새로운 순환부호의 해밍중 유도

*최성태O, *김지엽, *노종선, **정하봉
*서울대학교 전기컴퓨터공학부, 뉴미디어통신공동연구소
**홍익대학교 전자전기공학부

Hamming Weight Distribution of New Cyclic Code

*Sung-Tai ChoiO, *Ji-Youp Kim, *Jong-Seon No, and **Habong Chung
*Department of EECS, INMC, Seoul National University
**School of Electronics and Electrical Engineering, Hongik University,
{stchoi,lakroforce}@ccl.snu.ac.kr, jsno@snu.ac.kr, habchung@hongik.ac.kr

요약

본 논문에서는 소수 $p \equiv 3 \bmod 4$, 홀수 n, 그리고 $d=(p^n+1)/(p^k+1)+(p^n-1)/2$, $k|n$에 대해서 a,b가 유한체 F_{p^n}에서 변할 때 $S(a,b)=\sum_{x\in F_{p^n}} \omega^{\mathrm{tr}_1^n(ax+bx^d)}$로 정의된 지수합 값의 분포를 유도하였다. 여기서 ω는 p-차 복소 원시근이다. 유도된 분포로부터 순환 부호 $\mathcal{C}$의 해밍중 분포를 구한다. F_p상에서 정의된 순환부호 $\mathcal{C}$의 차원 $\dim_{F_p}\mathcal{C}=2n$이고 길이 $L=p^n-1$인 부호 워드들로 이루어진다.

1. 개요

부호의 최소 거리는 그 부호의 오류 정정 능력과 관계된다. 만약 선형부호인 경우 최소 거리는 부호의 최소 해밍중과 같기 때문에 부호의 최소 해밍중이 부호의 오류 정정 능력을 결정한다. 소수 p상에서 정의된 선형부호의 해밍중 분포에 대한 연구 결과들이 최근까지 발표되었다. [2]–[4]

본 논문에서는 a,b가 F_{p^n}에서 변할 때 지수합 $S(a,b)$의 값의 분포를 구한다. 또한 그 결과를 이용하여 순환부호 $\mathcal{C}$의 해밍중 분포를 유도한다.

2. 사전 지식 및 기호

A. 지수합과 부호 $\mathcal{C}$의 해밍중

p는 소수이고 F_{p^n}은 p^n개의 원소를 갖는 유한체라 놓자. F_{p^n}에서 F_{p^m}로 가는 trace 함수 $\mathrm{tr}_m^n(\cdot)$는 다음과 같이 정의된다.

$$\mathrm{tr}_m^n(x)=\sum_{i=0}^{\frac{n}{m}-1} x^{p^{mi}}$$

여기서 $x\in F_{p^n}$이고 $m|n$이다. α는 F_{p^n}의 원시 원소이고 $F_{p^n}^*=F_{p^n}\setminus\{0\}$이다.

본 논문에서는 a,b가 F_{p^n}에서 변할 때 다음과 같이 정의된 지수합 $S(a,b)$의 값의 분포를 유도할 것이다.

$$S(a,b)=\sum_{x\in F_{p^n}} \chi(ax+bx^d)$$

여기서 ω는 p-차 복소 원시근이고 $\chi(\cdot)=\omega^{\mathrm{tr}_1^n(\cdot)}$는 F_{p^n}의 canonical multiplicative character이다.

B. 이차 형식

변수가 k개인 F_{p^s} 상에서 이차 형식은 $F_{p^s}[x_1,\ldots,x_k]$에 속한 동차다항식이고 다음과 같이 정의한다.

$$f(\mathbf{x})=f(x_1,\ldots,x_k)=\sum_{i,j=1}^{k} a_{ij}x_ix_j$$

여기서 p는 소수이고 $a_{ij}=a_{ji}\in F_{p^s}$이다.

