김일성종합대학학보
수 학

주체109(2020)년
제66권 제1호

유한체우에서 몇가지 완전치환다항식들의 구성

김광연, 리영성

유한체우에서 새로운 치환다항식을 찾는 미해명문제를 해결하기 위한 많은 연구과정에 일련의 치환다항식과 완전치환다항식들이 얻어졌다.

완전치환다항식은 대체로 단항식들로서 선행연구[1]에서는 $\mathbf{F}_{2^{2k}}$ 우에서 $v^{-1}X^{2^k+2}$, 선행연구[2]에서는 $\mathbf{F}_{2^{2k}}$ 우에서 $v^{-1}X^{2^{k+1}+3}$, $v^{-1}X^{2^{k+2}(2^k+3)}$, $\mathbf{F}_{2^{3k}}$ 우에서 $v^{-1}X^{2^{2k}+2^k+2}$, $\mathbf{F}_{2^{2m}}$ 우에서 $v^{-1}X^{(2^{2m+1}+1)/3}$, 선행연구[4]에서는 $\mathbf{F}_{3^{2m}}$ 우에서 $v^{-1}X^{3^m+2}$, $v^{-1}X^{2\cdot 3^m+3}$ 형태의 완전치환단항식과 p가 홀씨수일 때 $\mathbf{F}_{p^{2m}}$ 우에서 $v^{-1}X^{s(p^m-1)+1}$ 모양의 완전치환단항식들이 얻어졌다.

한편 선행연구[3]에서는 표수가 2인 유한체 $\mathbf{F}_{q^n}$ 우에서 선형화다항식 $L(X)\in\mathbf{F}_q[X]$와 흔적을 리용하여 $X(L(\mathrm{Tr}(X))+u\cdot\mathrm{Tr}(X)+u(X)+vX$ 형태로 새로운 완전치환다항식을 구성하였다.

론문에서는 새로운 몇가지 완전치환다항식들을 구성하였다.

먼저 $q=2^{2m}$, $v\in\mathbf{F}_q^{\times}$, ξ 를 $\mathbf{F}_q$ 의 원시원소라고 하고 $D_0=<\xi^3>$, $D_1=\xi\cdot<\xi^3>$, $D_2=\xi^2\cdot<\xi^3>$, $\alpha=\xi^{(2^{2m}-1)/3}$ 이라고 하자.

보조정리 1 $f(X)=X^{(2^{2m}+2)/3}+vX$ 가 $\mathbf{F}_q$ 우에서 치환다항식이기 위하여서는 $v^3\neq 1$ 이고

$$\frac{\alpha+v}{1+v},\ \frac{1+v}{\alpha^2+v},\ \frac{\alpha^2+v}{\alpha+v}\notin D_2$$

일것이 필요하고 충분하다.

$g(X)=X^{(2^{2m}+2)/3}+v^2X$ 일 때 다항식 $f(X)=X^{(2^{2m}+2)/3}+vX$ 가 치환다항식이라는것은 $f^2(X)=X^{2\cdot(2^{2m}+2)/3}+v^2X^2$ 이 치환다항식이라는것과 동등하다. 그리고 $f^2(X)=g(X^2)$ 이고 X^2이 치환다항식이므로 $f(X)$가 치환다항식이라는것은 $g(X)$가 치환다항식이라는것과 동등하다.

또한 $x\notin D_2$ 이기 위하여서는 $x^4\notin D_2$ 일것이 필요하고 충분하다.

따름 1 $X^{(2^{2m}+2)/3}+vX$ 가 $\mathbf{F}_q$ 우에서 치환다항식이기 위하여서는 $X^{(2^{2m}+2)/3}+\alpha vX$ 가 치환다항식일것이 필요하고 충분하다.

이제 $u:=1+\alpha/(1+v)$ 라고 놓자.

보조정리 2 $f(X)=X^{(2^{2m}+2)/3}+vX$ 가 우에서 치환다항식이기 위하여서는 $v^3\neq 1$ 이면서 $\alpha^2u,\ \alpha(u+1)\in D_0$ 이거나 $\alpha^2u\in D_1,\ \alpha(u+1)\in D_2$ 일것이 필요하고 충분하다.

따름 2 $m\not\equiv 2\pmod 3$ 일 때 $u\in D_1,\ u+1\in D_2,\ v^3\neq 1$ 이면 $f(X)=X^{(2^{2m}+2)/3}+vX$ 는

$\mathbf{F}_q$ 우에서 치환다항식이다.

정리 1 $v^{-1}X^{(2^{2m}+2)/3}$이 $\mathbf{F}_q$ 우에서 완전치환단항식이기 위하여서는 $m\not\equiv 2 \pmod 3$, $v^3\neq 1$이고 $\alpha^2u,\ \alpha(u+1)\in D_0$ 또는 $\alpha^2u\in D_1,\ \alpha(u+1)\in D_2$가 성립할것이 필요하고 충분하다.

증명 $m\not\equiv 2 \pmod 3$이면 $\gcd\left(\frac{2^{2m}+2}{3},\ 2^{2m}-1\right)=1$이므로 $v^{-1}X^{(2^{2m}+2)/3}$은 $\mathbf{F}_q$ 우에서 치환다항식이다.

