논문 99-24-1A-4 한국통신학회논문지 '99-1 Vol.24 No.1A

Z_4위의 Newton 항등식과 Goethals 부호에의 응용

정회원 임 두 루*, 양 경 철**

Newton'S Identity Over Z_4 And Its Application To Decoding Of Goethals Codes

Dooroo Lim*, Kyeongcheol Yang** *Regular Member*

요 약

길이가 2^m인 Z_4위의 Goethals 부호는 $2^{2^{m+1}-3m-2}$개의 부호어를 가지는 Z_4위의 선형부호로서 m이 홀수인 경우 최소 거리가 8이다. 본 논문에서는 Galois 환에서 Newton 항등식이 존재함을 보이고, 이를 이용하여 Z_4위의 Goethals 부호의 복호 알고리즘을 제시한다.

ABSTRACT

The Goethals code over Z_4 of length 2^m is a linear code over Z_4 with $2^{2^{m+1}-3m-2}$ codewords and minimum distance 8 for odd integer m. In this paper Newton's identity over Galois Rings is derived. A decoding algorithm for Goethals code over Z_4 is also presented using Newton's identity.

I. 서 론

지금까지 비선형부호는 복호방법의 복잡성 등의 이유로 구현이 어려웠다. 그러나 Hammons, Kumar, Calderbank, Sloane과 Solé는 Nordstrom-Robinson 부호, Kerdock 부호, Preparata 부호, Goethals 부호와 Delsarte-Goethals 부호 등이 Z_4위에서 적절히 정의하면 선형부호가 된다는 것을 증명하였다[1]. 이들 부호들은 주어진 길이(code length)와 최소거리(minimum distance)에 대해 지금까지 알려진 어떠한 이진선형부호(binary linear code)보다 더 많은 부호어를 가지는 비선형부호(nonlinear code)이다. 예를 들어 Goethals 부호는 확장된 삼중오류정정(extended triple-error-correcting) BCH 부호보다 네 배의 부호어를 가진다.

최적의 비선형부호들이 Z_4위의 선형부호로 변환됨으로써 선형성으로 인한 복호방법의 간략화가 가능하게 되었으며, 이에 대한 연구가 진행되고 있다. Hammons 등은 Z_4위의 Preparata 부호에 관한 복호 알고리즘을 발표하였으며[1], Helleseth와 Kumar는 Z_4위의 Goethals 부호에 대한 복호 알고리즘을 제시하였다[2]. 특히 Rong과 Helleseth는 Gröbner 기저(Gröbner basis)를 이용한 Z_4위의 Calderbank-McGuire 부호의 복호 알고리즘을 발표하였으며, 이는 Z_4위의 Preparata 부호와 Goethals 부호에도 적용할 수 있다[3].

본 논문에서는 유한체(finite fields)뿐만 아니라 Galois 환(Galois rings)에서도 Newton 항등식(Newton's identity)이 존재함을 보이며, 이를 이용하여 Z_4위의 Goethals 부호의 복호 알고리즘을 제시한다.

---

* 현대전자 통신연구 9실 근무(dooroo@hei.co.kr)
논문번호 : 98007-0106, 접수일자 : 1998년 1월 6일
※이 논문은 한국과학재단 핵심전문연구 961-0923-129-2에 의한 결과임.

Ⅱ. Z_4위의 Goethals 부호

이진선형부호를 유한체(finite fields 또는 Galois fields)에서 다루듯이 Z_4위의 선형부호에 대한 접근은 Galois 환(Galois rings)에서 이루어진다.

$R_m=$ GR (4^m)을 지표(characteristic)가 4이고, 4^m개의 원소를 가지는 Galois 환이라 하자. R_m^*를 R_m에서 곱셈에 대한 역원을 가지는 원소들의 집합이라 할 때, R_m^*에는 차수가 2^m-1인 원소 β가 존재한다. T_m을 $T_m=\{0,1,\beta,\beta^2,\cdots,\beta^{2^m-2}\}$로 정의하면, R_m에 속하는 임의의 원소 γ를 아래와 같이 유일하게 표현 할 수 있다 :

$$\gamma=A+2B,\quad A,B\in T_m.$$

μ를 모듈로(modulo) 2로 취하는 축약사상(reduction map)이라 하고, $\mu(\beta)=\alpha$라 하면, $\mu(T_m)=\{0,1,\alpha,\alpha^2,\cdots,\alpha^{2^m-2}\}$는 유한체 GF (2^m)이 된다[1], [4].