보조정리 1: $x\in F_{p^n}$상에서의 다음과 같이 정의된 함수를 고려하자.

$$\mathrm{tr}_1^n\Big(\sum_i a_i x^{p^i+1}\Big)=\mathrm{tr}_1^s\big(f(x)\big),\ 0\le i<n$$

여기서 $a_i\in F_{p^n}^*$이고 s는 n과 모든 0이 아닌 i들의 최대 공약수이다. 그러면

$$f(x)=\mathrm{tr}_s^n\Big(\sum_i a_i x^{p^i+1}\Big)$$

는 F_{p^s}상에서 이차 형식이다. ■

보조정리 2 (Luo and Feng [3]): $F_{p^{sk}}$에서 F_{p^s}로 가는 이차 형식 $f(x)$의 rank r이라 놓자. 그러면 모든 $x\in F_{p^{sk}}$에 대해서 $f(x+y)-f(x)-f(y)=0$를 만족하는 해 $y\in F_{p^{sk}}$의 개수는 $(p^s)^{k-r}$로 주어진다. ■

보조정리 3 (Luo and Feng [3]): $f(x)$는 $F_{p^{sk}}$에서 F_{p^s}로 가고 rank r과 행렬식 Δ인 이차 형식 $f(\mathbf{x}) \in F_{p^s}[x_1, x_2, \ldots, x_k]$이라 하자. 이때 다음 수식이 성립한다.

$$\sum_{x \in F_{p^{sk}}} \omega^{\mathrm{tr}_1^s(f(x))} = \begin{cases} \eta(\Delta)(p^s)^{k-\frac{r}{2}}, & \text{if } p^s \equiv 1 \bmod 4 \\ j^r \eta(\Delta)(p^s)^{k-\frac{r}{2}}, & \text{if } p^s \equiv 3 \bmod 4 \end{cases}$$

여기서 $j = \sqrt{-1}$. ■

3. $S(a,b)$의 값의 분포

A. 기호

본 논문에서는 a, b가 F_{p^n}에서 변할 때 $S(a,b)$의 분포를 고려한다. 각 정리들의 증명은 지면 분량상 최대한 생략하였다. 본 논문에서는 다음의 기호들을 사용한다:

- p는 $p \equiv 3 \bmod 4$인 소수;
- n은 홀수;
- $d = (p^n+1)/(p^k+1) + (p^n-1)/2$, $k|n$.

B. $S(a,b)$의 값 구하기

이 장에서는 a, b F_{p^n}에서 변할 때 $S(a,b)$가 어떤 값을 갖는지 유도한다.

보조정리 4: a 또는 b가 0이면, $S(a,b)$는 다음과 같이 구할 수 있다.

$$S(a,b) = \begin{cases} p^n, & \text{when } a = b = 0 \\ 0, & \text{when } a \neq 0 \text{ and } b = 0 \\ \pm j p^{\frac{n}{2}}, & \text{when } a = 0 \text{ and } b \neq 0. \end{cases}$$

■

$a, b \in F_{p^n}^*$이면, $S(a,b)$는 이차 형식을 이용하여 다음과 같이 표현할 수 있다.

$$\begin{aligned} S(a,b) &= \sum_{x \in F_{p^n}} \chi(ax + bx^d) \\ &= \frac{1}{2}\Big(\sum_{x \in F_{p^n}} \chi(ax^{p^k+1} + bx^2) \\ &\quad + \sum_{x \in F_{p^n}} \chi(-ax^{p^k+1} + bx^2)\Big) \\ &= \frac{1}{2}(S_1(a,b) + S_2(a,b)) \end{aligned} \tag{2}$$

여기서 $S_1(a,b) = \sum_{x \in F_{p^n}} \chi(ax^{p^k+1} + bx^2)$이고 $S_2(a,b) = \sum_{x \in F_{p^n}} \chi(-ax^{p^k+1} + bx^2)$. $\gcd(p^k+1, p^n-1) = 2$이고 -1는 F_{p^n}에서 비제곱원이다. 보조정리 1로부터,

$$Q_1(x) = \mathrm{tr}_k^n(ax^{p^k+1} + bx^2)$$

와

$$Q_2(x) = \mathrm{tr}_k^n(-ax^{p^k+1} + bx^2)$$

는 F_{p^k}상에서 이차 형식임을 알 수 있다. $S_1(a,b)$와 $S_2(a,b)$의 값을 구하기 위해 각 이차 형식의 rank를 구해야 한다. 보조정리 2로부터 다음을 만족하는 해 $x \in F_{p^n}$의 개수를 구해야 한다.

