김일성종합대학학보 주체109(2020)년
수 학 제66권 제3호

3개의 령점을 가진 순환부호의 무게분포와 지표합사이의 관계

신 창 현

위대한 령도자 **김정일**동지께서는 다음과 같이 교시하시였다.

《새로운 과학기술분야를 개척하기 위한 사업도 전망성있게 밀고나가야 합니다.》(《**김정일**선집》 증보판 제11권 138페지)

최근에 순환부호 $C_{(q,\ m,\ h,\ e)}$의 무게분포가 많이 연구되였다. 여기서 $q:=p^s$인데 p는 홀씨수이고 s는 정의 웅근수이다. 그리고 m은 정의 웅근수이고 h는 $q-1$의 정의 약수이며 e는 h의 정의 약수이다. $N:=\gcd(m,\ e(q-1)/h)$로 놓자. 선행연구[1]에서는 $e>1$, $N=1$인 경우와 $e=2$, $N=2$인 경우에 이 부호의 무게분포를 결정하고 나머지경우들에도 무게분포를 결정하는것이 필요하다는데 대하여 밝혔다. 그후부터 지금까지 무게분포가 결정된 경우들은 다음과 같다.

① $e=2$, $N=3$인 경우, $e=2$, $p^j+1\equiv 0\pmod N$인 경우[2]

② $e=3$, $N=2$인 경우[3]

③ $e=4$, $N=2$인 경우, $e=3$, $N=3$인 경우, $e=3$, $p^j+1\equiv 0\pmod N$인 경우[4－6]

론문에서는 순환부호 $C_{(q,\ m,\ h,\ e)}$의 무게분포를 지금까지 해결되지 않은 경우들중의 하나인 $e=4$, $N=3$인 경우에 대하여 연구하였다. 이 경우에 검사다항식은 공액이 아닌 3개의 령점을 가지게 되는데 이때 순환부호는 3개의 령점을 가진다고 말한다.

원소수가 q인 유한체를 $\mathbf{F}_q$로 표시하자. 또한 $r:=q^m$이라고 하자. 그리고 $\mathbf{F}_r^*$을 $\mathbf{F}_r$의 곱하기군이라고 하자. 또한 α를 $\mathbf{F}_r^*$의 생성원소라고 하자. 그리고

$$g:=\alpha^{(q-1)/h},\ \ n:=\frac{h\ \ (r-1)}{(q-1)},\ \ \beta:=\alpha^{(r-1)/e}$$

으로 놓자. 그러면 순환부호 $C_{(q,\ m,\ h,\ e)}:=\{\boldsymbol{c}_{(a,\ b)}\mid a,\ b\in\mathbf{F}_r\}$의 부호단어 $\boldsymbol{c}_{(a,\ b)}$는 다음과 같이 표시할수 있다.

$$\boldsymbol{c}_{(a,\ b)}:=(\mathrm{Tr}(ag^i+b(\beta g)^i))_{i=0}^{n-1}$$

여기서 Tr는 $\mathbf{F}_r$를 $\mathbf{F}_q$에로 넘기는 고유합함수이다. 또한 $C^{(N,\ r)}$는 $\mathbf{F}_r$의 령이 아닌 완전 N제곱원소들전부로 이루어진 $\mathbf{F}_r$의 부분군이라고 하자. 그러면 임의의 $u(\in\mathbf{F}_r)$에 대하여 가우스주기 $\eta_u^{(N,\ r)}$는 다음과 같이 정의된다.

$$\eta_u^{(N,\ r)}:=\sum_{z\in C^{(N,\ r)}}\psi(zu)$$

여기서 ψ는 $\mathbf{F}_r$의 표준더하기지표이다. 론문에서는 $\eta_u^{(N,\ r)}$를 간단히 η_u로 표시하겠다. 그러면 $uC^{(N,\ r)}=u'C^{(N,\ r)}$일 때 $\eta_u=\eta_{u'}$이다. 그러므로 $u=1,\ \alpha,\ \cdots,\ \alpha^{N-1}$에 대응하는 N개의 가우스주기들만을 생각하겠다.