부호길이가 n인 Z_4위의 선형부호 C는 가산군(additive subgroup) Z_4^n의 부분군(subgroup)으로 정의된다. Z_4위의 선형부호의 성능을 결정하는 가장 중요한 요소중 하나는 최소 Lee 무게(minimum Lee weight)이다. Z_4에 속하는 $0,1,2$와 3의 Lee 무게는 각각 $0,1,2,1$이 되고, Z_4^n에 속하는 벡터 $\mathbf{a}=(a_1,a_2,\cdots,a_n)$의 Lee 무게는 각 원소의 Lee 무게들의 합이 된다.

부호길이가 2^m인 Z_4위의 Goethals 부호 G_m은 $2^{2^{m+1}-3m-2}$개의 부호어를 가지고, m인 경우 최소 Lee 거리가 8인 부호로서 아래의 행렬을 검사행렬로 가진다:

$$H=\begin{bmatrix}1 & 1 & 1 & 1 & \cdots & 1\\ 0 & 1 & \beta & \beta^2 & \cdots & \beta^{2^m-2}\\ 0 & 2 & 2\beta^3 & 2\beta^6 & \cdots & 2\beta^{3(2^m-2)}\end{bmatrix}.$$

보조정리 1 ([1],[5]) Z_4위의 Goethals 부호는 아래의 비선형 순열변환들로 구성된 이중추이군(doubly transitive group)에 대해 불변의 성질을 갖는다:

$$X\rightarrow(AX+B)^{2^m}.$$

여기서 $A,B\in T_m$이고 $A\neq 0$이다.

보조정리 2 ([2]) Z_4위의 벡터 $\mathbf{e}=(e_X)_{X\in T_m}$가 주어질 때 $j=0,1,2,3$에 대해 $E_j=\{X\mid e_X=j\}$라 하면, 다음의 식

$$\sum_{X\in T_m}e_XX=A+2B,\quad A,B\in T_m,\ e_X\in Z_4$$

은 아래의 두 식과 등가이다:

$$a=\sum_{X\in E_1\cup E_3}x,$$
$$b^2=\sum_{X\in E_2\cup E_3}x^2+\sum_{\substack{X,Y\in E_1\cup E_3\\ X<Y}}xy.$$

여기서 a,b,x와 y는 각각 $\mu(A),\mu(B),\mu(X)$와 $\mu(Y)$를 의미하며, '$<$'는 T_m의 원소들에 대한 임의의 순서(ordering)를 뜻한다.

위의 보조정리를 이용하여 R_m위에서 정의된 하나의 식을 GF (2^m)위에서 정의된 두 개의 식으로 변환할 수 있다.

Ⅲ. Galois 환에서 정의되는 Newton 항등식

T_m^*을 $T_m^*=T_m\setminus\{0\}$라 하고, C를 Z_4위의 선형부호로서 길이가 2^m-1인 순회부호라 하자. $\mathbf{r}=(r_X)_{X\in T_m^*}$를 수신벡터라 하고, $\mathbf{e}=(e_X)_{X\in T_m^*}$를 오류벡터라 하면, 수신벡터의 오증 $S_j=A_j+2B_j$와 $2S_j=2A_j$는 다음과 같이 정의된다:

$$S_j=\sum_{X\in T_m^*}e_X\cdot X^j,\quad 2S_j=2\sum_{X\in T_m^*}e_XX^j.$$

Z_4위의 선형부호는 비이진 부호이므로 오류위치뿐만 아니라 그 위치에서의 오류값도 구해야 한다. ν개의 오류가 다음과 같이 발생했다고 가정하자:

오류값 : $e_{X_1},e_{X_2},\cdots,e_{X_\nu}$, 오류위치 : $X_1,X_2,\cdots,X_\nu$.

여기서 $e_{X_i}\in Z_4$이고 $X_i\in T_m^*$이다. 수신벡터 $\mathbf{r}$의 오류위치 다항식(error locator polynomial) $\sigma(z)$는 오류위치에 대한 정보를 가지는 다항식으로

$$\sigma(z)=\prod_{i=1}^{\nu}(1-zX_i)=\sigma_0+\sigma_1z+\cdots+\sigma_\nu z^\nu \quad (1)$$

와 같이 정의된다. 이 때 오류위치 다항식의 계수들을 X_i로 나타내면, 아래와 같이 기초대칭함수

(elementary symmetric function)로 표현된다[6]:

$$\sigma_0 = 1,$$
$$\sigma_1 = -(X_1 + X_2 + \cdots + X_\nu),$$
$$\vdots \qquad \vdots$$
$$\sigma_\nu = (-1)^\nu (X_1 X_2 \cdots X_\nu).$$

