김일성종합대학학보 주체110(2021)년
수 학 제67권 제3호

유한체우에서 길이가 $2l^m p^n$ 인 중복뿌리에르미트자기쌍대부순환부호

량명국, 김률

경애하는 **김정은**동지께서는 다음과 같이 말씀하시였다.

《과학기술을 확고히 앞세우고 과학기술과 생산을 밀착시키며 경제건설에서 제기되는 모든 문제들을 과학기술적으로 풀어나가는 기풍을 세워 나라의 경제발전을 과학기술적으로 확고히 담보하여야 합니다.》

$\mathbf{F}_q$ 가 q 개의 원소들로 이루어진 표수가 p 인 유한체이고 n은 q와 서로 소인 정의 옹근수라고 하자. 이때 매 옹근수 $s\,(0\le s\le n)$ 에 대하여 모임

$$Cl_{s,\,q}:=\{s,\ sq,\ sq^2,\ \cdots,\ sq^{n_s-1}\}$$

을 s를 포함하는 모듈 n에 관한 $q-$원분합동류라고 부른다. 여기서 n_s 는

$$s\equiv sq^{n_s}\pmod{n}$$

인 최소의 정의 옹근수이다.

α 가 $\mathbf{F}_q$ 의 어떤 확대체에서 1의 원시 n 차뿌리일 때

$$M_{s,\,q}(x):=\prod_{i\in Cl_{s,\,q}}(x-\alpha^i)$$

은 $\mathbf{F}_q$ 우에서 α^s 의 최소다항식이다.[5]

C 가 $\mathbf{F}_q$ 우의 길이가 n 인 선형부호 즉 선형공간 $\mathbf{F}_q^n$ 의 부분공간이라고 하자. 이때 령이 아닌 원소 $\lambda(\in \boldsymbol{F}_q)$ 와 매 $(a_0,\ a_1,\ \cdots,\ a_{n-1})(\in C)$ 에 대하여 $(\lambda a_{n-1},\ a_0,\ \cdots,\ a_{n-2})\in C$ 이면 C 를 $\lambda-$ 일정순환부호라고 부른다. 특히 $\lambda=1$ 일 때 $\lambda-$ 일정순환부호를 순환부호, $\lambda=-1$ 일 때 $\lambda-$ 일정순환부호를 부순환부호라고 부른다.

$\lambda-$ 일정순환부호는 환 $\mathbf{F}_q[x]/<x^n-\lambda>$ 에서 $x^n-\lambda$ 의 유일한 모니크인수 $g(x)$ 에 의하여 생성된 이데알로 볼수 있다. 이 $g(x)$ 를 $\lambda-$ 일정순환부호의 생성다항식이라고 부른다.

또한 $\mathbf{F}_q$ (또는 $\mathbf{F}_{q^2}$)우의 선형부호 C 에 대하여

$$C^{\perp}:=\left\{(x_0,\ \cdots,\ x_{n-1})\in\mathbf{F}_q^n\ \middle|\ \sum_{i=0}^{n-1}x_ic_i=0,\ \forall(c_0,\ \cdots,\ c_{n-1})\in C\right\}$$

$$\left(\text{또는 } C^{\perp_H}:=\left\{(x_0,\ \cdots,\ x_{n-1})\in\mathbf{F}_{q^2}^n\ \middle|\ \sum_{i=0}^{n-1}x_ic_i^q=0,\ \forall(c_0,\ \cdots,\ c_{n-1})\in C\right\}\right)$$

를 C 의 유클리드(또는 에르미트)쌍대부호라고 부른다. 그리고 $C=C^{\perp}$ (또는 $C=C^{\perp_H}$)이면 C를 유클리드(또는 에르미트)자기쌍대부호라고 부른다.[6]

우선 선행연구[1]에서는 q 가 홀씨수의 제곱이고 l 이 q 와 서로 소인 홀씨수이며 m

이 정의 옹근수일 때 모듈 $4l^m$ 에 관한 $q-$원분합동류들을 얻고 길이가 $2l^m$ 인 유클리드자기쌍대부순환부호들전부를 다음과 같이 구성하였다.

