김일성종합대학학보 주체107(2018)년
(수 학) 제64권 제1호

표수가 2인 유한체우에서 흔적과 선형화다항식을 리용한 몇가지 치환다항식의 구성법

김광연, 최수련

우리는 표수가 2인 유한체우에서 치환다항식의 구성법에 대하여 연구하였다.

최근에 흔적을 리용한 치환다항식의 구성에 대한 연구가 표수가 2인 유한체우에서도 많이 진행되고있다.

선행연구[2]에서는 $\mathbf{F}_{2^{2m}}$ 우에서 $(X^{2^m}+X+\delta)^s+X$ (여기서 $s\in\{2^{m+1}-1,\ 2^{m+1}+3\}$ 이다.)와 같은 형태의 치환다항식의 구성에 대하여 연구하였으며 선행연구[3]에서는 보다 일반적으로 표수가 2인 유한체우에서 흔적넘기기를 리용하여 구성된 $(Tr_{km/m}(X)+\delta)^s+X$, $(Tr_{km/m}(X)+\delta)^s+Tr_{km/m}(X)+X$ (여기서 l은 옹근수이고 k는 짝수이며 $s=(2^n-1)l/(2^m-1)+1$ 이다.), $(Tr_{4m/m}(X)+\delta)^s+X$ (여기서 $s=(2^{4m}-1)2^{m-2}/(2^m-1)+1$ 이다.), 그리고 $(Tr_{3m/m}(X)+\delta)^s+Tr_{3m/m}(X)+X$ (여기서 $s=(2^{3m}-1)/(2^m-1)+1$ 이다.)와 같은 형태의 다항식들이 치환다항식으로 되기 위한 충분조건들을 밝혔다.

론문에서는 흔적과 일반적인 선형화다항식을 리용하여 $\mathbf{F}_{2^m}$ 의 유한차확대체 $\mathbf{F}_{2^n}$ 우에서 $(Tr_{n/m}(X)+\delta)^s+L(X)$ 와 같은 형태를 가지면서 선행연구[3]에서의 치환다항식클라스보다 넓은 다항식클라스를 이루는 다항식들이 치환다항식으로 되기 위한 필요충분조건들을 유도하였다.

다음의 보조정리는 최근 치환다항식의 구성에 리용되는 중요한 결과이다.

보조정리 1 (AGW판정조건) A, S, $\overline{S}$ 를 유한모임이라고 하고 $|S|=|\overline{S}|$ 라고 하자. 그리고 넘기기 $\lambda:A\to S$, $\overline{\lambda}:A\to\overline{S}$ 들은 우로의 넘기기이고 넘기기 $f:A\to A$, $\overline{f}:S\to\overline{S}$ 는 $\overline{\lambda}\circ f=\overline{f}\circ\lambda$ 를 만족시키는 넘기기들이라고 하자. 그러면 다음의 사실들은 서로 동등하다.[1]

1) f는 A우의 치환이다.

2) $\overline{f}$ 는 우로의 1대1넘기기이며 f는 모든 $s(\in S)$에 대하여 $\lambda^{-1}(s)$ 우에서 1대1넘기기이다.

m이 정의 옹근수로서 3과 서로 소라고 하고 $p(X)=X^3+X+1$은 $\mathbf{F}_2$ 우에서 기약다항식이라고 하자. 이때 β를 $\mathbf{F}_{2^3}$ 에서의 $p(X)$의 임의의 뿌리라고 하면 임의의 원소 $x(\in\mathbf{F}_{2^{3m}})$는 $x=x_0+x_1\beta+x_2\beta^2$ 과 같은 형태로 유일하게 표시된다.(여기서 $x_i\in\mathbf{F}_{2^m}$ $(i\in\{0,\ 1,\ 2\})$이다.) 이때

$$\beta^{2^m}=\begin{cases}\beta^2 & (m\equiv 1\ (\mathrm{mod}\,3)\text{인 경우})\\ \beta^4 & (m\equiv 2\ (\mathrm{mod}\,3)\text{인 경우}\end{cases},\quad \beta^{2^{2m}}=\begin{cases}\beta^4 & (m\equiv 1\,(\mathrm{mod}\ 3)\text{인 경우})\\ \beta^2 & (m\equiv 2\,(\mathrm{mod}\ 3)\text{인 경우})\end{cases}$$

이 성립하고 $Tr_{3m/m}(\beta)=Tr_{3m/m}(\beta^2)=0$ 이 성립하므로 $Tr_{3m/m}(x)=x_0$ 이 성립한다.

