김일성종합대학학보 주체109(2020)년
수 학 제66권 제3호

길이가 $3p^s.2^k$ 인 중복뿌리 2 차원일정순환부호

김 률

λ_1과 λ_2를 체 $\mathbf{F}$의 령이 아닌 원소, $(x_0,\ x_1,\ \cdots,\ x_{m-1})$은 $\mathbf{F}^{nm}$($n,\ m$은 정의 옹근수)의 임의의 원소라고 하자. 여기서 매 $i\,(0\le i\le m-1)$에 대하여 $x_i=(x_{0,\ i},\ x_{1,\ i},\ \cdots,\ x_{n-1,\ i})\in\mathbf{F}^n$이다. 이때 $\mathbf{F}^{nm}$우의 순환밀기 $\tau^{0,\ 1}_{(\lambda_1,\ \lambda_2)}$과 $\tau^{1,\ 0}_{(\lambda_1,\ \lambda_2)}$을 다음과 같이 정의한다.

$$\tau^{0,\ 1}_{(\lambda_1,\ \lambda_2)}(x_0,\ x_1,\ \cdots,\ x_{m-1}):=(\lambda_2 x_{m-1},\ x_0,\ \cdots,\ x_{m-2})$$

$$\tau^{1,\ 0}_{(\lambda_1,\ \lambda_2)}(x_0,\ x_1,\ \cdots,\ x_{m-1}):=(x'_0,\ x'_1,\ \cdots,\ x'_{m-1})$$

여기서 $x'_i:=(\lambda_1 x_{n-1,\ i},\ x_{0,\ i},\ \cdots,\ x_{n-2,\ i})$이다. 또한 길이가 nm인 2차원선형부호 C가 조건

$$\tau^{0,\ 1}_{(\lambda_1,\ \lambda_2)}(C)=C,\ \tau^{1,\ 0}_{(\lambda_1,\ \lambda_2)}(C)=C$$

를 만족시킬 때 C를 $\mathbf{F}$우의 $(\lambda_1,\ \lambda_2)-$일정순환부호라고 부른다.[3] 부호단어의 다항식표시를 리용하면 유한체 $\mathbf{F}_q$ 우의 길이가 nm 인 2차원 $(\lambda_1,\ \lambda_2)-$ 일정순환부호는 환 $\mathbf{F}_q[x,\ y]/\langle x^n-\lambda_1,\ y^m-\lambda_2\rangle$의 이데알이다. 이 부호의 길이를 1차원부호의 길이와 구별하기 위하여 $n.m$(또는 $n\cdot m$)으로 표시한다.

선행연구[1]에서는 p가 홀씨수일 때 체 $\mathbf{F}_{p^m}$ 우의 길이가 $2p^s$(s는 정의 옹근수)인 중복뿌리일정순환부호를 구성하였으며 선행연구[2]에서는 p가 3이 아닌 씨수일 때 체 $\mathbf{F}_{p^m}$ 우의 길이가 $3p^s$인 중복뿌리일정순환부호를 구성하였다. 선행연구[3]에서는 선행연구[4]에서 제기한 2차원순환부호의 구성방법을 리용하여 p가 홀씨수일 때 체 $\mathbf{F}_{p^m}$ 우의 길이가 $2p^s.2^k$($s,\ k$는 정의 옹근수)인 중복뿌리2차원일정순환부호를 구성하였다.

론문에서는 p가 3이 아닌 홀씨수일 때 체 $\mathbf{F}_{p^m}$ 우의 길이가 $3p^s.2^k$인 중복뿌리2차원일정순환부호를 구성하였다.