정리 3 모든 양의정수 j에 대해 S_j는 다음의 관계를 만족한다:

$$S_{j+\nu} + \sigma_1 S_{j+\nu-1} + \cdots + \sigma_\nu S_j = 0.$$

(증명) 식 (1)의 양변에 $e_{X_i} X_i^{j+\nu}$를 곱하면 식 (1)은

$$e_{X_i} X_i^{j+\nu} \sigma(z) = e_{X_i} X_i^{j+\nu} + \cdots + e_{X_i} X_i^{j+\nu} \sigma_\nu z^\nu \quad (2)$$

와 같다. $X_i \in T_m^*$은 곱셈에 대한 역원을 가지므로, $z = X_i^{-1}$을 대입하면 식 (2)의 좌변은 0이 된다:

$$0 = e_{X_i} X_i^{j+\nu} + e_{X_i} X_i^{j+\nu-1} \sigma_1 + \cdots + e_{X_i} X_i^j \sigma_\nu .$$

$i = 1, 2, \cdots, \nu$에 대해 각 항을 더해주면 $\sigma(z)$와 오증과의 관계는

$$\left(\sum_{i=1}^{\nu} e_{X_i} X_i^{j+\nu}\right) + \cdots + \sigma_\nu \left(\sum_{i=1}^{\nu} e_{X_i} X_i^j\right)$$
$$= \left(\sum_{X \in T} e_X X^{j+\nu}\right) + \cdots + \sigma_\nu \left(\sum_{X \in T} e_X X^j\right)$$
$$= S_{j+\nu} + \cdots + \sigma_\nu S_j = 0$$

와 같다.

길이가 2^m인 Z_4위의 확장된 순회부호의 경우, 부호어의 성분에 대한 첨자로 T_m을 사용하면, 0의 위치에서도 오류가 발생할 수 있다. 0은 곱셈에 대한 역원이 존재하지 않으므로 Newton 항등식으로는 이 위치에서 발생한 오류를 검출할 수 없다. 그러나 0의 위치에서 발생한 오류는 오증에 아무런 영향을 주지 못하므로, 이후로는 0의 위치를 포함하여 아래와 같이 오증을 정의한다:

$$S_j = \sum_{X \in T_m} e_X \cdot X^j, \quad 2 S_j = 2 \sum_{X \in T_m} e_X X^j.$$

0의 위치에서의 오류의 발생여부는 전체의 패리티를 검사하는 성분과 오증을 이용하여 결정한다.

본 논문에서 영문자 대문자는 T_m의 원소를 의미하고, 소문자는 그 원소에 대해 축약사상을 취한 값으로서 GF(2^m)의 원소를 가리킨다. 즉 $a_j = \mu(A_j)$이고 $b_j = \mu(B_j)$이다. 또한 오류위치다항식의 계수를 $\sigma_j = A_j' + 2B_j'$라 할 때, α_j와 β_j는 각각 $\mu(A_j')$와 $\mu(B_j')$를 가리킨다.

Ⅳ. Newton 항등식을 이용한 Z_4위의 Goethals 부호의 복호방법

본 논문에서 전체적인 복호과정은 다음과 같이 이루어진다. 먼저 검사행렬을 이용하여 오증을 구한 후, 오증으로부터 Newton 항등식을 이용하여 오류값이 '1' 또는 '3'인 오류의 위치를 구한다. 그 후 오류값이 '2'인 오류의 위치와 각 위치에서의 오류값을 추정한다.

수신벡터의 오증을 S라 하면 S는

$$S = rH^T = eH^T = (s, A_1 + 2B_1, 2A_3)$$

와 같이 주어지며, 각 원소는 다음과 같다. 여기서 H^T은 검사행렬 H의 전치행렬이다:

$$\sum_{X \in T_m} e_X = s, \quad s \in Z_4$$
$$\sum_{X \in T_m} e_X X = A_1 + 2B_1, \quad A_1, B_1 \in T_m$$
$$2 \sum_{X \in T_m} e_X X^3 = 2A_3, \quad A_3 \in T_m.$$

본 논문에서는 s에 따라 복호과정을 구분하여 설명한다. 그리고 편의상 오류벡터에서 오류값이 '1' 또는 '3'인 오류의 개수를 η로 정의한다.