$$\begin{aligned} &Q_1(x+y) - Q_1(x) - Q_1(y) = 0, \text{ for all } y \in F_{p^n} \\ &\Leftrightarrow \phi_{a,b}(x) = a^{p^k} x^{p^{2k}} + 2b^{p^k} x^{p^k} + ax = 0. \end{aligned} \tag{1}$$

$\phi_{a,b}(x)$는 F_{p^n}상에서 선형 방정식이기 때문에 근 $x \in F_{p^n}$의 개수는 1, p^k, 또는 p^{2k}이다. 그러므로 보조정리 2로부터, $Q_1(x)$의 rank는 e, $e-1$, 또는 $e-2$이다, 여기서 $e = n/k$. 비슷하게 $Q_2(x)$의 rank 또한 e, $e-1$, 또는 $e-2$이다.

보조정리 3로부터, 지수합 $S_1(a,b)$과 $S_2(a,b)$는 다음의 값들을 갖는다.

$$\begin{cases} \pm j p^{\frac{n}{2}}, & \text{for } r = e \\ \pm j\sqrt{p^k} p^{\frac{n}{2}}, & \text{for } r = e-1 \\ \pm j p^k p^{\frac{n}{2}}, & \text{for } r = e-2 \end{cases} \tag{3}$$

여기서 $j = \sqrt{-1}$이고 r은 각 이차 형식의 rank를 가리킨다.

[5]에서 사용된 방법과 비슷하게 두 지수합의 값들 중 실제로 나오지 않는 값들은 다음의 보조정리와 같이 배제될 수 있다.

보조정리 5: $\phi_{a,b}(x)$와 $\phi_{-a,b}(x)$ 중 적어도 한 개의 다항식은 F_{p^n}에서 한 개의 근을 갖는다. 다시 말해서 $Q_1(x)$와 $Q_2(x)$ 중 적어도 하나는 rank e를 갖는다. ■

보조정리 6: $S(a,b)$의 값들 중 $\pm j(p^k-1)/2p^{n/2}$는 a, b가 F_{p^n}에서 변하는 동안 실제로 발생하지 않는다. ■

정리 1: $a, b \in F_{p^n}$일 때 지수합 $S(a,b)$는 다음의 값들을 가질 수 있다.

$$\{p^n, 0, \pm j p^{\frac{n}{2}}, \frac{\sqrt{p^k} \pm j}{2} p^{\frac{n}{2}}, \frac{-\sqrt{p^k} \pm j}{2} p^{\frac{n}{2}}, \pm j \frac{p^k+1}{2} p^{\frac{n}{2}}\}. \tag{4}$$

Proof: 보조정리 4, 5, 6, 그리고 (3)를 이용하여 증명 가능하다. ■

C. $S(a,b)$의 값의 분포

이번 장에서는 a, b가 F_{p^n}에서 변할 때 각 $S(a,b)$ 값들이 몇 번 씩 발생하는지 유도한다. 앞 장에서 $S(a,b)$의 값은 최대 10개 임을 증명하였다. v_i와 Ω_i, $0 \leq i \leq 9$, 는 각각 i번째 $S(a,b)$의 값과 그 값이 발생하는 횟수라고 놓자. 그러면 다음 식들이 성립함을 알 수 있다.

$$\sum_{i=0}^{9} v_i \Omega_i = \sum_{b,x \in F_{p^n}} \omega^{\mathrm{tr}_1^n(bx^d)} \sum_{a \in F_{p^n}} \omega^{\mathrm{tr}_1^n(ax)} = p^{2n}$$