ξ가 1의 원시(p^m-1)차뿌리라고 하자. 그러면

$$\mathbf{F}_{p^m}=\{0,\ \xi,\ \cdots,\ \xi^{p^m-1},\ \xi^{p^m-1}=\xi^0=1\}=\{0\}\cup\{\xi^k\mid k\in A\}$$

로 쓸수 있다. 여기서 $A:=\{0,\ 1,\ 2,\ \cdots,\ p^{m-2}\}$이다. A의 부분모임

$$A_0:=\{(3j)\ \mathrm{mod}\ (p^m-1)\mid j\in A\},\ A_1:=\{(3j+1)\ \mathrm{mod}\ (p^m-1)\mid j\in A\}$$

$$A_2:=\{(3j+2)\ \mathrm{mod}\ (p^m-1)\mid j\in A\}$$

에 대하여

$$\mathbf{A}_i:=\{\xi^j\mid j\in A_i\}\ \ (i=0,\ 1,\ 2)$$

로 놓자. 이때 $p^m\equiv 2\pmod 3$이면 $2p^m-1\equiv 0\pmod 3$이고

$$1\equiv p^m\equiv 2p^m-1\ (\mathrm{mod}\ (p^m-1))$$

이므로 $1\in A_0$ 이고 따라서 $A_0=A$ 이다. 이것은 $\mathbf{F}_{p^m}$ 의 령이 아닌 임의의 원소 Θ_0 이 어떤 $\theta_0\ (\in\mathbf{F}_{p^m})$ 이 존재하여 $\Theta_0=\theta_0^3$ 의 형태로 표시된다는것을 의미한다.

한편 $p^m\equiv 1\ (\text{mod } 3)$ 이면 $p^m-1\equiv 0\ (\text{mod } 3)$ 이므로 $A_0,\ A_1,\ A_2$ 는 비지 않은 모임들이고 A 의 분할을 이룬다. 따라서 이 경우에 다음의 식이 성립된다.

$$\mathbf{F}_{p^m}=\{0\}\cup\mathbf{A}_0\cup\mathbf{A}_1\cup\mathbf{A}_2$$

이제 $\Theta_0,\ \Theta_1,\ \Theta_2$ 가 각각 $\mathbf{A}_0,\ \mathbf{A}_1,\ \mathbf{A}_2$ 의 임의의 원소들이라고 하자. 그러면

$$\Theta_0=\theta_0^3,\ \Theta_1=\theta_1^3\xi,\ \Theta_2=\theta_2^3\xi^2$$

을 만족시키는 원소 $\theta_0,\ \theta_1,\ \theta_2\ (\in\mathbf{F}_{p^m})$ 가 존재한다.

보조정리 1 [2] 다음의 식을 만족시키는 $\mathbf{F}_{p^m}$ 의 원소 $\hat{\Theta}_0,\ \hat{\Theta}_1,\ \hat{\Theta}_2$ 이 존재한다.

$$\hat{\Theta}_0^{3p^s}=\Theta_0^{-1},\ \hat{\Theta}_1^{3p^s}=\Theta_1^{-1}\xi,\ \hat{\Theta}_2^{3p^s}=\Theta_2^{-1}\xi^2$$

보조정리 2 [3] 체 $\mathbf{F}_{p^m}$ 에서 $\gcd(p^m-1,\ 2^k)=j$ 이고 $\{\xi^j,\ \xi^{2j},\ \cdots,\ \xi^{\frac{p^m-1}{j}j}\}$ 의 원소 Δ 를 선택하면 $\delta^{2^k}=\Delta^{-1}$ 인 원소 $\delta\ (\in\mathbf{F}_{p^m})$ 가 존재한다.