4.1 $s=0$인 경우

보조정리 4 $a_1 = 0$이면 $\eta = 0$이다.

(증명) $\eta = 2$라 가정하자. e_X와 e_Y는 1또는 3이므로 $a_1 = x + y$이다. x와 y는 서로 다르므로 $a_1 = x + y \neq 0$이다.

정리 5 $a_1 \neq 0$이면 $\gamma_1 = a_1$이라 하고 $\gamma_2 = a_3/a_1 + a_1^2$이라 하자. $u^2 + \gamma_1 u + \gamma_2 = 0$이 서로 다른 두 근을 가지고, 두 근중 하나가 $(b_1^2 + \gamma_2)^{1/2}$와 같으면 오류벡터는 $e = X + 3Y$이다. 이 때 $y = (b_1^2 + \gamma_2)^{1/2}$이고 $x = a_1 + y$이다.

(증명) 오류벡터가 $e=X+3Y$라 가정하면, 오증식 (syndrome equation)은 아래와 같이 주어지며

$$X+3Y=A_1+2B_1,\quad 2X^3+2Y^3=2A_3$$

보조정리 2에 의해 이는 아래의 식과 등가이다:

$$a_1 = x+y,\quad b_1^2 = y^2+xy,\quad a_3 = x^3+y^3. \quad (3)$$

x와 y는 서로 다르므로 $a_1 \neq 0$이다. 오류벡터의 해밍무게가 2이므로, 오증은 Newton 항등식 $S_3+\sigma_1 S_2+\sigma_2 S_1=0$을 만족하며 보조정리 2에 의해 아래의 수식이 성립한다:

$$a_3+\alpha_1 a_2+\alpha_2 a_1=0.$$

$\gamma_1=a_1=\alpha_1$이고 $\gamma_2=a_3/a_1+a_1^2=\alpha_2$이므로, x와 y는 $u^2+\gamma_1 u+\gamma_2=0$의 근이다. 그리고 식 (3)으로부터 $y=(b_1^2+\gamma_2)^{1/2}$이고 $x=a_1+y$이다.

$s=0$인 경우 Goethals 부호의 복호 알고리즘을 흐름도로 나타내면 그림 1과 같다. 여기서 Tr는 $GF(2^m)$에서 $GF(2)$로의 트레이스(trace) 함수를 의미한다.

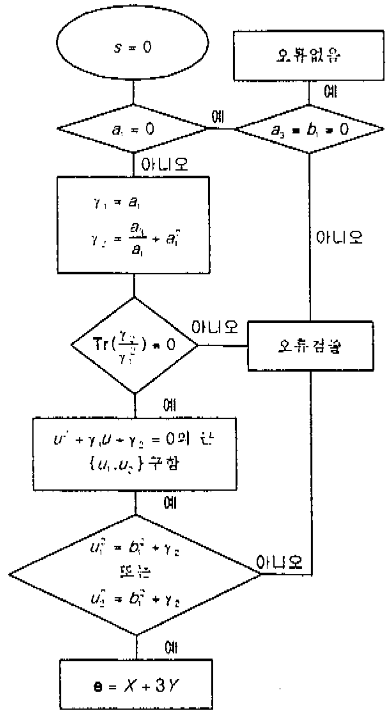

그림 1. $s=0$인 경우 복호 알고리즘의 흐름도

4.2 $s=1$인 경우

보조정리 6 $a_3=a_1^3$이면 $\eta=1$이다.

(증명) $\eta=3$이라 가정하고 $a_1=x+y+z$, $a_3=x^3+y^3+z^3$이라 하자. $a_3=a_1^3$이면

$$\begin{aligned} a_1^3+a_3 &= (x+y+z)^3+x^3+y^3+z^3 \\ &= x^2(y+z)+y^2(x+z)+z^2(x+y) = 0 \end{aligned}$$

이다. 보조정리 1로부터 일반성을 잃지 않고 $y=1$, $z=0$으로 놓을 수 있다. 그러면 $a_1^3+a_3=x^2+x=x(x+1)$이고, x, y와 z는 서로 다르므로 $x\neq 0$이고 $x\neq 1$이다. 따라서 $a_1^3+a_3\neq 0$, 즉 $a_1^3\neq a_3$이다.

보조정리 6으로부터 주어진 오증이 $a_1^3+a_3=0$을 만족하면, 오류벡터를 $e=X$ 또는 $e=3X+2Y$로 가정할 수 있다.