$q\equiv 1\ (\bmod\ 4)$ 일 때 임의의 옹근수 $h(1\le h\le m)$ 에 대하여 $\mathrm{ord}_{l^h}(q)=\mathrm{ord}_{4l^h}(q)$ 가 성립한다. 여기서 $\mathrm{ord}_{l^h}(q)$ 는 모듈 l^h 에 관한 q 의 곱하기위수 즉 $q^f\equiv 1\ (\bmod\ l^h)$ 인 최소의 정의 옹근수 f 이다.

이제 $\lambda(h):=\mathrm{ord}_{l^h}(q),\ \delta(h):=\phi(l^h)/\lambda(h)$ 으로 놓자. 여기서 ϕ 는 오일러의 함수이다. 그리고 r 가 임의의 h 에 대하여 모듈 l^h 에 관한 원시뿌리이면서 $r\equiv 1\ (\bmod\ 4)$ 인 옹근수라고 하자.(이런 옹근수의 존재성은 선행연구[1]에서 밝혀짐.) 그러면 $q\equiv 1\ (\bmod\ 4)$ 일 때 모듈 $4l^m$ 에 관한 $q-$원분합동류들전부는 다음과 같다.

$$Cl_{0,q}=\{0\},\ Cl_{l^m,q}=\{l^m\},\ Cl_{-l^m,q}=\{-l^m\},\ Cl_{2l^m,q}=\{2l^m\}$$

$$Cl_{al^{m-h}r^k,q}=\{al^{m-h}r^k,\ al^{m-h}r^kq,\ \cdots,\ al^{m-h}r^kq^{\lambda(h)-1}\} \tag{1}$$

$$(a\in\{1,\ -1,\ 2,\ 4\},\ 1\le h\le m,\ 0\le k\le\delta(h)-1)$$

그리고 $\mathbf{F}_q$ 우에서 $x^{2l^m}+1$ 의 인수분해는 다음과 같다.

$$x^{2l^m}+1=M_{l^m,q}(x)M_{-l^m,q}(x)\prod_{h=1}^{m}\prod_{k=0}^{\delta(h)-1}M_{l^{m-h}r^k,q}(x)M_{-l^{m-h}r^k,q}(x) \tag{2}$$

따라서 길이가 $2l^m$ 인 부순환부호들전부는 다음과 같다.

$$\left\langle (M_{l^m,q}(x))^{\nu}(M_{-l^m,q}(x))^{\mu}\prod_{h=1}^{m}\prod_{k=0}^{\delta(h)-1}(M_{l^{m-h}r^k,q}(x))^{\alpha_{k,h}}(M_{-l^{m-h}r^k,q}(x))^{\beta_{k,h}}\right\rangle \tag{3}$$

여기서 $\nu,\ \mu,\ \alpha_{k,h},\ \beta_{k,h}\in\{0,\ 1\}\ (1\le h\le m,\ 0\le k\le\delta(h)-1)$ 이다.

또한 선행연구[4]에서는 유한체 $\mathbf{F}_q$ 의 2차확대체 $\mathbf{F}_{q^2}$ 우에서 에르미트자기쌍대부순환부호가 존재하기 위한 다음의 필요충분조건을 얻었다.

보조정리 1 어떤 홀수 n' 에 대하여 $\mathbf{F}_{q^2}$ 우의 길이가 $2^a n'$ 인 에르미트자기쌍대부순환부호가 존재하기 위하여서는 $q\not\equiv -1\ (\bmod\ 2^{a+1})$ 일것이 필요하고 충분하다.

또한 선행연구[7]에서는 선행연구[1]의 결과를 확장하여 l 이 홀씨수의 제곱 q 와 서로 소인 홀씨수일 때 길이가 $2^n l^m$ 인 유클리드자기쌍대 및 유클리드자기직교부순환부호들전부를 결정하였으며 선행연구[3]에서는 l 이 홀씨수의 제곱 q 와 서로 소인 홀씨수일 때 길이가 $2l^m p^s$ 인 중복뿌리유클리드자기쌍대일정순환부호들의 생성다항식과 그것들의 개수를 결정하였다.