보조정리 2 m이 3과 서로 소인 정의 옹근수일 때 모임

$$\Lambda := \{x \in \mathbf{F}_{2^{3m}} \mid (Tr_{3m/m}(x^2(x^{2^m} + x^{2^{2m}}))^2 = (Tr_{3m/m}(x^2 + x^{1+2^m}))^3\}$$

의 원소수는 $3 \cdot 2^{2m} - 2^{m+1}$ 이다.

보조정리 3 m이 3과 서로 소인 정의 옹근수이고 $p,\ q(\in \mathbf{F}_{2^m}^{\times})$가 $q^2 = p^3$을 만족시킨다고 하면 다항식 $x^3 + px + q$는 $\mathbf{F}_{2^m}$에서 뿌리를 가지지 않는다.

증명 $p,\ q \neq 0$이므로 방정식 $x^3 + px + q = 0$은 령풀이를 가지지 않는다. 이 방정식이 $\mathbf{F}_{2^m}^{\times}$에서 풀이 x를 가진다면 다음의 식이 성립한다.

$$1 + \frac{p}{x^2} + \frac{q}{x^3} = 0 \tag{1}$$

그런데 $q^2 / p^3 = 1$이므로 식 (1)을 다음과 같이 고쳐쓸수 있다.

$$1 + \frac{p}{x^2} + \frac{q}{x^3} = 1 + \frac{q^2}{p^3}\left(\frac{p}{x^2} + \frac{q}{x^3}\right) = 1 + \left(\frac{q}{px}\right)^2 + \left(\frac{q}{px}\right)^3 = 0 \tag{2}$$

따라서 $\mu := q/(px)$는 $X^3 + X^2 + 1$의 뿌리이며 $t := \mu + 1$은 $X^3 + X^2 + 1$의 $\mathbf{F}_{2^m}$에서의 뿌리이다. 그런데 이것은 다항식 $X^3 + X^2 + 1$이 $\mathbf{F}_{2^m}$에서 뿌리를 가지지 않는다는데 모순된다.(증명끝)

정리 1 m이 3과 서로 소인 정의 옹근수이고 δ를 보조정리 2에서 정의된 모임 Λ의 원소라고 하자. 그리고 $s := (2^{3m} - 1)/(2^m - 1) + 1$이라고 하면 다항식 $f(X) := (Tr_{3m/m}(X) + \delta)^s + Tr_{3m/m}(X) + X$는 $\mathbf{F}_{2^{3m}}$ 우에서 치환다항식이다.

증명 m과 s사이의 관계식으로부터

$$(s-1)(2^m - 1) = \frac{2^{3m} - 1}{2^m - 1}(2^m - 1) \equiv 0 \pmod{2^{3m} - 1}$$

이 성립하므로 임의의 $x(\in \mathbf{F}_{2^{3m}})$에 대하여 $(x^{s-1})^{2^m - 1} = 1$ 즉 x^{s-1}은 $\mathbf{F}_{2^m}$의 원소이다.

이제

$$\lambda(x) := Tr_{3m/m}(x) + \delta,\ \ \overline{\lambda}(x) := Tr_{3m/m}(x),\ \ g(x) := x^{s-1} Tr_{3m/m}(x)$$
$$S := \{\lambda(x) \mid x \in \mathbf{F}_{2^{3m}}\} = \{x + \delta \mid x \in \mathbf{F}_{2^m}\},\ \ \overline{S} = \{\overline{\lambda}(x) \mid x \in \mathbf{F}_{2^{3m}}\} = \mathbf{F}_{2^m}$$

으로 놓으면 임의의 $x(\in \mathbf{F}_{2^{3m}})$에 대하여

$$\begin{aligned}\overline{\lambda}(f(x)) &= Tr_{3m/m}((\mathrm{Tr}_{3m/m}(x) + \delta)^s) + Tr_{3m/m}(Tr_{3m/m}(x)) + Tr_{3m/m}(x) = \\ &= Tr_{3m/m}((\mathrm{Tr}_{3m/m}(x) + \delta)^s) = Tr_{3m/m}(\lambda^s(x)) = \\ &= \lambda^{s-1}(x)\mathrm{Tr}_{3m/m}(\lambda(x)) = g(\lambda(x))\end{aligned}$$