정리 7 오증이 $a_1^3+a_3=0$을 만족한다고 하자.

i) $b_1=0$이면 오류벡터는 $e=X$이다. 이 때 $x=a_1$이다.

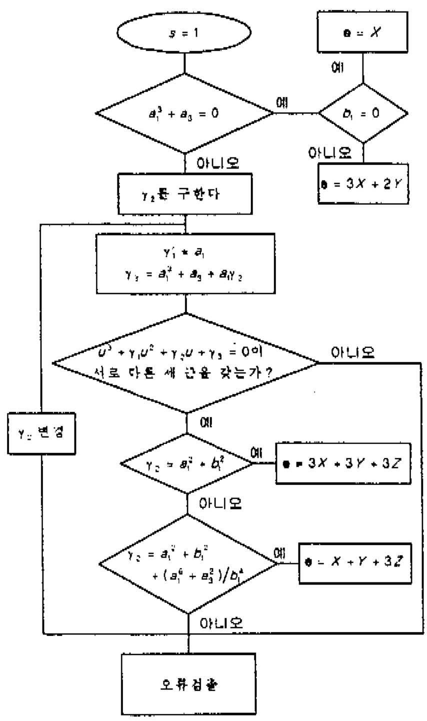

그림 2. $s=1$인 경우 복호 알고리즘의 흐름도

ii) $b_1\neq 0$이면 오류벡터는 $e=3X+2Y$이다. 이

때 $x=a_1$이고 $y=b_1+a_1$이다.

(증명) i) 오류벡터가 $e=X$라 가정하면 오증은 다음과 같다 :

$$a_1 = x, \quad b_1 = 0, \quad a_3 = x^3.$$

오증으로부터 $a_1^3+a_3=0$이고 $b_1=0$이다. 이 때 $x=a_1$이다.

ii) 오류벡터가 $e=3X+2Y$라 하면 오증은 다음과 같다:

$$a_1 = x, \quad b_1^2 = x^2+y^2, \quad a_3 = x^3.$$

오증으로부터 $a_1^3+a_3=0$이고 x와 y는 서로 다르므로 $b_1\neq 0$이다. 이 때 $x=a_1$이고 $y=a_1+b_1$이다.

보조정리 6에 의해 $a_1^3+a_3\neq 0$이면 $\eta=3$이라 할 수 있다. $\eta=3$인 경우 오류벡터의 성분은 '1' 또는 '3'으로만 이루어져 있다. 즉, 오류값이 '2'인 오류가 발생하지 않으므로, α_1, α_2와 α_3는 다음과 같은 관계를 가진다 :

$$\alpha_1=a_1, \quad \alpha_2, \quad \alpha_3=a_3+\alpha_1 a_2+\alpha_2 a_1. \qquad (4)$$

이 때 β_1, β_2와 β_3는

$$\beta_1^2=\alpha_1^2+\alpha_2, \quad \beta_2^2=\alpha_1\alpha_3, \quad \beta_3^2=\alpha_3^2 \qquad (5)$$

와 같이 주어진다. 따라서 α_2를 알면 오류위치를 알 수 있다.

보조정리 8 $\eta=3$이라 하자. $a_1=\alpha_1=0$이면 α_2는 다음 이차방정식의 근이다:

$$b_1^4u^2+a_3^2u+a_3^2b_1^2+b_1^8=0. \qquad (6)$$

(증명) 오류벡터의 해밍무게가 3이므로 $S_4+\sigma_1S_3+\sigma_2S_2+\sigma_3S_1=0$이 성립한다. 이는 보조정리 2에 의해 아래와 같이 유한체에서 정의된 두 식으로 변환되며

$$a_4+\alpha_1a_3+\alpha_2a_2+\alpha_3a_1 = 0,$$

$$\begin{aligned} & b_4^2+\alpha_1^2b_3^2+\alpha_2^2b_2^2+\alpha_3^2b_1^2+\beta_1^2a_3^2+\beta_2^2a_2^2+\beta_3^2a_1^2 \\ & +\alpha_1a_3a_4+\alpha_2a_2a_4+\alpha_3a_1a_4+\alpha_1\alpha_2a_2a_3 \\ & +\alpha_1\alpha_3a_1a_3+\alpha_2\alpha_3a_1 = 0 \end{aligned}$$