이고

$$\begin{aligned} \sum_{i=0}^{9} v_i^2 \Omega_i &= p^n \sum_{a,x,y \in F_{p^n}} \omega^{\mathrm{tr}_1^n(a(x^d+y^d))} \sum_{b \in F_{p^n}} \omega^{\mathrm{tr}_1^n(b(x+y))} \\ &= p^n \sum_{a,y \in F_{p^n}} \omega^{\mathrm{tr}_1^n(2ay^d)} = p^{2n}. \end{aligned}$$

[7]의 결과를 이용하여 a, b가 F_{p^n}에서 변할 때 이차 형식 $Q_1(x)$와 $Q_2(x)$들이 가질 수 있는 rank들의 분포를 유도할 수 있다.

보조정리 7: 다음 식이 성립함을 알 수 있다.

$$N_1 = \Omega_4 + \Omega_5 + \Omega_6 + \Omega_7 = 2p^{n-k}(p^n - 1)$$
$$N_2 = \Omega_8 + \Omega_9 = \frac{2(p^{n-k}-1)(p^n-1)}{p^{2k}-1}.$$

■

정리 2: a, b가 F_{p^n}에서 변할 때 $S(a,b)$의 값의 분포는 다음과 같이 구할 수 있다.

$$S(a,b) = \begin{cases} p^n, & \text{once} \\ 0, & \frac{(p^k-1)(p^{2n}-1)}{2(p^k+1)} \text{ times} \\ \pm jp^{n/2}, & \frac{p^{2n}-1}{4} - \frac{(p^n-1)^2}{2(p^k-1)} \text{ times} \\ \frac{\sqrt{p^k}\pm j}{2}p^{\frac{n}{2}}, & \frac{(p^n-1)(p^{n-k}+p^{\frac{n-k}{2}})}{2} \text{ times} \\ \frac{-\sqrt{p^k}\pm j}{2}, & \frac{(p^n-1)(p^{n-k}-p^{\frac{n-k}{2}})}{2} \text{ times} \\ \pm j\frac{p^k+1}{2}p^{\frac{n}{2}}, & \frac{(p^{n-k}-1)(p^n-1)}{p^{2k}-1} \text{ times.} \end{cases}$$

Proof: 두 값이 켤레복소수 관계인 경우 두 값은 항상 같은 횟수만큼 발생하고 $S(a,b) = p^n$은 $a = b = 0$일 때 한번 발생한다. 그러므로 우리는 Ω_i에 관한 5개의 방정식만이 필요하다. 이미 유도한 방정식들로부터 Ω_i를 모두 결정하는 것이 가능하다. ■

4. 부호 $\mathcal{C}$의 해밍중 분포

순환부호 $\mathcal{C}$를 F_p상에서 길이 $L = p^n - 1$인 부호 워드들로 구성된 집합이라 놓자. 각 순환부호는 다음과 같이 주어진다.

$$c(a,b) = (c_0, c_1, \ldots, c_{L-1}),\ a, b \in F_{p^n}$$

여기서 $c_i = \mathrm{tr}_1^n(a\alpha^i + b\alpha^{di})$, $0 \le i \le L-1$. $c(a,b)$의 해밍중은 다음과 같이 $S(a,b)$로 표현할 수 있다.

$$\begin{aligned} w_H(c(a,b)) &= \left|\{i | 0 \le i \le L-1, c_i \neq 0\}\right| \\ &= p^{n-1}(p-1) - \frac{1}{p}\mu(S(a,b)) \end{aligned} \quad (5)$$

여기서 $\mu(S(a,b)) = \sum_{j=1}^{p-1} S(ja, jb)$라고 정의한다. $\{w_0, w_1, \ldots, w_L\}$를 $\mathcal{C}$의 해밍중 분포라 놓자. 이때 w_i는 a, b가 F_{p^n}에서 변할 때 해밍중이 i, $0 \le i \le L$인 $c(a,b)$의 개수이다.