다음의 명제는 부호단어 $\boldsymbol{c}_{(a,\ b)}$의 무게와 가우스주기사이의 관계를 보여준다.

명제 1[1] 부호단어 $\boldsymbol{c}_{(a,\ b)}$의 무게는 $h(r-1)/q-(hN/eq)\mu(a,\ b)$이다. 여기서 $\mu(a,\ b)=$

$=\sum_{i=1}^{e}\eta_{(a+\beta^i b)g^i}^{(N,\ r)}$ 이다.

$\mu(a,\ b)$를 부호단어 $\boldsymbol{c}_{(a,\ b)}$의 변경된 무게라고 부른다.

명제 2[7] 임의의 $u(\in\mathbf{F}_r)$에 대하여 $G_u=\sum_{x\in\mathbf{F}_r}\psi(ux^N)$으로 놓자. 그러면 $G_u=N\eta_u+1$

이다. 또한 만일 $N=3$이면 다음의 사실들이 성립한다.

① $p\equiv 2\pmod 3$이고 $2|sm$이며 $sm/2$이 홀수이고 $(p+1)/3$이 짝수이면 $G_1=2\sqrt{r}$, $G_\alpha=G_{\alpha^2}=-\sqrt{r}$ 이다.

② $p\equiv 2\pmod 3$이고 $2|sm$이며 $sm/2$이 홀수이고 $(p+1)/3$이 홀수이면 $G_\alpha=2\sqrt{r}$, $G_1=G_{\alpha^2}=-\sqrt{r}$ 이다.

③ $p\equiv 2\pmod 3$이고 $4|sm$이면 $G_1=-2\sqrt{r}$, $G_\alpha=G_{\alpha^2}=\sqrt{r}$ 이다.

④ $p\equiv 1\pmod 3$이고 $3|sm$이면 $G_1=c_1p^{sm/3}$, $G_\alpha=-(c_1+9d_1)p^{sm/3}/2$, $G_{\alpha^2}=-(c_1-9d_1)p^{sm/3}/2$ 이다. 여기서 c_1과 d_1은 $c_1^2+27d_1^2=4p^{sm/3}$, $c_1\equiv 1\pmod 3$과 $\gcd(c_1,\ p)=1$에 의하여 결정되는 옹근수들이다.

유한군에서의 원소의 위수에 관한 성질을 리용하여 다음의 명제를 쉽게 증명할수 있다.

명제 3 순환부호 $C_{(q,\ m,\ h,\ e)}$의 정의식에서 리용된 파라메터들은 다음의 성질들을 가진다.

① $\beta\in\mathbf{F}_q$

② $(q-1)N|(r-1)$ 즉 $\mathbf{F}_q^*$의 원소들은 $\mathbf{F}_r$에서 완전 N제곱원소들이다.

$\chi(0):=0$으로 놓고 $\mathbf{F}_r^*$의 곱하기지표 χ를 $\mathbf{F}_r$에로 확장하자. 그리고 λ와 χ를 $\mathbf{F}_r$의 곱하기지표라고 하자. 이때 합

$$J(\lambda,\ \chi):=\sum_{\substack{a+b=1\\ a,\ b\in\mathbf{F}_r}}\lambda(a)\chi(b)$$

를 야꼬비합이라고 부른다.

보조정리 1 $r\equiv 1\pmod 6$이고 χ는 $\mathbf{F}_r$의 3차지표라고 하자. 이때 다음의 사실들이 성립한다.

① 임의의 $a(\in\mathbf{F}_r^*)$에 대하여 $\sum_{x\in\mathbf{F}_r}\chi(x^3+ax^2)=-1$ 이다.

② $\chi(4)=1$이면 $\sum_{x\in\mathbf{F}_r}\chi(x^2+x)=\sum_{x\in\mathbf{F}_r}\chi(x^2-x)=\sum_{x\in\mathbf{F}_r}\chi(x^2-1)=J(\chi,\ \chi)$ 이다.

③ $\chi(4)=1$이면 $\sum_{x\in\mathbf{F}_r}\chi(x^3-x)=J(\chi,\ \chi)-1$이다.