식 (4)와 (5)를 이용하면 아래의 식이 성립한다:

$$b_1^4\alpha_2^2+a_3^2\alpha_2+a_3^2b_1^2+b_1^8 = 0. \qquad (7)$$

보조정리 9 $\eta=3$이라 하자. $a_1\neq 0$이면 α_2는 아래의 사차방정식의 근이다:

$$\begin{aligned} & u^4(a_1^4b_1^4+b_1^8)+u^3(a_1^{10}+a_1^4a_3^2) \\ & +u^2(a_1^{10}b_1^2+a_1^4b_1^8+a_1^6a_3^2+a_1^4b_1^2a_3^2+a_1^2b_1^4a_3^2+a_3^4) \\ & +u(a_1^{14}+a_1^2a_3^4)+a_1^{14}b_1^2+b_1^{16}+a_1^6b_1^4a_3^2+a_1^2b_1^8a_3^2 \\ & +a_1^2b_1^2a_3^4+b_1^4a_3^4 = 0. \end{aligned} \qquad (8)$$

(증명) 오증은 $S_4+\sigma_1S_3+\sigma_2S_2+\sigma_3S_1=0$을 만족하므로, b_3^2은 아래와 같이 주어지며

$$\begin{aligned} b_3^2=\frac{1}{a_1^2}\{ & \alpha_2^2(a_1^2b_1^2+b_1^4)+\alpha_2(a_1^3a_3+a_3^2) \\ & +a_1^8+a_1^6b_1^2+a_1^2a_3^2+a_3^2b_1^2+b_1^8\} \end{aligned}$$

이를 이용하면 b_5^2은 다음과 같다:

$$\begin{aligned} b_5^2 = {} & \alpha_2^2b_3^2+\alpha_2^2(a_1^3a_3+a_1^2b_1^4+a_3^2) \\ & +a_1^{10}+a_1^7a_3+a_1^6b_1^4+a_1^4a_3^2+a_1^2b_1^8+a_1a_3^3+a_3^2b_1^4. \end{aligned}$$

b_3^2과 b_5^2을 $S_6+\sigma_1S_5+\sigma_2S_4+\sigma_3S_3=0$에 대입하고 정리하면

$$\begin{aligned} & \alpha_2^4(a_1^4b_1^4+b_1^8)+\alpha_2^3(a_1^{10}+a_1^4a_3^2) \\ & +\alpha_2^2(a_1^{10}b_1^2+a_1^4b_1^8+a_1^6a_3^2+a_1^4b_1^2a_3^2+a_1^2b_1^4a_3^2+a_3^4) \\ & +\alpha_2(a_1^{14}+a_1^2a_3^4)+a_1^{14}b_1^2+b_1^{16}+a_1^6b_1^4a_3^2+a_1^2b_1^8a_3^2+a_1^2b_1^2a_3^4+b_1^4a_3^4= \end{aligned}$$

이 성립한다.

정리 10 오류벡터의 오증이 $a_1^3+a_3\neq 0$이면, a_1에 따라 식 (6) 또는 (7)의 근을 γ_2라 하고, γ_1과 γ_3를 각각 $\gamma_1=a_1$와 $\gamma_3=a_3+a_1^3+a_1\gamma_2$와 같이 정의하며, $u^3+\gamma_1u^2+\gamma_2u+\gamma_3=0$이 서로 다른 세 근을 가진다고 하자.

i) $\gamma_2=a_1^2+b_1^2+(a_1^6+a_3^2)/b_1^4$이면 $e=X+Y+3Z$이다. 이 때 $z=a_1+(a_1^3+a_3)/b_1^2$이고, x와 y는 삼차방정식의 나머지 두 근이다.

ii) $\gamma_2=a_1^2+b_1^2$이면 $e=3X+3Y+3Z$ 이고, x, y와 z는 삼차방정식의 세 근이다.

(증명) i) 오류벡터가 $e=X+Y+3Z$라 하면 오증

은 아래와 같다:

$$a_1 = x+y+z,\quad b_1^2 = z^2+xy+xz+yz,\quad a_3 = x^3+y^3+z^3.$$

오증으로부터 $z = a_1 + (a_1^3+a_3)/b_1^2$이므로 a_2는

$$a_2 = xy+xz+yz = a_1^2+b_1^2+(a_1^6+a_3^2)/b_1^4$$

와 같이 주어진다.

ii) 오류벡터가 $e=3X+3Y+3Z$ 라 하면 오증은 $a_1 = x+y+z$, $a_3 = x^3+y^3+z^3$, $b_1^2 = x^2+y^2+z^2+xy+xz+yz$ 와 같이 주어지고, $a_2 = a_1^2+b_1^2$이다. 이 때 $a_1^3+a_3 \neq 0$이므로 보조정리 8 또는 9로부터 구한 γ_2는 i)과 ii)의 조건을 동시에 만족하지 못한다. □

$s=1$인 경우 Goethals 부호의 복호 알고리즘을 흐름도로 나타내면 그림 2와 같다.