보조정리 3 [4] C 를 길이가 $n:=s.2^k$ 인 2차원순환부호라고 하자. 그러면 C 에 대응하는 이데알 I 는 다음과 같은 생성다항식모임을 가진다.

$$I:=\left\langle p_1(x)\left(\sum_{i=0}^{2^k-1}y^i\right),\ p_2(x)\left(\sum_{i=0}^{2^k-1}(-1)^i y^i\right),\ p_3(x)\left(\sum_{i=0}^{2^{k-1}-1}(-1)^i y^{2i}\right),\ p_4(x)\left(\sum_{i=0}^{2^{k-2}-1}(-1)^i y^{4i}\right),\ \cdots\right.$$
$$\left.\cdots,\ p_{k+1}(x)\left(\sum_{i=0}^{2^1-1}(-1)^i y^{2^{k-1}i}\right)\right\rangle$$

여기서 $p_1(x),\ p_2(x),\ \cdots,\ p_{k+1}(x)$ 는 x^s-1 의 약수들이다.

보조정리 4 임의의 $\Theta_i\ (\in\boldsymbol{A}_i;\ i=0,\ 1,\ 2)$ 와 $\Delta\ (\in\{\xi^j,\ \xi^{2j},\ \cdots,\ \xi^{\frac{p^m-1}{j}j}\})$ 에 대하여 넘기기

$$\Phi_i:\frac{\mathbf{F}_{p^m}[x,\ y]}{\langle x^{3p^s}-\xi^i,\ y^{2^k}-1\rangle}\to\frac{\mathbf{F}_{p^m}[x,\ y]}{\langle x^{3p^s}-\Theta_i,\ y^{2^k}-\Delta\rangle}$$
$$f(x,\ y)\mapsto f(\hat{\Theta}_i x,\ \delta y)$$

는 환동형넘기기이다.

증명 만일

$$f(x,\ y)\equiv g(x,\ y)\ \ (\text{mod } \langle x^{3p^s}-\xi^i,\ y^{2^k}-1\rangle)$$

이라면 다항식 $h_1(x,\ y),\ h_2(x,\ y)\ (\in\mathbf{F}_{p^m}[x,\ y])$ 가 존재하여 다음의 식이 성립한다.

$$f(x,\ y)-g(x,\ y)=h_1(x,\ y)(x^{3p^s}-\xi^i)+h_2(x,\ y)(y^{2^k}-1)$$

따라서 보조정리 1, 2에 의하여 우의 식은 다음의 식과 동등하다.

$$f(\hat{\Theta}_i x,\ \delta y)-g(\hat{\Theta}_i x,\ \delta y)=h_1(\hat{\Theta}_i x,\ \delta y)((\hat{\Theta}_i x)^{3p^s}-\xi^i)+h_2(\hat{\Theta}_i x,\ \delta y)((\delta y)^{2^k}-1)=$$

$$= h_1(\hat{\Theta}_i x,\ \delta y)(\hat{\Theta}_i^{3p^s} x^{3p^s} - \xi^i) + h_2(\hat{\Theta}_i x,\ \delta y)(\delta^{2^k} y^{2^k} - 1) =$$
$$= \Theta_i^{-1} h_1(\hat{\Theta} x,\ \delta y)(\Theta_i \hat{\Theta}_i^{3p^s} x^{3p^s} - \Theta_i \xi^i) + \Delta^{-1} h_2(\hat{\Theta}_i x,\ \delta y)(\Delta \delta^{2^k} y^{2^k} - \Delta) =$$
$$= \Theta_i^{-1} \xi^i h_1(\hat{\Theta} x,\ \delta y)(x^{3p^s} - \Theta_i) + \Delta^{-1} h_2(\hat{\Theta}_i x,\ \delta y)(y^{2^k} - \Delta)$$

따라서

$$f(\hat{\Theta}_i x,\ \delta y) \equiv g(\hat{\Theta}_i x,\ \delta y) \pmod{\langle x^{3p^s} - \Theta_i,\ y^{2^k} - \Delta \rangle}$$

이다. 그러므로 Φ_i 는 잘 정의되며 1대1이다.

또한 Φ_i 가 환준동형넘기기라는것과 우로의 넘기기라는것은 분명하다.(증명끝)

우선 $p^m \equiv 2 \pmod 3$ 인 경우에 길이가 $3p^s.2^k$ 인 $\mathbf{F}_{p^m}$ 우의 2차원일정순환부호를 구성하자.