가 성립한다. 이때 AGW판정법으로부터 f가 $\mathbf{F}_{2^{3m}}$ 우에서 치환다항식이기 위하여서는 임의의 $z(\in S)$에 대하여 f가 $\lambda^{-1}(z)$우에서 1대1이고 g가 S를 $\overline{S}$에로 넘기는 우로의 1대1넘기기 즉 임의의 $y(\in \overline{S} = \mathbf{F}_{2^m})$에 대하여 $y = g(x + \delta)$인 $x(\in \mathbf{F}_{2^m})\ (x + \delta \in S)$가 유일존재할것이 필요하고 충분하다. 그런데 임의의 $z(\in S)$에 대하여 f는 분명히 $\lambda^{-1}(z)$우에서 1대1이라는것은 분명하다.

이제는 임의의 $y(\in \mathbf{F}_{2^m})$에 대하여 $y = g(x + \delta)$를 만족시키는 $x(\in \mathbf{F}_{2^m})$가 유일존재한다는것을 밝히면 된다. 여기서 $x + \delta \in S$이다.

$$y=g(x+\delta)=(x+\delta)^{s-1}Tr_{3m/m}(x+\delta)=(x+\delta)^{(2^{3m}-1)/(2^m-1)}(x+Tr_{3m/m}(\delta))=$$
$$=(x+\delta)(x+\delta^{2^m})(x+\delta^{2^{2m}})(x+\mathrm{Tr}_{3m/m}(\delta))=$$
$$=(x^3+Tr_{3m/m}(\delta)x^2+Tr_{3m/m}(\delta^{1+2^m})x+\delta^{s-1})(x+Tr_{3m/m}(\delta))=$$
$$=x^4+Tr_{3m/m}(\delta)x^3+Tr_{3m/m}(\delta^{1+2^m})x^2+\delta^{s-1}x+Tr_{3m/m}(\delta)x^3+$$
$$+(Tr_{3m/m}(\delta))^2x^2+Tr_{3m/m}(\delta)\mathrm{Tr}_{3m/m}(\delta^{1+2^m})x+Tr_{3m/m}(\delta)\delta^{s-1}=$$
$$=x^4+Tr_{3m/m}(\delta^{1+2^m}+\delta^2)x^2+(\delta^{2^{2m}+2^m+1}+Tr_{3m/m}(\delta)Tr_{3m/m}(\delta^{1+2^m}))x+Tr_{3m/m}(\delta)\delta^{s-1} \quad (3)$$

이 성립한다는것을 알수 있다. 그러면

$$\delta^{2^{2m}+2^m+1}+Tr_{3m/m}(\delta)Tr_{3m/m}(\delta^{1+2^m})=$$
$$=\delta^{2^{2m}+2^m+1}+(\delta^{2^{2m}+2^m+1}+\delta^{1+2\cdot 2^m}+\delta^{2+2^m}+\delta^{2^m+2\cdot 2^{2m}}+\delta^{2\cdot 2^m+2^{2m}}+$$
$$+\delta^{2^{2m}+2^m+1}+\delta^{1+2\cdot 2^{2m}}+\delta^{2^{2m}+2^m+1}+\delta^{2+2^{2m}})=$$
$$=Tr_{3m/m}(\delta^{2+2^m})+Tr_{3m/m}(\delta^{2+2^{2m}})=Tr_{3m/m}(\delta^2(\delta^{2^m}+\delta^{2^{2m}}))$$

이라는것을 고려하여 식 (3)을 다음과 같이 변형할수 있다.

$$y=x^4+Tr_{3m/m}(\delta^{1+2^m}+\delta^2)x^2+Tr_{3m/m}(\delta^2(\delta^{2^m}+\delta^{2^{2m}}))x+Tr_{3m/m}(\delta)\delta^{s-1}$$

그러므로 $y=g(x+\delta)$ 인 $x(\in\mathbf{F}_{2^m})$ 가 유일존재한다는것은

$$X^4+Tr_{3m/m}(\delta^{1+2^m}+\delta^2)X^2+Tr_{3m/m}(\delta^2(\delta^{2^m}+\delta^{2^{2m}}))X \quad (4)$$