한편 $\mathbf{F}_{q^2}$ 우의 상수항이 가역인 다항식 $f(x):=a_nx^n+a_{n-1}x^{n-1}+\ \cdots\ +a_1x+a_0\ (a_n\ne 0)$ 에 대하여

$$f^{\dagger}(x):=a_0^{-q}(a_0^qx^n+a_1^qx^{n-1}+\ \cdots\ +a_{n-1}^qx+a_n^q)$$

을 $f(x)$ 의 공액상반다항식이라고 부른다.[2]

또한 선행연구[6]에서는 $\mathbf{F}_{q^2}$ 우에서 길이가 n 인 부순환부호 C 의 생성다항식이 $g(x)$ 이면 그것의 에르미트쌍대부호 $C^{\perp_H}$ 도 부순환부호이며 그것의 생성다항식은 $h^{\dagger}(x)$ 라는

것이 밝혀졌다. 여기서 $h(x):=(x^n+1)/g(x)$ 이다.

이와 같이 선행연구에서는 에르미트자기쌍대부순환부호가 존재하기 위한 한가지 필요충분조건과 q 가 홀씨수의 제곱이고 l 이 q 와 서로 소인 홀씨수이며 p 가 유한체 $\mathbf{F}_q$ 의 표수일 때 길이가 $2^n l^m$ 인 단순뿌리유클리드자기쌍대부순환부호와 길이가 $2l^m p^n$ 인 중복뿌리유클리드자기쌍대부순환부호들의 생성다항식과 그것들의 개수에 대한 연구가 진행되였지만 에르미트스칼라적에 관해서는 이러한 부순환부호들이 구성되지 못하였다. 그러므로 론문에서는 l 과 q 에 대한 우와 같은 조건밑에서 $\mathbf{F}_q$ 의 2차확대체 $\mathbf{F}_{q^2}$ 우의 길이가 $2l^m$ 인 단순뿌리에르미트자기쌍대부순환부호들을 구성하고 그에 기초하여 길이가 $2l^m p^n$ 인 중복뿌리에르미트자기쌍대부순환부호들을 구성한 다음 이 부호들의 개수를 결정하였다.

우선 α 가 $\mathbf{F}_{q^2}$ 의 어떤 확대체에서 1의 원시 n 차뿌리이고 $M_{s,q^2}(x):=\prod_{i\in Cl_{s,q^2}}(x-\alpha^i)$ 이 α^s 의 최소다항식이라고 하자. 이때

$$M^{\dagger}_{s,q^2}(x)=\prod_{i\in Cl_{s,q^2}}(x-\alpha^{-qi})=M_{-qs,q^2}(x) \tag{4}$$

이다. 사실

$$M_{s,q^2}(x):=a_{n_s}x^{n_s}+a_{n_s-1}x^{n_s-1}+\cdots+a_1x+a_0$$

이고 β 가 $M_{s,q^2}(x)$ 의 뿌리라고 하면

$$\begin{aligned}M^{\dagger}_{s,q^2}(\beta^{-q})&=a_0^{-q}(a_0^q\beta^{-qn_s}+a_1^q\beta^{-q(n_s-1)}+\cdots+a_{n_s-1}^q\beta^{-q}+a_{n_s}^q)=\\&=a_0^{-q}\beta^{-qn_s}(a_{n_s}^q\beta^{qn_s}+a_{n_s-1}^q\beta^{q(n_s-1)}+\cdots+a_1^q\beta^q+a_0^q)=\\&=a_0^{-q}\beta^{-qn_s}(M_{s,q^2}(\beta))^q=0\end{aligned}$$

이므로 β^{-q} 은 $M^{\dagger}_{s,q^2}(x)$ 의 뿌리이고 따라서 식 (4)의 첫 등식이 나온다. 그리고 식 (4)의 둘째 등식은 정의로부터 분명하다.

다음으로 보조정리 1에 의하여 $q\equiv 3\ (\mathrm{mod}\ 4)$ 인 경우에는 $\mathbf{F}_{q^2}$ 우의 길이가 $2l^m$ 인 에르미트자기쌍대부순환부호가 존재하지 않으므로 $q\equiv 1\ (\mathrm{mod}\ 4)$ 이라고 가정하자. 이때 에르미트쌍대부호의 생성다항식을 얻기 위하여 모듈 $4l^m$ 에 관한 q^2-원분합동류들에서 대표원소의 새로운 표시를 구해보자.