정리 1 $p^m \equiv 2 \pmod 3$ 일 때 $\mathbf{F}_{p^m}$ 의 령이 아닌 임의의 원소 Θ_0 과 임의의 $\Delta(\in \{\xi^j,\ \xi^{2j},\ \cdots,\ \xi^{\frac{p^m-1}{j}j}\})$ 에 대하여 길이가 $3p^s.2^k$ 인 $\mathbf{F}_{p^m}$ 우의 2차원$(\Theta_0,\ \Delta)-$일정순환부호는 다음과 같다.

$$C = \Bigg\langle (\hat{\Theta}_0 x - 1)^{a_1} (\hat{\Theta}_0^2 x^2 + \hat{\Theta}_0 x + 1)^{b_1} \left(\sum_{i=1}^{2^k-1} (\delta y)^i \right),\ (\hat{\Theta}_0 x - 1)^{a_2} (\hat{\Theta}_0^2 x^2 + \hat{\Theta}_0 x + 1)^{b_2} \left(\sum_{i=1}^{2^k-1} (-1)^i (\delta y)^i \right),$$
$$(\hat{\Theta}_0 x - 1)^{a_3} (\hat{\Theta}_0^2 x^2 + \hat{\Theta}_0 x + 1)^{b_3} \left(\sum_{i=1}^{2^{k-1}-1} (-1)^i (\delta y)^{2i} \right),\ (\hat{\Theta}_0 x - 1)^{a_4} (\hat{\Theta}_0^2 x^2 + \hat{\Theta}_0 x + 1)^{b_4} \left(\sum_{i=1}^{2^{k-2}-1} (-1)^i (\delta y)^{4i} \right),\ \cdots$$
$$\cdots,\ (\hat{\Theta}_0 x - 1)^{a_{k+1}} (\hat{\Theta}_0^2 x^2 + \hat{\Theta}_0 x + 1)^{b_{k+1}} \left(\sum_{i=1}^{2^1-1} (-1)^i (\delta y)^{2^{k-1} i} \right) \Bigg\rangle$$

여기서 $0 \le a_j,\ b_j \le p^s\ (j = 1,\ 2,\ \cdots,\ k+1)$ 이다.

증명 $p^m \equiv 2 \pmod 3$ 이면 $\mathbf{F}_{p^m}$ 에서 $x^2 + x + 1$ 은 기약이다. 그것은 $x^2 + x + 1$ 이 가약이라면 그것의 뿌리의 위수 3이 $p^m - 1$ 을 완제하기때문이다. 이로부터 $x^{3p^s} - 1$ 의 $\mathbf{F}_{p^m}$ 에서의 기약인수분해는 다음과 같다.

$$x^{3p^s} - 1 = (x-1)^{3p^s} (x^2 + x + 1)^{3p^s}$$

그러므로 보조정리 3에 의하여 길이가 $3p^s.2^k$ 인 2차원중복뿌리(1, 1)−일정순환부호는

$$C = \Bigg\langle (x-1)^{a_1} (x^2 + x + 1)^{b_1} \left(\sum_{i=1}^{2^k-1} y^i \right),\ (x-1)^{a_2} (x^2 + x + 1)^{b_2} \left(\sum_{i=1}^{2^k-1} (-1)^i y^i \right),$$
$$(x-1)^{a_3} (x^2 + x + 1)^{b_3} \left(\sum_{i=1}^{2^{k-1}-1} (-1)^i y^{2i} \right),\ (x-1)^{a_4} (x^2 + x + 1)^{b_4} \left(\sum_{i=1}^{2^{k-2}-1} (-1)^i y^{4i} \right),\ \cdots$$
$$\cdots,\ (x-1)^{a_{k+1}} (x^2 + x + 1)^{b_{k+1}} \left(\sum_{i=1}^{2^1-1} (-1)^i y^{2^{k-1} i} \right) \Bigg\rangle$$

이다. 여기서 $0\le a_j,\ b_j\le p^s\ (j=1,\ 2,\ \cdots,\ k+1)$이다. 이 식에 보조정리 4를 적용하면 결과가 나온다.(증명끝)

다음으로 $p^m\equiv 1\ (\mathrm{mod}\ 3)$인 경우에 길이가 $3p^s.2^k$인 $\mathbf{F}_{p^m}$우의 2차원일정순환부호를 구성하자.