④ 임의의 다항식 $f(\in\mathbf{F}_r[x])$에 대하여 $\sum_{x\in\mathbf{F}_r}\chi(f(x^3))=\sum_{x\in\mathbf{F}_r}(1+\chi(x)+\chi(x^2))\chi(f(x))$ 이다.

보조정리 2 $r\equiv 1\pmod 6$이고 λ는 $\mathbf{F}_r$의 위수가 6인 곱하기지표라고 하자. 이때

다음의 사실이 성립한다.

① $J(\lambda^4,\ \lambda^2)=-1$

또한 $\lambda^2(4)=1$일 때 다음의 사실들이 성립한다.

② $J(\lambda,\ \lambda^2)=J(\lambda^3,\ \lambda^2)=J(\lambda^2,\ \lambda^2)$

③ $J(\lambda,\ \lambda^2)=\overline{J(\lambda^5,\ \lambda^2)}$

④ $\sum\limits_{x\in\mathbf{F}_r}\lambda^2(x^6-1)=3J(\lambda^2,\ \lambda^2)+\overline{J(\lambda^2,\ \lambda^2)}-1$

⑤ $\sum\limits_{x\in\mathbf{F}_r}\lambda^2(x^2(x^2-1))=2\mathrm{Re}\,J(\lambda^2,\ \lambda^2)$

보조정리 3 $\underline{c}=(c_1,\ \cdots,\ c_e)\in(\mathbf{F}_r^*)^e$일 때 모임

$F(\underline{c}):=\{(a,\ b)\in\mathbf{F}_r^2\mid (a+\beta^i b)g^i c_i\ (1\le\forall i\le e)$는 $\mathbf{F}_r$의 령이 아닌 완전 N제곱원소이다.$\}$

의 원소수는 다음과 같다.

$$f(\underline{c})=\frac{r-1}{N^e}\sum_{\substack{1\le i<e\\0\le k_i<N}}\prod_{i=1}^{e-1}\chi^{k_i}(g^i c_i c_e^{-1})\sum_{b\in\mathbf{F}_r}\prod_{i=1}^{e-1}\chi^{k_i}(b+\gamma_i)$$

여기서 χ는 위수가 N인 $\mathbf{F}_r$의 곱하기지표이고 $\gamma_i:=\beta^i/(1-\beta^i)\ (i=1,\ 2,\ \cdots,\ e-1)$이다.

보조정리 4 $e=4$, $N=3$이면 다음의 식이 성립한다.

$$f(\underline{c})=\frac{r-1}{81}\sum_{0\le k_i\le 2}\prod_{i=1}^{3}\chi^{k_i}(c_i c_4^{-1})\sum_{b\in\mathbf{F}_r}\chi^{k_1}(b+1)\chi^{k_2}(b)\chi^{k_3}(b-1)$$

여기서 χ는 $\mathbf{F}_r$의 3차지표이다.

증명 보조정리 3에 의하여

$$f(\underline{c})=\frac{r-1}{81}\sum_{\substack{1\le i\le 3\\0\le k_i<3}}\prod_{i=1}^{3}\chi^{k_i}(c_i c_4^{-1})\sum_{b\in\mathbf{F}_r}\prod_{i=1}^{3}\chi^{k_i}(b+\gamma_i)$$

가 성립한다. 그런데 $\gamma_1-\gamma_2=\beta/2$이고 $\gamma_3-\gamma_2=-\beta/2$이다. 그러므로

$$\sum_{b\in\mathbf{F}_r}\chi^{k_1}(b+\gamma_1)\chi^{k_2}(b+\gamma_2)\chi^{k_3}(b+\gamma_3)=\sum_{b\in\mathbf{F}_r}\chi^{k_1}(b+\beta/2)\chi^{k_2}(b)\chi^{k_3}(b-\beta/2)$$

가 성립한다. 또한 다음의 식이 성립한다.

$$\sum_{b\in\mathbf{F}_r}\chi^{k_1}\left(b+\frac{\beta}{2}\right)\chi^{k_2}(b)\chi^{k_3}\left(b-\frac{\beta}{2}\right)=\prod_{i=1}^{3}\chi^{k_i}\left(\frac{\beta}{2}\right)\left(\sum_{b\in\mathbf{F}_r}\chi^{k_1}(b+1)\chi^{k_2}(b)\chi^{k_3}(b-1)\right)$$