정리 3: F_p상에서 순환부호 $\mathcal{C}$의 차원은 $\dim_{F_p}\mathcal{C} = 2n$이고 해밍중 분포 $\{w_0, w_1, \ldots, w_L\}$는 다음과 같이 구할 수 있다.

$$i = \begin{cases} 0, & w_i = 1 \\ p^{n-1}(p-1), & \\ & w_i = (p^n-1)(p^n - 2p^{n-k} + 1) \\ (p-1)(p^{n-1} + \frac{1}{2}p^{\frac{n+k}{2}-1}), & \\ & w_i = (p^n-1)(p^{n-k} - p^{\frac{n-k}{2}}) \\ (p-1)(p^{n-1} - \frac{1}{2}p^{\frac{n+k}{2}-1}), & \\ & w_i = (p^n-1)(p^{n-k} + p^{\frac{n-k}{2}}). \end{cases}$$

Proof: (5)로부터, $w_H(c(a,b))$를 구하기 위해 다음을 계산하여야 한다.

$$\mu(S(a,b)) = \sum_{j=1}^{p-1} S(ja, jb) = \sum_{j=1}^{p-1} \sigma_j(S(a,b))$$

$p \equiv 3 \bmod 4$이고 n은 홀수 이기 때문에, $\pm jp^{\frac{n}{2}}$는 $\pm(\sqrt{p^*})^n$와 같다. 그러므로 다음의 값들을 구할 수 있다.

$$\begin{aligned} \mu(0) &= \mu(\pm jp^{\frac{n}{2}}) = \mu(\pm j\frac{p^k+1}{2}p^{\frac{n}{2}}) \\ &= \sum_{l=1}^{p-1}\sigma_l(\pm\sqrt{p^*})^n = (\pm\sqrt{p^*})^n\sum_{l=1}^{p-1}(\frac{l}{p}) = 0 \\ \mu(&\frac{\sqrt{p^k}}{2}p^{\frac{n}{2}} \pm \frac{1}{2}jp^{\frac{n}{2}}) = \frac{\sqrt{p^k}}{2}(p-1)p^{\frac{n}{2}} \\ \mu(&-\frac{\sqrt{p^k}}{2}p^{\frac{n}{2}} \pm \frac{1}{2}jp^{\frac{n}{2}}) = -\frac{\sqrt{p^k}}{2}(p-1)p^{\frac{n}{2}} \\ \mu(&p^n) = (p-1)p^n. \end{aligned}$$

그러므로, (5)를 통해 증명된다. ■

5. 감사의 글

본 연구는 방송통신위원회의 차세대통신네트워크원천기술개발사업 (KCA-2012-08-911-04-003)과 2012년도 정부 (교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2012-0000186).

6. 참고문헌

[1] H. M. Trachtenberg, "On the cross-correlation functions of maximal recurring sequences," *Ph.D. dissertation*, Univ. of Southern California, Los Angeles, CA, 1970.

[2] K. Feng and J. Luo, "Weight distribution of some reducible cyclic codes," *Finite Fields Appl.*, vol. 14, no. 2, pp. 390–409, Apr. 2008.

[3] J. Luo and K. Feng, "Cyclic codes and sequences from generalized Coulter-Matthew function," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5345–5353, Dec. 2008.

[4] J. Luo and K. Feng, "On the weight distributions of two classes of cyclic codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5332–5344, Dec. 2008.

[5] Y. Xia, X. Zeng, and L. Hu, "Further crosscorrelation properties of sequences with the decimation factor $d = (p^n+1)/(p+1) - (p^n-1)/2$," *Appl. Algebra Eng. Commun. Comput.*, vol. 21, no. 5, pp. 329–342, 2010.

[6] R. Lidl and H. Niederreiter, *Finite Fields*, vol. 20 of *Encyclopedia of Mathematics and Its Applications*. Reading, MA: Addison-Wesley, 1983.

[7] A. W. Bluher, "On $x^{q+1} + ax + b$," *Finite Fields and Their Applications*, vol. 10, no. 3, pp. 285-305, Jul. 2004.