가 $\mathbf{F}_{2^m}$ 에서 령뿌리만을 가진다는것과 동등하다. 그런데

$$X^4+Tr_{3m/m}(\delta^{1+2^m}+\delta^2)X^2+Tr_{3m/m}(\delta^2(\delta^{2^m}+\delta^{2^{2m}}))X=$$
$$=X(X^3+Tr_{3m/m}(\delta^{1+2^m}+\delta^2)X+Tr_{3m/m}(\delta^2(\delta^{2^m}+\delta^{2^{2m}})))$$

이므로 식 (4)가 $\mathbf{F}_{2^m}$ 에서 령뿌리만을 가지기 위해서는

$$X^3+Tr_{3m/m}(\delta^{1+2^m}+\delta^2)X+Tr_{3m/m}(\delta^2(\delta^{2^m}+\delta^{2^{2m}})) \quad (5)$$

가 $\mathbf{F}_{2^m}$ 에서 뿌리를 가지지 않을것이 필요하고 충분하다. 그런데 정리의 조건에 의하여

$$(Tr_{3m/m}(\delta^{1+2^m}+\delta^2))^3=(Tr_{3m/m}(\delta^2(\delta^{2^m}+\delta^{2^{2m}})))^2$$

이 성립하므로 보조정리 3으로부터 식 (5)는 $\mathbf{F}_{2^m}$ 에서 뿌리를 가지지 않는다. 따라서 임의의 $y(\in\overline{S}=\mathbf{F}_{2^m})$ 에 대하여 $y=g(x+\delta)$ 인 $x(\in\mathbf{F}_{2^m})$ 가 유일존재한다. 즉 g는 S를 $\overline{S}$ 에로 넘기는 우로의 1대1넘기기이다.(증명끝)

실례 1 $m=2$ 일 때 원시다항식 $X^6+X^5+X^3+X^2+1$ 을 리용하여 유한체 $\mathbf{F}_{2^6}$ 을 구성하고 $s=22$, $\delta=1$로 놓으면 정리 1에서와 같이 구성된 $(\mathrm{Tr}_{6/2}(X)+1)^{22}+\mathrm{Tr}_{6/2}(X)+X$ 는 $\mathbf{F}_{2^6}$ 우에서 치환다항식이라는것을 알수 있다.

선행연구[3]에서는 m이 3으로 완제되지 않는 정의 옹근수일 때 모임

$$\Omega:=\{x\in\mathbf{F}_{2^{3m}}\mid \mathrm{Tr}_{3m/m}(x^2(x^{2^m}+x^{2^{2m}}))=\mathrm{Tr}_{3m/m}(x^2+x^{1+2^m})=1\}$$

의 원소수가 $3\cdot 2^m$ 이라는것을 밝히고 Ω에 속하는 원소 δ에 대하여 다항식

$(Tr_{3m/m}+X)^s+Tr_{3m/m}(X)+X$ 가 $\mathbf{F}_{2^{3m}}$ 우에서 치환다항식이라는것을 밝혔다. 정리 1에서는 모임 Ω를 포함하는 보다 큰 모임 Λ의 원소 δ에 의하여 선행연구[3]에서와 같은 형태의 치환다항식을 구성할수 있다는것을 밝힘으로써 선행연구[3]에서 밝힌 치환다항식클라스를 넓혔다.

선행연구[3]에서는 m이 홀수이고 $n=4m$이라고 할 때 모임

$$\Gamma:=\{x\in\mathbf{F}_{2^n}\mid [\mathrm{Tr}_{n/m}(x^{2^m+1})+\mathrm{Tr}_{2m/m}(x^{2^{2m}+1})]^2=\mathrm{Tr}_{n/m}(x^{1+2^m+2^{2m}}),\ \mathrm{Tr}_{n/m}(x)=1\} \quad (6)$$

의 원소수가 $2^{2m}+1$이라는것과 $s=((2^n-1)2^{m-2})/(2^m-1)+1$일 때 Γ에 속하는 임의의 원소 δ에 대하여 다항식 $(Tr_{n/m}(X)+\delta)^s+X$ 가 $\mathbf{F}_{2^n}$우에서 치환다항식이라는것을 밝혔다. 이와 관련하여 다항식 $(Tr_{n/m}(X)+\delta)^s+X$ 가 $\mathbf{F}_{2^n}$ 우에서 치환다항식이면서 흔적이 1로 되게 하는 δ들은 Γ의 원소들뿐이라는 다음의 결과가 얻어졌다.