그런데 $\chi(\beta/2)=1$이므로 결국 보조정리의 결과가 나온다.(증명끝)

보조정리 5 $e=4$, $N=3$이면 다음의 식이 성립한다.

$$\begin{aligned}\frac{81}{r-1}f(\underline{c})=r-3-4\mathrm{Re}(&\chi(c_1')+\chi(c_2')+\chi(c_3')+\chi(c_1'c_2'^2)+\chi(c_1'c_3'^2)+\chi(c_2'c_3'^2))+\\&+2\mathrm{Re}(\chi(c_1'c_2')+\chi(c_1'c_3')+\chi(c_2'c_3')+\chi(c_1'c_2'c_3'))(J_r-1)+\\&+4\mathrm{Re}(\chi(c_1'c_2'^2c_3'))J_r+2\mathrm{Re}(\chi(c_1'c_2'c_3'^2)+\chi(c_1'c_2'^2c_3'^2))Q_r\end{aligned}$$

여기서

$$c_i' := \frac{c_i}{c_4}\ (i=1,2,3),\ \ J_r := \mathrm{Re}\sum_{x\in\mathbf{F}_r}\chi(x-x^2),\ \ Q_r := \sum_{x\in\mathbf{F}_r}\chi(x(x-1)^2(x+1))$$

이다.

증명 보조정리 4로부터

$$f(\underline{c}) = \frac{r-1}{81}\sum_{0\le k_i\le 2}\prod_{i=1}^{3}\chi^{k_i}(c_i c_4^{-1})f_{k_1,\ k_2,\ k_3}$$

이 성립한다. 여기서

$$f_{k_1,\ k_2,\ k_3} := \sum_{b\in\mathbf{F}_r}\chi^{k_1}(b+1)\chi^{k_2}(b)\chi^{k_3}(b-1)$$

이다. 그런데 $\chi(0)=0$이므로 $f_{0,\ 0,\ 0} = \sum_{b\in\mathbf{F}_r\setminus\{-1,\ 0,\ 1\}} 1 = r-3$이다.

또한 지표의 직교성과 명제 3의 결과 ②로부터

$$f_{1,\ 0,\ 0} = f_{0,\ 1,\ 0} = f_{0,\ 0,\ 1} = f_{2,\ 0,\ 0} = f_{0,\ 2,\ 0} = f_{0,\ 0,\ 2} = -2$$

가 성립한다. 그리고 보조정리 1의 결과 ②로부터

$$f_{1,\ 1,\ 0} = f_{0,\ 1,\ 1} = f_{1,\ 0,\ 1} = \sum_{x\in\mathbf{F}_r}\chi(x-x^2) - 1$$

이 성립한다. 또한 $\chi^2 = \overline{\chi}$이므로 다음의 식이 성립한다.

$$f_{2,\ 2,\ 0} = f_{2,\ 0,\ 2} = f_{0,\ 2,\ 2} = \overline{f_{0,\ 1,\ 1}}$$

또한 보조정리 1의 결과 ①로부터 다음의 식이 성립한다.

$$f_{1,\ 2,\ 0} = f_{0,\ 2,\ 1} = f_{2,\ 1,\ 0} = f_{0,\ 1,\ 2} = f_{1,\ 0,\ 2} = f_{2,\ 0,\ 1} = -2$$

또한 보조정리 1의 결과 ③으로부터 다음의 식이 성립한다.

$$f_{1,\ 1,\ 1} = f_{0,\ 1,\ 1} - 1$$

또한 보조정리 2의 결과 ⑤로부터 다음의 식이 성립한다.

$$f_{1,\ 2,\ 1} = 2J_r$$

그런데 $f_{2,\ 1,\ 2} = \overline{f_{1,\ 2,\ 1}}$이다. 그러므로 $f_{2,\ 1,\ 2} = 2\mathrm{Re}\,J_r$이다.

한편 $f_{1,\ 1,\ 2} = Q_r$가 성립한다는것은 분명하다.