$\Theta_i\in \boldsymbol{A}_i\ (i=0,\ 1,\ 2)$라고 하자. 그리고 $\gamma:=\xi^{(p^m-1)/3}$으로 놓자. 그러면 $\gamma^{-1}=\xi^{2(p^m-1)/3}$이고 $x^{3p^s}-1$은 $\mathbf{F}_{p^m}$에서 다음과 같이 기약인수분해된다.

$$x^{3p^s}-1=(x-1)^{p^s}(x-\gamma)^{p^s}(x-\gamma^{-1})^{p^s}$$

또한 s를 m으로 나눈 나머지를 r라고 할 때 $x^{3p^s}-\xi$와 $x^{3p^s}-\xi^2$은 $\mathbf{F}_{p^m}$에서 각각

$$x^{3p^s}-\xi=(x^3-\xi^{p^{m-r}})^{p^s},\quad x^{3p^s}-\xi^2=(x^3-\xi^{2p^{m-r}})^{p^s}$$

으로 기약인수분해된다.[2]

정리 2 $p^m\equiv 1\ (\mathrm{mod}\ 3)$이라고 하자. 그러면 임의의 $\Delta(\in\{\xi^j,\ \xi^{2j},\ \cdots,\ \xi^{\frac{p^m-1}{j}j}\})$에 대하여 길이가 $3p^s.2^k$인 $\mathbf{F}_{p^m}$우의 $(\Theta_0,\ \Delta)-$일정순환부호는

$$C=\left\langle(\hat{\Theta}_0x-1)^{a_1}(\hat{\Theta}_0x-\gamma)^{b_1}(\hat{\Theta}_0x-\gamma^{-1})^{c_1}\left(\sum_{i=1}^{2^k-1}(\delta y)^i\right),\right.$$

$$(\hat{\Theta}_0x-1)^{a_2}(\hat{\Theta}_0x-\gamma)^{b_2}(\hat{\Theta}_0x-\gamma^{-1})^{c_2}\left(\sum_{i=1}^{2^k-1}(-1)^i(\delta y)^i\right),$$

$$(\hat{\Theta}_0x-1)^{a_3}(\hat{\Theta}_0x-\gamma)^{b_3}(\hat{\Theta}_0x-\gamma^{-1})^{c_3}\left(\sum_{i=1}^{2^{k-1}-1}(-1)^i(\delta y)^{2i}\right),$$

$$(\hat{\Theta}_0x-1)^{a_4}(\hat{\Theta}_0x-\gamma)^{b_4}(\hat{\Theta}_0x-\gamma^{-1})^{c_4}\left(\sum_{i=1}^{2^{k-2}-1}(-1)^i(\delta y)^{4i}\right),\ \cdots$$

$$\left.\cdots,\ (\hat{\Theta}_0x-1)^{a_{k+1}}(\hat{\Theta}_0x-\gamma)^{b_{k+1}}(\hat{\Theta}_0x-\gamma^{-1})^{c_{k+1}}\left(\sum_{i=1}^{2^1-1}(-1)^i(\delta y)^{2^{k-1}i}\right)\right\rangle$$