정리 2 m이 3이상인 홀수이고 $n=4m$, $s=((2^n-1)2^{m-2})/(2^m-1)+1$이며 $\delta(\in\mathbf{F}_{2^n})$가 $Tr_{n/m}(\delta)=1$을 만족시킬 때 다항식 $f(X)=(Tr_{n/m}(X)+\delta)^s+X$ 가 $\mathbf{F}_{2^n}$우에서 치환다항식이기 위하여서는 $\delta\in\Gamma$가 성립할것이 필요하고 충분하다.

증명 $\lambda(x)=\overline{\lambda}(x):=Tr_{n/m}(x)+\delta$, $g(x):=x^{s-1}Tr_{n/m}(x)+x$로 놓으면 $\mathbf{F}_{2^n}$의 모든 x에 대하여

$$\begin{aligned}\overline{\lambda}(f(x))&=Tr_{n/m}((\mathrm{Tr}_{n/m}(x)+\delta)^s+x)+\delta=\\&=Tr_{n/m}((\mathrm{Tr}_{n/m}(x)+\delta)^s)+Tr_{n/m}(x)+\delta=\\&=Tr_{n/m}(\lambda^s(x))+\lambda(x)=\lambda^{s-1}(x)Tr_{n/m}(\lambda(x))+\lambda(x)=g(\lambda(x))\end{aligned}$$

가 성립한다. 이제

$$S=\overline{S}:=\{\lambda(x)\mid x\in\mathbf{F}_{2^{3m}}\}=\{x+\delta\mid x\in\mathbf{F}_{2^m}\}$$

으로 놓자. 그러면 보조정리 1로부터 f가 $\mathbf{F}_{2^n}$ 우에서 치환다항식이기 위하여서는 임의의 $z(\in S)$에 대하여 f가 $\lambda^{-1}(z)$에서 1대1이며 $g:S\to\overline{S}$가 1대1일것이 필요하고 충분하다. 그런데 넘기기들의 구성으로부터 분명히 임의의 $z(\in S)$에 대하여 f는 $\lambda^{-1}(z)$우에서 1대1이다. 따라서 f가 $\mathbf{F}_{2^n}$우에서 치환다항식이라는것은 g의 1대1성과 동등하다는 결론이 얻어진다. 그런데 $\mathbf{F}_{2^m}$의 임의의 원소 x에 대하여

$$g(x+\delta)=(x+\delta)^{s-1}Tr_{n/m}(x+\delta)+(x+\delta)=(x+\delta)^{s-1}Tr_{n/m}(\delta)+(x+\delta)$$

가 성립하며 한편 $Tr_{n/m}(\delta)=1$이 성립하므로 $x,\ y(\in\mathbf{F}_{2^m})$가

$$y+\delta=g(x+\delta) \quad (7)$$

을 만족시킨다는것은

$$y=(x+\delta)^{s-1}Tr_{n/m}(\delta)+x=(x+\delta)^{((2^n-1)2^{m-2})/2^m-1}+x$$

가 성립한다는것과 같다. 이것은 또한

$$\begin{aligned}y^4&=(x+\delta)^{(2^n-1)2^m/(2^m-1)}+x^4=(x+\delta)^{1+2^m+2^{2m}+2^{3m}}+x^4=x^4+(\delta+\delta^{2^m}+\delta^{2^{2m}}+\delta^{2^{3m}})x^3+\\&+(\delta^{1+2^m}+\delta^{1+2^{2m}}+\delta^{1+2^{3m}}+\delta^{2^m+2^{2m}}+\delta^{2^m+2^{3m}}+\delta^{2^{2m}+2^{3m}})x^2+\\&+(\delta^{1+2^m+2^{2m}}+\delta^{1+2^m+2^{3m}}+\delta^{1+2^{2m}+2^{3m}}+\delta^{2^m+2^{2m}+2^{3m}})x+\delta^{1+2^m+2^{2m}+2^{3m}}+x^4=\\&=Tr_{n/m}(\delta)x^3+(Tr_{n/m}(\delta^{1+2^m})+Tr_{2m/m}(\delta^{1+2^{2m}}))x^2+Tr_{n/m}(\delta^{1+2^m+2^{2m}})x+\delta^{1+2^m+2^{2m}+2^{3m}}=\end{aligned}$$

$$= x^3 + (Tr_{n/m}(\delta^{1+2^m}) + Tr_{2m/m}(\delta^{1+2^{2m}}))x^2 + Tr_{n/m}(\delta^{1+2^m+2^{2m}})x + \delta^{1+2^m+2^{2m}+2^{3m}}$$