또한 다음의 식이 성립한다는것을 알수 있다.

$$f_{1,\ 1,\ 2} = \sum_{x\in\mathbf{F}_r}\chi(x(x+1)(x-1)^2) = \sum_{x\in\mathbf{F}_r}\chi(-x(-x+1)(-x-1)^2) = f_{2,\ 1,\ 1}$$

계속하여 다음의 식도 성립한다는것을 알수 있다.

$$f_{1,\ 1,\ 2} = \sum_{x\in\mathbf{F}_r}\chi(x(x+1)(x-1)^2) = \sum_{x\in\mathbf{F}_r}\chi\left(\frac{(1+x)(1-x)^2}{x^4}\right) = \sum_{x\in\mathbf{F}_r}\chi(x^2(1+x)(1-x)^2) = f_{1,\ 2,\ 2}$$

그런데 $f_{2,\ 1,\ 1} = \overline{f_{1,\ 2,\ 2}}$, $f_{1,\ 1,\ 2} = \overline{f_{2,\ 2,\ 1}}$이다. 그러므로 $f_{1,\ 1,\ 2} = f_{2,\ 2,\ 1}$이다. 따라서 우에서

얻어진 식들을 식 (1)에 대입하면 결과식이 나온다.(증명끝)

정리 $e=4$, $N=3$ 인 경우에 $p\equiv 2 \pmod 3$, $s\equiv 2 \pmod 4$ 이면 순환부호 $C_{(q,\ m,\ h,\ e)}$의 무게분포는 다음의 표와 같다.

표. $e=4$, $N=3$ 인 경우의 무게분포

변경된 무게	빈도수
$(r-1)/3+2\sqrt{r}-1$	$4(r-1)/3$
$(r-1)/3-\sqrt{r}-1$	$8(r-1)/3$
$(8\sqrt{r}-4)/3$	$(r-1)(r+12\sqrt{r}+4Q_r-35)/81$
$(5\sqrt{r}-4)/3$	$(r-1)(8r-24\sqrt{r}-16Q_r-64)/81$
$(2\sqrt{r}-4)/3$	$(r-1)(24r+24Q_r+24)/81$
$(-\sqrt{r}-4)/3$	$(r-1)(32r+24\sqrt{r}-16Q_r-40)/81$
$(-4\sqrt{r}-4)/3$	$(r-1)(16r-12\sqrt{r}+4Q_r-128)/81$

실례 $q=25$, $m=3$, $e=h=4$ 라고 하자. 그러면 $N=3$ 이고 $n=2\,604$, $r=15\,625$, $Q_{15\,625}=$ $=-74$ 이다. 따라서 정리 1에 의하여 순환부호 $C_{(q,\ m,\ h,\ e)}$의 무게계수다항식은 다음과 같다.

$$A(x)=1+20\ 832x^{1\,845}+41\ 664x^{1\,890}+3\ 239\ 376x^{2\,460}+23\ 748\ 480x^{2\,475}+$$
$$+71\ 995\ 392x^{2\,490}+97\ 243\ 776x^{2\,505}+47\ 851\ 104x^{2\,520}$$

참 고 문 헌

[1] Changli Ma et al.; IEEE Trans. Inform. Theory, 57, 1, 397, 2011.

[2] Cunsheng Ding et al.; IEEE Trans. Inform. Theory, 57, 12, 8000, 2011.

[3] Baocheng Wang et al.; IEEE Trans. Inform. Theory, 58, 12, 7253, 2012.

[4] Maosheng Xiong; Finite Fields Appl., 18, 5, 933, 2012.

[5] Maosheng Xiong; Des. Codes Cryptogr., 72, 3, 511, 2012.

[6] Maosheng Xiong; Finite Fields Appl., 21, 1, 84, 2013.

[7] G. Myserson; Acta Arith., 39, 3, 251, 1981.

주체109(2020)년 3월 15일 원고접수

A Relation between the Weight Distributions of Cyclic Codes with Three Zeros and Character Sums

Sin Chang Hyon

Recently, the weight distributions of cyclic codes with two zeros have been determined for several cases. In this paper, we present a relation between the weight distributions of cyclic codes with three zeros and character sums over a finite field.

Keywords: cyclic code, weight distribution, character sum