이고(여기서 $0\le a_j,\ b_j,\ c_j\le p^s\ (j=1,\ 2,\ \cdots,\ k+1)$) $(\Theta_1,\ \Delta)-$일정순환부호는

$$C=\left\langle((\hat{\Theta}_1x)^3-\xi^{p^{m-r}})^{a_1}\left(\sum_{i=0}^{2^k-1}(\delta y)^i\right),\ ((\hat{\Theta}_1x)^3-\xi^{p^{m-r}})^{a_2}\left(\sum_{i=0}^{2^k-1}(-1)^i(\delta y)^i\right),\right.$$

$$((\hat{\Theta}_1x)x^3-\xi^{p^{m-r}})^{a_3}\left(\sum_{i=0}^{2^{k-1}-1}(-1)^i(\delta y)^{2i}\right),\ ((\hat{\Theta}_1x)x^3-\xi^{p^{m-r}})^{a_4}\left(\sum_{i=0}^{2^{k-2}-1}(-1)^i(\delta y)^{4i}\right),\cdots$$

$$\left.\cdots,\ ((\hat{\Theta}_1x)x^3-\xi^{p^{m-r}})^{a_{k+1}}\left(\sum_{i=0}^{2^1-1}(-1)^i(\delta y)^{2^{k-1}i}\right)\right\rangle$$

이며(여기서 $0 \le a_j \le p^s$ $(j=1,\ 2,\ \cdots,\ k+1)$) $(\Theta_2,\ \Delta)$ – 일정순환부호는

$$C = \left\langle ((\hat{\Theta}_2 x)^3 - \xi^{2p^{m-r}})^{a_1}\left(\sum_{i=0}^{2^k-1}(\delta y)^i\right),\ ((\hat{\Theta}_2 x)^3 - \xi^{2p^{m-r}})^{a_2}\left(\sum_{i=0}^{2^k-1}(-1)^i(\delta y)^i\right),\right.$$
$$((\hat{\Theta}_2 x)x^3 - \xi^{2p^{m-r}})^{a_3}\left(\sum_{i=0}^{2^{k-1}-1}(-1)^i(\delta y)^{2i}\right),\ ((\hat{\Theta}_2 x)x^3 - \xi^{2p^{m-r}})^{a_4}\left(\sum_{i=0}^{2^{k-2}-1}(-1)^i(\delta y)^{4i}\right),$$
$$\left.\cdots,\ ((\hat{\Theta}_2 x)x^3 - \xi^{2p^{m-r}})^{a_{k+1}}\left(\sum_{i=0}^{2^1-1}(-1)^i(\delta y)^{2^{k-1}i}\right)\right\rangle$$

이다.(여기서 $0 \le a_j \le p^s$ $(j=1,\ 2,\ \cdots,\ k+1)$)

증명 정리 1의 증명에서와 마찬가지로 $x^{3p^s}-1,\ x^{3p^s}-\xi,\ x^{3p^s}-\xi^2$ 의 기약인수분해식으로부터 보조정리 3을 리용하여 매 $i\,(=0,\ 1,\ 2)$ 에 대하여 길이가 $3p^s.2^k$ 인 2차원중복뿌리 $(\xi^i,\ 1)$ －일정순환부호들을 얻은 다음 보조정리 4를 적용하면 결과가 나온다.(증명끝)

참 고 문 헌

[1] H. Q. Dinh; Finite Fields Appl., 18, 133, 2012.
[2] H. Q. Dinh; Discrete Math., 313, 983, 2013.
[3] Z. Rajabi, K. Khashyarmanesh; Finite Fields Appl., 50, 122, 2018.
[4] Z. Sepasdar, K. Khashyarmanesh; Finite Fields Appl., 41, 97, 2016.

Repeated-Root Two-Dimensional Constacyclic Codes of Length $3p^s.2^k$

Kim Ryul

In terms of polynomial generators we obtain the algebraic structure of some repeated-root two-dimensional constacyclic codes of length $3p^s.2^k$ over a finite field $\mathbf{F}_{p^m}$, where p is an odd prime and $p \ne 3$.

Keywords: constacyclic code, finite field