132	0.449396	0.2634277	0.2634277
(7,1,3)	0.0436725	0.1112121	0.0499115	0.0499115
(15,7,4)	1.645242E-02	2.757145E-02	1.645242E-02	1.645242E-02
(15,5,5)	2.13828E-03	4.077108E-03	2.138282E-03	7.138282E-03
(15,7,5)	0.5474003	0.9173493	0.5474003	0.5474003
(31,17,7)	6.18375E-05	9.644682E-05	6.18375E-05	6.18375E-05
(31,15,8)	5.625843E-06	9.349755E-06	5.625843E-06	5.625843E-06
(31,15,9)	4.465336E-04	7.421074E-04	4.465336E-04	4.465336E-04
(31,15,10)	3.051664E-02	5.071617E-02	3.051644E-02	3.051644E-02

표3은 (7,5,1), (7,3,2), (7,1,3)RS보호와 (15,7,4), (15,5,5), (15,7,5)RS부호, 그리고 (31,17,7),(31,15,8),(31,15,9),(31,15,10)RS부호에 대하여 식(1)의 Q, 식(3)의 Q', 식(5)의 Q*, 그리고 복호기 오류확률 $P_E(u)$를 구한 결과를 나타내고 있다. 표3에서 복호

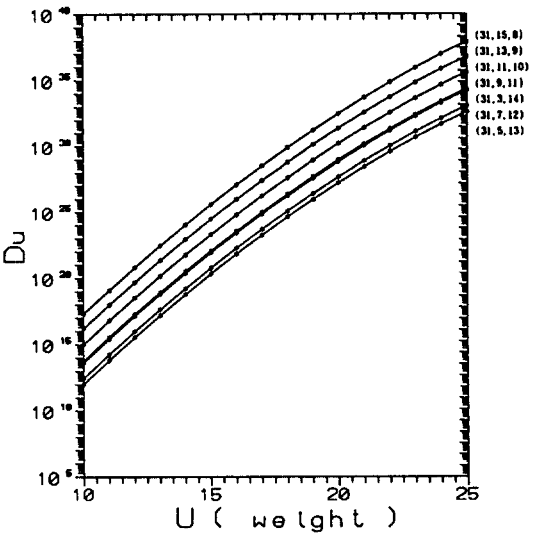

그림 2. n=31일때 RS부호에 대한 복호가능어의 근사값.
Figure 2. Approximaion values of th decodable words for the RS codes on n=31.

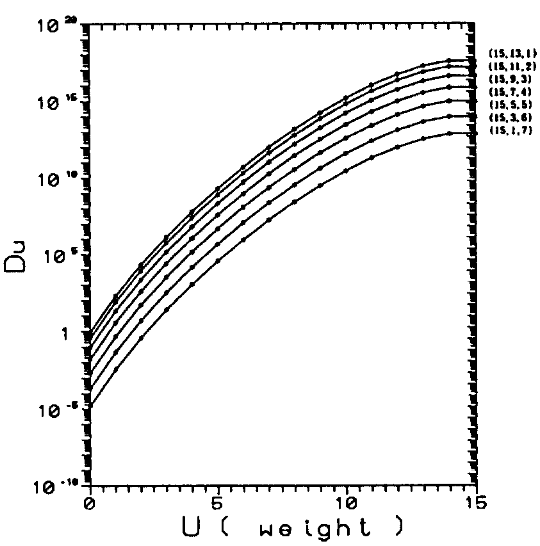

그림 3. n=15일때 RS부호에 대한 복호가능어의 근사값
Figure 3. Approximation values of jthe decodable words for the RS codes on n=15.

기 오류확률은 McEliece가 제안했던 Q값이나 K.M. Cheung이 제안했던 Q'값에 근접하고 있으나, 본 논문에서 제시한 식 Q",와는 일치된 결과를 나타내고 있다.

그림 2는 n=31일때 (k,t)가 (15,8),(13,9),(11,10),(9,11),(7,12),(5,13),(3,14)인 RS부호에 대한 복호가능어 근사값의 분포를 나타내고 있다. 그림에서 가중치 u가 커질수록 D_u'값은 지수함수적으로 증가함을 알수있다.