임의의 옹근수 $h(1\le h\le m)$ 에 대하여 $\rho(h):=\mathrm{ord}_{l^h}(q^2)$ 으로 표시하자. 그러면 $\rho(h)$ 는 $\phi(l^h)$ 을 완제하므로 어떤 옹근수 $\theta(h)$ 에 의하여 $\phi(l^h)=\rho(h)\cdot\theta(h)$ 로 쓸수 있다. 그리고 임의의 홀수 q 에 대하여 $q^2\equiv 1\ (\mathrm{mod}\ 4)$ 이므로 식 (1)에 의하여 모듈 $4l^m$ 에 관한 q^2-원분합동류들전부는 다음과 같다.

$$Cl_{0,q^2}=\{0\},\ Cl_{l^m,q^2}=\{l^m\},\ Cl_{-l^m,q^2}=\{-l^m\},\ Cl_{2l^m,q^2}=\{2l^m\}$$

$$Cl_{al^{m-h}r^k,q^2}=\{al^{m-h}r^k,\ al^{m-h}r^kq^2,\ \cdots,\ al^{m-h}r^kq^{2(\rho(h)-1)}\}$$

$$(a\in\{1,\ -1,\ 2,\ 4\},\ 1\le h\le m,\ 0\le k\le\theta(h)-1)$$

보조정리 2 모듈 $4l^m$에 관한 q^2-원분합동류들사이에 다음의 관계식이 성립한다.

$$Cl_{bl^m,\,q^2}=Cl_{bql^m,\,q^2}\quad(b\in\{1,\ -1\})$$

증명 $q\equiv 1\pmod 4$이므로 어떤 옹근수 k가 있어서 $q=4k+1$이고 따라서

$$bql^m-bl^m=bl^m(q-1)=bl^m(4k+1-1)=4bl^mk$$

이다. 이것은 $j=0$일 때

$$bql^m\equiv bl^mq^{2j}\pmod{4l^m}$$

이 성립한다는것을 의미한다. 그러므로 보조정리의 결과가 성립한다.(증명끝)

정리 1 모듈 $4l^m$에 관한 q^2-원분합동류들전부는 다음과 같다.

$$Cl_{0,\,q^2}=\{0\},\ Cl_{l^m,\,q^2}=\{l^m\},\ Cl_{-ql^m,\,q^2}=\{-l^m\},\ Cl_{2l^m,\,q^2}=\{2l^m\},$$

$$\{Cl_{l^{m-h}r^k,\,q^2},\ Cl_{-ql^{m-h}r^k,\,q^2},\ Cl_{2l^{m-h}r^k,\,q^2},\ Cl_{4l^{m-h}r^k,\,q^2}\mid 1\le h\le m,\ 0\le k\le\theta(h)-1\}$$

증명 우선 원분합동류 $Cl_{-ql^{m-h}r^k,\,q^2}$과 $Cl_{al^{m-h}r^k,\,q^2}$이 서로 다르다는것을 밝히자. 여기서 $1\le h\le m,\ 0\le k\le\theta(h)-1,\ a\in\{1,\ 2,\ 4\}$이다.

어떤 $a(\in\{1,\ 2,\ 4\})$와 $1\le h_i\le m,\ 0\le k_i\le\theta(h_i)-1\,(i\in\{1,\ 2\})$인 어떤 $h_i,\ k_i$에 대하여

$$Cl_{al^{m-h_1}r^{k_1},\,q^2}=Cl_{-ql^{m-h_2}r^{k_2},\,q^2}$$

이라고 하자. 그러면 어떤 옹근수 j에 대하여

$$al^{m-h_1}r^{k_1}\equiv -q^{2j+1}l^{m-h_2}r^{k_2}\pmod{4l^m}$$

이므로

$$\gcd(al^{m-h_1}r^{k_1},\ 4l^m)=\gcd(-q^{2j+1}l^{m-h_2}r^{k_2},\ 4l^m)$$

이다. r와 q는 l과 서로 소인 홀수들이므로 $h_1=h_2,\ a=1$이다. 이로부터

$$l^{m-h_1}r^{k_1}\equiv -q^{2j+1}l^{m-h_1}r^{k_2}\pmod{4l^m}$$

이고

$$r^{k_1-k_2}\equiv -q^{2j+1}\pmod{4l^{h_1}}$$

이다. 즉

$$r^{k_1-k_2}\equiv -q^{2j+1}\pmod 4$$

이다. 조건 $q\equiv 1\pmod 4$와 $r\equiv 1\pmod 4$로부터 $1\equiv -1\pmod 4$이 나오는데 이것은 모순이다.