이 성립한다는것과 같다. 즉

$$\alpha = Tr_{n/m}(\delta^{1+2^m}) + Tr_{2m/m}(\delta^{1+2^{2m}}),\ \ \beta = Tr_{n/m}(\delta^{1+2^m+2^{2m}})$$

으로 놓으면

$$x^3 + \alpha x^2 + \beta x + \delta^{1+2^m+2^{2m}+2^{3m}} + y^4 = 0 \tag{8}$$

이 성립한다는것은 식 (7)이 성립한다는것과 같다. 따라서 임의의 $y(\in \mathbf{F}_{2^m})$에 대하여 방정식 (7)이 유일풀이를 가진다는것은 방정식 (8)이 유일풀이를 가진다는것과 동등하다.

이제 $z := x + \alpha$ 로 놓으면 방정식 (8)은

$$z^3 + (\alpha^2 + \beta)z + \alpha\beta + \delta^{(2^n-1)/(2^m-1)} + y^4 = 0 \tag{9}$$

으로 표시할수 있으며 이때 $\alpha^2 + \beta = 0$이면 방정식 (9)는

$$z^3 + \alpha\beta + \delta^{(2^n-1)/(2^m-1)} + y^4 = 0$$

으로 되는데 $\gcd(2^m - 1,\ 3) = 1$이므로 이 방정식은 유일풀이를 가진다.

다음으로 $\alpha^2 + \beta \neq 0$인 경우 식 (8)의 풀이가 유일하지 않다는것을 보기로 하자.

만일 $y := (\alpha\beta + \delta^{(2^n-1)/(2^m-1)})^{2^{m-2}}$ 으로 놓으면 $\alpha\beta + \delta^{(2^n-1)/(2^m-1)} + y^4 = 0$이 성립하고 이때 방정식 (9)는 $z^3 + (\alpha^2 + \beta)z = 0$으로 되는데 이 방정식의 풀이는 $z_1 = 0$과 $z_2 = (\alpha^2 + \beta)^{2^m-1}$으로서 이 방정식이 2개의 풀이를 가진다는것을 알수 있다. 즉 $\alpha^2 + \beta \neq 0$인 경우에는 어떤 $y(\in \mathbf{F}_{2^m})$에 대하여서는 방정식 (8)의 풀이가 유일하지 않으며 따라서 g가 1대1넘기기로 될 수 없다. 그러므로 g가 1대1넘기기이기 위하여서는 $\alpha^2 + \beta = 0$일것이 필요하고 충분하다. 이로부터 f의 $\mathbf{F}_{2^m}$ 우에서의 치환성은 $\alpha^2 + \beta = 0$이라는 조건과 동등하게 된다.(증명끝)

정리 3 $k,\ m \in \mathbf{N}$이고 k는 짝수이며 $n = km$이고 $s = (2^n - 1)l/(2^m - 1) + 1\ (l \in \mathbf{Z})$이라고 하자. 또한 $L(X)(\in \mathbf{F}_{2^m}[X])$는 선형화다항식이고 $\delta(\in \mathbf{F}_{2^n})$가 $\mathrm{Tr}_{n/m}(\delta) = 0$을 만족시킬 때 $f(X) := (Tr_{n/m}(X) + \delta)^s + L(X)$ 가 $\mathbf{F}_{2^n}$ 우에서 치환다항식이기 위하여서는 $L(X)$가 $T_0 := \{x \in \mathbf{F}_{2^n} \mid Tr_{n/m}(x) = 0\}$ 우에서 1대1일것이 필요하고 충분하다.