4.1.3 $s=2$인 경우

$s=2$인 경우 전체적인 복호과정은 $s=0$과 유사하며, 단지 주어진 오류위치에 대한 오류값을 구하는 과정이 다르다.

정리 11 $a_1 \neq 0$이면 $\gamma_1 = a_1$이라 하고 $\gamma_2 = a_3/a_1 + a_1^2$이라 하자.

i) $a_1 = a_3 = 0$이면, $e=2X$ 이고 $x=b_1$이다.

ii) $a_1 \neq 0$이고 $u^2+\gamma_1 u+\gamma_2=0$이 서로 다른 두 근을 가지며, $b_1^2=\gamma_2$이면, $e=X+Y$ 이고 x와 y는 이차방정식의 근이다.

iii) $a_1 \neq 0$이고 $u^2+\gamma_1 u+\gamma_2=0$이 서로 다른 두 근을 가지며, $b_1^2 = a_1^2+\gamma_2$이면, $e=3X+3Y$이고 x와 y는 이차방정식의 근이다.

(증명) i) 오류벡터가 $e=2X$ 라 할 때 오증은 $a_1 = a_3 = 0$,

$b_1 = x$와 같고 이로부터 증명은 쉽게 유도된다.

ii) 오류벡터가 $e=X+Y$ 라 하면 오증은 아래와 같다:

$$a_1 = x+y,\quad b_1^2 = xy,\quad a_3 = x^3+y^3.$$

이 때 $\gamma_1 = a_1 = \alpha_1$이고 $\gamma_2 = a_3/a_1 + a_1^2 = \alpha_2$이므로, x와 y는 $u^2+\gamma_1 u+\gamma_2=0$의 근이고 $b_1^2=\gamma_2$이다.

iii) 오류벡터가 $e=3X+3Y$라 하면 오증은 아래와 같다 :

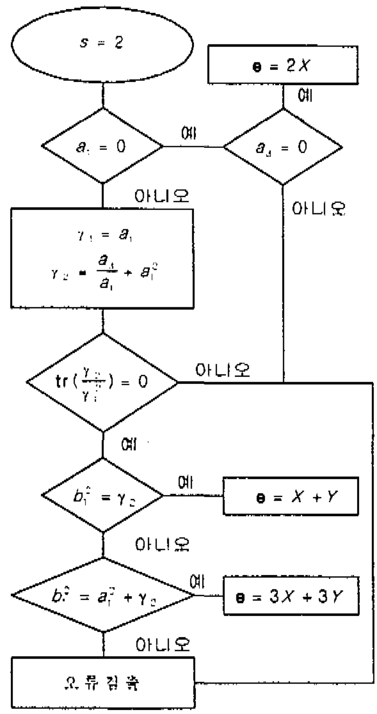

그림 3. $s=2$인 경우 복호 알고리즘의 흐름도

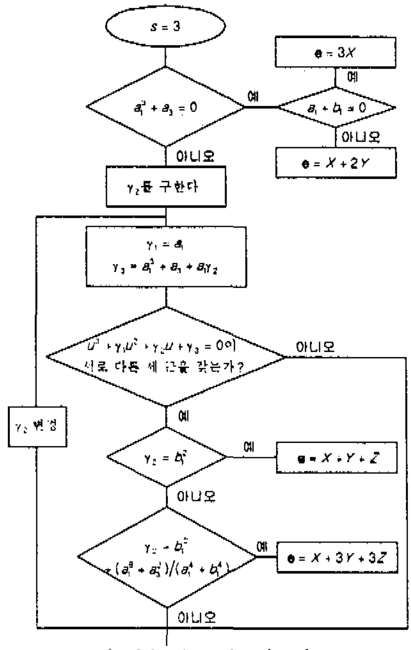

그림 4. $s=3$인 경우 복호 알고리즘의 흐름도

$$a_1 = x+y,\quad b_1^2 = x^2+y^2+xy,\quad a_3 = x^3+y^3.$$

이 때 $\gamma_1 = a_1 = \alpha_1$이고 $\gamma_2 = a_3/a_1 + a_1^2 = \alpha_2$이므로, x와 y는 $u^2+\gamma_1 u+\gamma_2=0$의 근이고 $b_1^2 = a_1^2+\gamma_2$이

다.