다음으로 원분합동류 $Cl_{-ql^{m-h}r^k,\,q^2}\ (1\le h\le m,\ 0\le k\le\theta(h)-1)$ 들이 서로 다르다는것을 밝히자. 이를 위하여 $1\le h_i\le m,\ 0\le k_i\le\theta(h_i)-1\,(i\in\{1,\ 2\})$인 어떤 $h_i,\ k_i$에 대하여

$$Cl_{-ql^{m-h_1}r^{k_1},\,q^2}=Cl_{-ql^{m-h_2}r^{k_2},\,q^2}$$

이라고 하자. 그러면 어떤 옹근수 j에 대하여

$$-ql^{m-h_1}r^{k_1}\equiv -q^{2j+1}l^{m-h_2}r^{k_2}\pmod{4l^m}$$

이고 우에서와 마찬가지로 $h_1=h_2$이므로

$$qr^{k_1}\equiv q^{2j+1}r^{k_2}\pmod{4l^{h_1}}$$

이다. 그리고 $\gcd(q,\ 4l^{h_1})=1$이므로

$$r^{k_1} \equiv q^{2j} r^{k_2} \pmod{4l^{h_1}}$$

즉

$$r^{k_1-k_2} \equiv q^{2j} \pmod{4l^{h_1}}$$

이다. 이 식의 량변을 $\rho(h_1)$ 제곱하면 다음과 같다.

$$r^{(k_1-k_2)\cdot\rho(h_1)} \equiv q^{2j\rho(h_1)} \pmod{4l^{h_1}}$$

따라서

$$r^{(k_1-k_2)\cdot\rho(h_1)} \equiv q^{2j\rho(h_1)} \pmod{l^{h_1}}$$

이다. 그런데

$$(q^2)^{\rho(h_1)} \equiv 1 \pmod{l^{h_1}}$$

이므로

$$r^{(k_1-k_2)\cdot\rho(h_1)} \equiv 1 \pmod{4l^{h_1}}$$

이다. r 가 모듈 l^{h_1} 에 관한 원시뿌리이므로 $\phi(l^{h_1}) \mid (k_1-k_2)\rho(h_1)$ 이고 $\phi(l^{h_1}) = \rho(h_1)\cdot\theta(h_1)$ 이므로 $\theta(h_1) \mid (k_1-k_2)$ 이다. 또한 $0 \le k_1,\ k_2 \le \theta(h_1)-1$ 이므로 $k_1 = k_2$ 이다. 그러므로 보조정리 2와 식 (1)로부터 정리의 결과가 나온다.(증명끝)

정리 2 $\mathbf{F}_{q^2}$ 우의 길이가 $2l^m$ 인 단순뿌리에르미트자기쌍대부순환부호들전부는 다음과 같다.

$$\left\langle (M_{l^m,\, q^2}(x))^{\nu} (M_{-ql^m,\, q^2}(x))^{1-\nu} \prod_{h=1}^{m} \prod_{k=0}^{\theta(h)-1} (M_{l^{m-h}r^k,\, q^2}(x))^{\mu_{k,h}} (M_{-ql^{m-h}r^k,\, q^2}(x))^{1-\mu_{k,h}} \right\rangle$$

그리고 이런 부호들의 개수는 $2^{1+\sum_{h=1}^{m}\theta(h)}$ 이다. 여기서 $\nu,\ \mu_{k,h} \in \{0,\ 1\}\ (1 \le h \le m,\ 0 \le k \le \delta(h)-1)$ 이다.

증명 C 가 $g(x)$ 를 생성다항식으로 가지는 길이가 $2l^m$ 인 $\mathbf{F}_{q^2}$ 우의 부순환부호라고 하자. 그러면 식 (3)과 정리 1로부터 C 의 생성다항식은 다음과 같다.

$$g(x) = \prod_{s\in S} (M_{s,\, q^2}(x))^{\varepsilon(s)}$$

여기서 $S = T \cup (-qT),\ T = \{l^m,\ l^{m-h}r^k \mid 1 \le h \le m,\ 0 \le k \le \theta(h)-1\}$ 이고 매 s 에 대하여 $\varepsilon(s) \in \{0,\ 1\}$ 이다. 이때 식 (2)로부터

$$h(x) = \frac{x^{2l^m}+1}{g(x)} = \prod_{s\in S} (M_{s,\, q^2}(x))^{1-\varepsilon(s)}$$