증명 임의의 $x(\in \mathbf{F}_{2^n})$에 대하여 $x^{s-1} = x^{((2^n-1)l)/(2^m-1)}$이므로 $x^{s-1} \in \mathbf{F}_{2^m}$이 성립한다. 그리고

$$\psi(x) := Tr_{n/m}(x) + \delta,\ \ \overline{\psi}(x) := Tr_{n/m}(x) + L(\delta),\ \ g(x) := L(x)$$

$$S := \{Tr_{n/m}(u) + \delta \mid u \in \mathbf{F}_{2^n}\} = \{u + \delta \mid u \in \mathbf{F}_{2^m}\}$$

$$\overline{S} := \{Tr_{n/m}(u) + L(\delta) \mid u \in \mathbf{F}_{2^n}\} = \{u + L(\delta) \mid u \in \mathbf{F}_{2^m}\}$$

으로 놓으면

$$\begin{aligned}\overline{\psi}(f(x)) &= Tr_{n/m}((Tr_{n/m}(x) + \delta)^s) + Tr_{n/m}(L(x)) + L(\delta) = \\ &= Tr_{n/m}((Tr_{n/m}(x) + \delta)^s) + L(Tr_{n/m}(x)) + L(\delta) = \\ &= Tr_{n/m}((Tr_{n/m}(x) + \delta)^s) + L(Tr_{n/m}(x) + \delta) =\end{aligned}$$

$$= (Tr_{m/n}(x)+\delta)^{s-1}(Tr_{n/m}(\mathrm{Tr}_{n/m}(x))+Tr_{n/m}(\delta))+L(Tr_{n/m}(x)+\delta)=$$
$$= L(\psi(x)) = g(\psi(x))$$

가 성립한다. 그러므로 f가 $\mathbf{F}_{2^n}$우에서 치환다항식이기 위하여서는 $g:S\to\overline{S}$가 1대1넘기기이고 임의의 $z(\in S)$에 대하여 f가 $\psi^{-1}(z)$우에서 1대1넘기기일것이 필요하고 충분하다. 그런데 임의의 $z(\in S)$와 임의의 $x,\ y(\in\psi^{-1}(z))$에 대하여

$$f(x)-f(y)=((Tr_{n/m}(x)+\delta)^s+L(x))-((Tr_{n/m}(y)+\delta)^s+L(y))=$$
$$=(z^s+L(x))-(z^s+L(y))=L(x-y)$$

가 성립하며 또한 임의의 $x,\ y$에 대하여

$$\psi(x)-\psi(y)=(Tr_{n/m}(x)+\delta)-(Tr_{n/m}(y)+\delta)=Tr_{n/m}(x-y)$$

가 성립하므로 $x,\ y\in\psi^{-1}(z)$라는것은 $x-y\in T_0$이라는것과 동등하며 따라서 f의 $\psi^{-1}(z)$우에서의 1대1성은 L의 T_0에서의 1대1성과 동등하다.

또한 $\mathbf{F}_{2^m}\subset T_0$이 성립하므로 g의 T_0에서의 1대1성은 g의 S우에서의 1대1성을 담보해준다. 그러므로 정리의 결과가 성립한다.(증명끝)

선행연구[3]에서는 정리 6에서와 같은 가정을 주고 다항식 $(Tr_{n/m}(X)+\delta)^s+X$, $(Tr_{n/m}(X)+\delta)^s+Tr_{n/m}(X)+X$ 들이 $\mathbf{F}_{2^n}$우에서 치환다항식이라는것을 밝혔다. 정리 3에서는 이것과 비교하여 X와 $Tr_{n/m}(X)+X$를 포함하는 일반적인 선형화다항식 $L(X)(\in\mathbf{F}_{2^m}[X])$를 리용함으로써 선행연구[3]에서의 치환다항식클라스보다 더 넓은 치환다항식클라스를 구성하였다.

정리 4 k와 n이 정의 옹근수이고 $n=4km$이며 δ는 $\mathbf{F}_{2^{2m}}$의 원소이고

$$s:=(2^n-1)l/(2^m+1)+1\ (l\in\mathbf{Z})$$

이라고 하자. 이때 선형화다항식 $L(X)(\in\mathbf{F}_{2^m}[X])$에 대하여 $f(X):=(Tr_{n/m}(X)+\delta)^s+L(X)$가 $\mathbf{F}_{2^n}$우에서 치환다항식이기 위하여서는 $L(X)$가

$$T_0:=\{x\in\mathbf{F}_{2^n}\mid Tr_{n/m}(x)=0\}$$

우에서 1대1일것이 필요하고 충분하다.