$s=2$인 경우 Goethals 부호의 복호 알고리즘을 흐름도로 나타내면 그림 3과 같다.

4.4 $s=3$인 경우

$s=3$인 경우의 오증을 $S=(3, A_1+2B_1, 2A_3)$라 할 때 S와 $s=1$의 오증사이의 관계는

$$-S=(-3, -(A_1+2B_1), -2A_3)$$
$$=(1, A_1+2(A_1+B_1), 2A_3)$$

와 같이 주어진다. 따라서 전체적인 복호 과정이 $s=1$과 유사하다.

정리 12 오증이 $a_1^3+a_3=0$을 만족한다고 하자.

i) $a_1+b_1=0$이면 오류벡터는 $e=3X$이다. 이 때 $x=a_1$이다.

ii) $a_1+b_1\neq 0$이면 오류벡터는 $e=X+2Y$이다. 이 때 $x=a_1$이고 $y=b_1$이다.

정리 13 오류벡터의 오증이 $a_1^3+a_3\neq 0$이면, a_1에 따라 식 (8) 또는 (9)의 근을 γ_2라 하고, $\gamma_1=a_1$, $\gamma_3=a_3+a_1^3+a_1\gamma_2$와 같이 정의하자. 또한 $u^3+\gamma_1 u^2+\gamma_2 u+\gamma_3=0$이 서로 다른 세 근을 가진다고 하자.

i) $\gamma_2=b_1^2+(a_1^6+a_3^2)/(a_1^4+b_1^4)$이면, $e=X+3Y+3Z$이다. 여기서 y와 z는 삼차방정식의 나머지 두 근이고, $x=a_1+(a_1^3+a_3)/(a_1^2+b_1^2)$이다.

ii) $\gamma_2=b_1^2$이면 $e=X+Y+Z$이고, x, y와 z는 삼차방정식의 세 근이다.

$s=3$인 경우 Goethals 부호의 복호 알고리즘을 흐름도로 나타내면 그림 4와 같다.

V. 결 론

본 논문에서는 유한체뿐만 아니라 Galois 환에서도 Newton 항등식이 존재함을 보였으며, 이를 이용하여 Z_4위의 Goethals 부호의 복호 알고리즘을 제안하였다.

참 고 문 헌

[1] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solë, "The Z_4-Linearity of Kerdock, Preparata, Goethals, and Related Codes," *IEEE Transaction on Information Theory*, vol. 40, no. 2, pp. 301-319, March 1994.

[2] T. Helleseth, and P. V. Kumar, "The Algebraic Decoding of the Z_4-Linear Goethals Code," *IEEE Transaction on Information Theory*, vol. 41, no. 6, November 1995.

[3] Chunming Rong, and T. Helleseth, "The Algebraic Decoding of the Z_4-Linear Calderbank-McGuire Code," *Proceedings of 1997 International Symposium on Information Theory (ISIT '97)*, p. 328, Ulm, Germany, June 29 - July 4, 1997.

[4] P. V. Kumar, T. Helleseth, and A. R. Calderbank, "An Upper Bound for Weil Exponential Sums over Galois Rings and Applications," *IEEE Transaction on Information Theory*, vol. 41, no. 2, March 1995.

[5] A. R. Calderbank, G. McGuire, P. V. Kumar, and T. Helleseth, "Cyclic Codes over Z_4, Locator Polynomial, and Newton's Identities, *IEEE Transaction on Information Theory*, vol. 42, no. 1, pp. 217-226, January 1996.

[6] F. J. MacWilliams, and N. J. A. Sloane, *The Theory of Error Correcting Codes*. Amsterdam: North-Holland, 1977.

임 두 루(DooRoo Lim) 정회원

1973년 7월 10일생

1996년 2월 : 한양대학교 전파공학과 졸업(공학사)

1998년 2월 : 한양대학교 대학원 전자통신공학과 졸업(공학석사)

1998년 2월~현재 : 현대전자 통신연구 9실 근무

양 경 철(KyeongCheol Yang) 정회원

1963년 9월 26일생

1986년 2월 : 서울대학교 전자공학과 졸업(공학사)

1988년 2월 : 서울대학교 대학원 전자공학과 졸업(공학석사)

1992년 12월 : Univ. of Southern California (USC) 전기공학과 졸업 (공학박사)

1993년 3월~1996년 2월 : 한양대학교 전자통신공학과 전임강사

1996년 3월~현재 : 한양대학교 전자통신공학과 조교수