이고 식 (4)에 의하여 $C^{\perp_H}$ 의 생성다항식 $h^{\dagger}(x)$ 는 다음과 같다.

$$h^{\dagger}(x) = \prod_{s\in S} (M^{\dagger}_{s,\, q^2}(x))^{1-\varepsilon(s)} = \prod_{s\in S} (M_{-qs,\, q^2}(x))^{1-\varepsilon(s)} = \prod_{s\in S} (M_{s,\, q^2}(x))^{1-\varepsilon(-qs)}$$

또한 부호 C 가 에르미트자기쌍대부호이기 위하여서는 $\langle g(x)\rangle = \langle h^{\dagger}(x)\rangle$ 일것이 필요하고 충분하므로 임의의 $s(\in S)$ 에 대하여 $\varepsilon(s) = 1-\varepsilon(-qs)$ 즉 $\varepsilon(s)+\varepsilon(-qs) = 1$ 일것이 필요하고 충분하다. 이것은 임의의 $s(\in S)$ 에 대하여 $g(x)$ 의 인수분해에서 $M_{s,\, q^2}(x)$ 와 $M_{-qs,\, q^2}(x)$

의 제곱지수의 합이 1이여야 한다는것 즉 $M_{s,q^2}(x)$ 와 $M_{-qs,q^2}(x)$ 가운데서 오직 1개만이 나타나야 한다는것을 의미한다.

한편 모임 T 의 농도는 다음과 같다.

$$|T| = 1 + \sum_{h=1}^{m} \theta(h)$$

그러므로 $g(x)$ 는 $1+\sum_{h=1}^{m}\theta(h)$ 개의 기약인수들을 가지고 또 매 기약인수의 제곱지수는 0 또는 1이여야 한다. 따라서 $C^{\perp_H}$ 의 생성다항식은 0 또는 1을 취하는 ν 와 매 k, h 에 대하여 0 또는 1을 취하는 $\mu_{k,h}$ 가 있어서 다음과 같은 형태를 가진다.

$$(M_{l^m,q^2}(x))^{\nu}(M_{-ql^m,q^2}(x))^{1-\nu}\prod_{h=1}^{m}\prod_{k=0}^{\theta(h)-1}(M_{l^{m-h}r^k,q^2}(x))^{\mu_{k,h}}(M_{-ql^{m-h}r^k,q^2}(x))^{1-\mu_{k,h}}$$

그리고 이러한 부호들의 개수는 $2^{1+\sum_{h=1}^{m}\theta(h)}$ 이다.(증명끝)

이제는 길이가 $2l^m p^n$ 인 중복뿌리에르미트자기쌍대부순환부호를 구성해보자.

식 (2)와 정리 1로부터 $\mathbf{F}_{q^2}$ 우에서 $x^{2l^m p^n}+1$ 의 인수분해는 다음과 같다는것을 알수 있다.

$$\begin{aligned} x^{2l^m p^n}+1 &= (x^{2l^m}+1)^{p^n} = \\ &= (M_{l^m,q^2}(x))^{p^n}(M_{-ql^m,q^2}(x))^{p^n}\prod_{h=1}^{m}\prod_{k=0}^{\theta(h)-1}(M_{l^{m-h}r^k,q^2}(x))^{p^n}(M_{-ql^{m-h}r^k,q^2}(x))^{p^n} \end{aligned} \tag{5}$$

정리 3 $\mathbf{F}_{q^2}$ 우의 길이가 $2l^m p^n$ 인 중복뿌리에르미트자기쌍대부순환부호들전부는

$$\left\langle (M_{l^m,q^2}(x))^{\tau}(M_{-ql^m,q^2}(x))^{p^n-\tau}\prod_{h=1}^{m}\prod_{k=0}^{\theta(h)-1}(M_{l^{m-h}r^k,q^2}(x))^{\sigma_{k,h}}(M_{-ql^{m-h}r^k,q^2}(x))^{p^n-\sigma_{k,h}} \right\rangle$$

이고 이 부호들의 개수는 $(p^n+1)^{1+\sum_{h=1}^{m}\theta(h)}$ 이다. 여기서 $0\le\tau,\ \sigma_{k,h}\le p^n\ (1\le h\le m,\ 0\le k\le\theta(h)-1)$ 이다.