그림3은 n=15일때 (k,t)가 (13,1),(11,2),(9,3),(7,4)(5,5),(3,6),(1,7)인 RS부호에 대한 복호가능어 근사값의 분포를 나타내고 있으며, u값이 n에 접근할수록 특정한 값으로 수렴함을 알수 있다.

Ⅳ. 결 론

본 논문에서는 복호가능어 분포 D_u와 근사분포 D_u'를 구하였으며, 이를 (n,k,t)RS부호의 가중치 분포에 대한 복호기 오류확률 $P_E(u)$에 적용하였다. 그 타당성을 확인하기 위하여 n,k,t가 (7,5,1),(7,3,2),(7,1,3)인 경우와 (15,7,5),(15,7,4),(15,5,5), 그리고 (31,17,7),(31,15,8),(31,15,9),(31,15,9),(31,15,10) 등의 RS부호에 컴퓨터시뮬레이션을 수행하였다. 그 결과 가중치 u가 커질때 복호기 오류확률 $P_E(u)$값이 완전확률오류형태 확률인 Q값과 Q'값에 접근하고, 본 논문에서 제안한 Q*값에는 일치함을 확인하였다. 그리고 정정가능한 오류의 수가 t 일때 복호기 오류확률은 1/t!보다 작음을 확인하였으며, 가중치 분포 A(u)에 Vn(t)값을 곱하면 복호 가능어 D_u와 일치함도 보였다.

또한, 가중치가 u인 복호가능어 D_u와 D_u'는 u가 증가할수록 서로 일하며, u가 부호의 길이 n에 접근했을때 그 값은 특정한 값에 접근함과 복호가능어의 접근도에 따라 복호기 오류확률 Pe(u)와 Pe(u')의 접근도가 일치해감을 알수 있었으며, P_E(u')값은 가중치 u에는 관계없이 항상 일정한 상수 값을 가짐도 확인하였다.

참 고 문 헌

1. Robert J.McEliece, Laif Swanson, "On the Decoder

Error Probability for Reed-Solomon Codes," IEEE Trans. on information Theory, VOL. 32, NO.5, PP. 701-703 1986.

2. Kar-Ming Cheung, "More on the Decoder Error Probability for Reed-Solomon Codes," IEEE Trans. on Information Theory, VOL. 35, NO.5, PP.895-900, 1989.
3. Kar-Ming Cheung, "Identities and Approximations for the Weight Distribution of q-ary Codes," IEEE Trans. on Information Theory, VOL. 36, NO.5, PP. 1149-1153, 1990.
4. Kar-Ming Cheung, "On the Decoder Error Probability of Block Codes," IEEE Trans. on Information Theory, VOL. 40, NO.5, pp.857-859, 1992.
5. Tadao Kasami, Shu Lin, "On the Probability of undetcted Error for the Maximum Distance Seperable Codes," IEEE Trans. on COMM., VOL. 32, NO.9, PP.998-1006, 1984.
6. Man Young Rhee, "Error Correcting Coding Theory," McGraw-Hill Publishing Co.1989.
7. T. Kasami, S. Lin, and W. W. Peterson, "Some results on weight distribution of BCH codes," IEEE Trans. Inform. Theory, VOL. IT-12, PP.274, 1966.
8. Richard E. Blahut, "Theory and Practice of Error Control Codes," Addison-Wesley Publishing Company, 1983.

▲정 제 홍

1955년 11월 16일생

1978년 2월 : 공주사범대학 수학과(이학사)

1984년 8월 : 한양대학교 전자계산학과(공학석사)

1993년 2월 : 청주대학교 전자공학과(공학박사)

1984년 9월~1993년 2월 : 혜전전문대학 전자계산학과

1993년 3월~현재 : 건양대학교 전자계산학과 조교수

▲박 진 수

1948년 8월 30일생

1975년 2월 : 한양대학교 전자공학과(공학사)

1977년 2월 : 한양대학교 전자공학과(공학석사)

1985년 2월 : 한양대학교 전자공학과(공학박사)

1987년 1월~1988년 1월 : Uni. of Colorado at Colorado spring(Post Doc.)

1987년 3월~현재 : 청주대학교 전자공학과 교수