증명 정리 3에서 정의된 $\psi(x),\ \overline{\psi}(x),\ g(x),\ S,\ \overline{S}$를 생각하자. 그러면 임의의 $x(\in\mathbf{F}_{2^n})$에 대하여 $\overline{\psi}\circ f(x)=g\circ\psi(x)$가 성립하므로 보조정리 1에 의하여 f가 $\mathbf{F}_{2^n}$우의 치환다항식이기 위하여서는 임의의 $z(\in S)$에 대하여 f가 $\psi^{-1}(z)$우에서 1대1넘기기이고 g가 1대1넘기기일것이 필요하고 충분하다. 그런데 임의의 $z(\in S)$와 임의의 $x,\ y(\in\psi^{-1}(z))$에 대하여

$$f(x)-f(y)=((\mathrm{Tr}_{n/m}(x)+\delta)^s+L(x))-((\mathrm{Tr}_{n/m}(y)+\delta)^s+L(y))=$$
$$=(z^s+L(x))-(z^s+L(y))=L(x-y)$$

가 성립하므로 $\psi^{-1}(z)$우에서 f의 1대1성은 $\psi^{-1}(z)$우에서 L의 1대1성과 동등하다.

한편 임의의 $x,\ y(\in\psi^{-1}(z))$에 대하여 $x-y\in T_0$이 성립하며 T_0은 벡토르공간 $\mathbf{F}_{2^n}$의 부분벡토르공간이므로 $\psi^{-1}(z)$에서 L의 1대1이라는것은 T_0에서 L의 1대1성과 동등하다는 결론이 얻어진다.

또한 $\mathbf{F}_{2^n}$이 $\mathbf{F}_{2^m}$의 짝수차확대이므로 $\mathbf{F}_{2^m}\subset T_0$이며 g가 T_0우에서 1대1이면 $\mathbf{F}_{2^m}$우에

서도 1대1이고 따라서 S우에서도 1대1넘기기이다. 그러므로 f가 $\mathbf{F}_{2^n}$우에서 치환다항식이기 위하여서는 L이 T_0우에서 1대1일것이 필요하고 충분하다.(증명끝)

실례 2 $m=1$, $l=1$이라고 하고 원시다항식 X^4+X+1의 뿌리를 α라고 할 때 $s=6$이 되는데 이때 $\delta=1$로 놓으면 정리 4에서와 같은 형태로 구성되는 다항식 $(Tr(X)+1)^6+Tr(X)+X$ 는 다음의 표에서 알수 있는것처럼 $\mathbf{F}_{2^4}$우에서 치환다항식이다.

표. $(Tr(X)+1)^6+Tr(X)+X$ 의 다항식값

x	$f(x)$	x	$f(x)$	x	$f(x)$	x	$f(x)$
α	α^4	α^5	α^{10}	α^9	α^7	α^{13}	α^6
α^2	α^8	α^6	α^{13}	α^{10}	α^5	α^{14}	α^3
α^3	α^{14}	α^7	α^9	α^{11}	α^{12}	$\alpha^{15}=1$	0
α^4	α	α^8	α^2	α^{12}	α^{11}	0	$\alpha^{15}=1$

정리 7의 결과는 선행연구[3]에서 $n=4m$일 때 s와 δ에 대한 같은 가정을 주고 $\mathbf{F}_{2^n}$우에서 치환다항식 $(Tr_{n/m}(X)+\delta)^s+X$ 를 구성한 결과를 확대차수는 4의 배수로 일반화하고 X를 일반화한 선형화다항식 $L(X)(\in\mathbf{F}_{2^m}[X])$를 리용함으로써 역시 $(Tr_{n/m}(X)+\delta)^s+X$ 와 같은 형태의 보다 큰 클라스를 이루는 치환다항식들에로 확장시킨것으로 된다.

참 고 문 헌

[1] A. Akbary et al.; Finite Fields Appl., 17, 56, 2011.

[2] Z. Tu et al.; Finite Fields Appl., 31, 12, 2015.

[3] X. Zeng et al.; Finite Fields Appl., 35, 36, 2015.

주체106(2017)년 8월 10일 원고접수

Some Methods for Constructing Permutation Polynomials over Finite Fields of Characteristic 2 using the Trace and Linearized Polynomials

Kim Kwang Yon, Choe Su Ryon

In this paper, using the trace and linearized polynomials, we derive the necessary and sufficient conditions for the polynomials of the form $(Tr_{n/m}(X)+\delta)^s+L(X)$ to be permutation polynomials over the finite extension $\mathbf{F}_{2^n}$ of $\mathbf{F}_{2^m}$. These permutation polynomials constitute a large class including some of the previous permutation polynomials.

Key words: permutation polynomial, trace, linearized polynomial