증명 $\mathbf{F}_{q^2}$ 우에서 길이가 $2l^m p^n$ 인 부순환부호 C 의 생성다항식은 식 (5)로부터 다음과 같다.

$$g(x) = \prod_{s\in S}(M_{s,q^2}(x))^{\varepsilon(s)}$$

여기서 $S = T\cup(-qT),\ T=\{l^m,\ l^{m-h}r^k \mid 1\le h\le m,\ 0\le k\le\theta(h)-1\}$, $0\le\varepsilon(s)\le p^n$ 이다. 따라서

$$h(x) = \frac{x^{2l^m p^n}+1}{g(x)} = \frac{\prod_{s\in S}(M_{s,q^2}(x))^{p^n}}{\prod_{s\in S}(M_{s,q^2}(x))^{\varepsilon(s)}} = \prod_{s\in S}(M_{s,q^2}(x))^{p^n-\varepsilon(s)}$$

이고 정리 2에서의 증명에서와 같이

$$h^{\dagger}(x)=\prod_{s\in S}(M^{\dagger}_{s,\,q^2}(x))^{p^n-\varepsilon(s)}=\prod_{s\in S}(M_{s,\,q^2}(x))^{p^n-\varepsilon(-qs)}$$

이라는것을 알수 있다. 또한 C 가 에르미트자기쌍대부호이기 위하여서는 $\langle g(x)\rangle=\langle h^{\dagger}(x)\rangle$ 일것이 필요하고 충분하므로 따라서 임의의 $s(\in S)$ 에 대하여

$$\varepsilon(s)=p^n-\varepsilon(-qs)$$

일것이 필요하고 충분하다. 이것은 $g(x)$ 의 인수분해에서 임의의 $s(\in S)$ 에 대하여 $M_{s,\,q^2}(x)$ 와 $M_{-qs,\,q^2}(x)$ 의 제곱지수의 합이 p^n 이여야 한다는것을 말해준다. 따라서 $C^{\perp_H}$ 의 생성다항식은 다음과 같다.

$$(M_{l^m,\,q^2}(x))^{\tau}(M_{-ql^m,\,q^2}(x))^{p^n-\tau}\prod_{h=1}^{m}\prod_{k=0}^{\theta(h)-1}(M_{l^{m-h}r^k,\,q^2}(x))^{\sigma_{k,\,h}}(M_{-ql^{m-h}r^k,\,q^2}(x))^{p^n-\sigma_{k,\,h}}$$

여기서 $0\le\tau,\ \sigma_{k,\,h}\le p^n\ (1\le h\le m,\ 0\le k\le\theta(h)-1)$ 이다. $\tau,\ \sigma_{k,\,h}$ 가 각각 p^n+1 개의 값을 가질수 있고 모임 T 의 농도는 $1+\sum_{h=1}^{m}\theta(h)$ 이므로 이런 부호들의 개수는 $(p^n+1)^{1+\sum_{h=1}^{m}\theta(h)}$ 이다. (증명끝)

참 고 문 헌

[1] G. K. Bakshi, M. Raka; Finite Fields Appl., 19, 39, 2013.
[2] A. Boripan et. al.; Finite Fields Appl., 55, 78, 2019.
[3] B. Chen et. al.; Finite Fields Appl., 33, 137, 2015.
[4] K. Guenda; Des. Codes Cryptogr., 62, 31, 2012.
[5] S. Ling, C. Xing; Coding Theory(A First Course) Cambridge University Press, 30～37, 2004.
[6] E. Sangwisut et. al.; Finite Fields Appl., 33, 232, 2015.
[7] A. Sharma; Discrete Math., 338, 576, 2015.

주체110(2021)년 3월 5일 원고접수

Repeated-Root Hermitian Self-Dual Negacyclic Codes of Length $2l^m p^n$ over a Finite Field

Ryang Myong Guk, Kim Ryul

In this paper, we construct all the simple-root Hermitian self-dual negacyclic codes of length $2l^m$ and the repeated-root Hermitian self-dual negacyclic codes of length $2l^m p^n$ over a finite field $\mathbf{F}_{q^2}$ of odd characteristic p and determine the number of such codes, where l is an odd prime different from p. Our study is based on a new observation about the complete set of representatives from distinct q^2 − cyclotomic cosets modulo $4l^m$.

Keywords: finite field, cyclotomic coset, self-dual negacyclic code