$v^{-1}X^{(2^{2m}+2)/3}$가 $\mathbf{F}_q$ 우에서 치환다항식이면

$$\gcd\left(\frac{2^{2m}+2}{3},\ 2^{2m}-1\right)=1$$

이 성립하므로 $m\not\equiv 2 \pmod 3$이 성립한다.

다음으로 $v^{-1}X^{(2^{2m}+2)/3}+X$가 $\mathbf{F}_q$ 우에서 치환다항식이기 위하여서는 $X^{(2^{2m}+2)/3}+vX$가 $\mathbf{F}_q$ 우에서 치환다항식일것이 필요하고 충분하며 따라서 $v^3\neq 1$과 $\alpha^2u,\ \alpha(u+1)\in D_0$ 또는 $\alpha^2u\in D_1,\ \alpha(u+1)\in D_2$가 성립할것이 필요하고 충분하다.(증명끝)

아핀3항식과 흔적을 리용하여 새로운 완전치환다항식들에 대한 구성법을 보기로 하자.

정리 2 $\mathbf{F}_{q^2}$의 표수가 홀씨수일 때 임의의 $\delta\in\mathbf{F}_q$에 대하여 다항식

$$f(X)=(X^q+X+\delta)^{(q^2-1)/2+q}-X^q$$

은 $\mathbf{F}_{q^2}$에서의 완전치환다항식이다.

증명 먼저 $S=\{x^q+x+\delta\mid x\in\mathbf{F}_{q^2}\},\ \overline{S}=\{x^q+x-\delta\mid x\in\mathbf{F}_{q^2}\}$으로 놓자. 그러면 $\delta\in\mathbf{F}_q$이므로 $S=\overline{S}=\mathbf{F}_q$이다. 이제 다음과 같은 넘기기

$$\varphi:\mathbf{F}_{q^2}\ni x\mapsto x^q+x+\delta\in S,\ \psi:\mathbf{F}_{q^2}\ni x\mapsto x^q+x-\delta\in\overline{S},\ h:S\ni x\mapsto x\in\overline{S}$$

들을 정의하면 임의의 $x\in\mathbf{F}_{q^2}$에 대하여

$$\psi\circ f(x)=(x^q+x+\delta)^{(q^2-1)/2+q}+(x^q+x+\delta)^{(q^2-1)/2+1}-x^q-x-\delta$$

가 성립한다. 그런데 $x^q+x+\delta\in\mathbf{F}_q$이므로 $(x^q+x+\delta)^{(q^2-1)/2}$은 0 또는 1이며

$$(x^q+x+\delta)^{(q^2-1)/2+1}=(x^q+x+\delta)^{(q^2-1)/2+q}=x^q+x+\delta$$

이고 따라서

$$\psi\circ f(x)=2(x^q+x+\delta)-x^q-x-\delta=x^q+x+\delta=h\circ\varphi(x)$$

가 성립한다는것을 알수 있다.

이때 $f(X)$가 $\mathbf{F}_{q^2}$에서의 치환다항식이기 위하여서는 임의의 $s\in S$에 대하여 $\varphi^{-1}(s)$우에서 $f(x)$가 1：1이고 $h(x)$가 S우에서 1：1일것이 필요하고 충분하다. 그런데 임의의 $s\in S$에 대하여 $\varphi^{-1}(s)$우에서는

$$f(x)=(x^q+x+\delta)^{(q^2-1)/2+q}-x^q=s^{(q^2-1)/2+q}-x^q$$

이므로 $f(x)$는 1：1이다.

그리고 S의 임의의 원소 x에 대하여 $h(x)=x$ 이므로 넘기기 $h(x)$는 1：1넘기기이므로 다항식 $f(X)$가 $\mathbf{F}_{q^2}$ 에서의 치환다항식이라는 결론을 얻는다.

다음으로 다항식 $f(X)+X=g(X)$ 도 역시 $\mathbf{F}_{q^2}$ 에서의 치환다항식이라는것을 류사한 방법으로 증명할수 있다.(증명끝)

다음은 표수가 2인 유한체의 홀수차확대체우에서 흔적을 리용하여 새로운 형태의 한 가지 완전치환다항식구성법에 대하여 보기로 하자.

정리 3 $\alpha\in\mathbf{F}_{2^n}$, $\mathrm{Tr}(\alpha)=1$일 때 정의 옹근수 m, n과 부아닌 옹근수 k가

$$2\nmid n,\ \gcd(k+m,\ n)=1$$

을 만족시키면

$$f(X)=X^{2^{k+m}}+(\alpha^{2^m}+1)\mathrm{Tr}(X^{2^k})$$

은 $\mathbf{F}_{2^n}$ 우에서 완전치환다항식이다.

증명 $\mathbf{F}_{2^n}$ 우에서 다항식 $f(X)$가 치환다항식이기 위해서는 $\mathbf{F}_{2^n}$의 임의의 령이 아닌 원소 λ에 대하여 $\sum_{x\in\mathbf{F}_{2^n}}(-1)^{\mathrm{Tr}(\lambda\cdot f(x))}=0$ 일것이 필요하고 충분하다.

또한

$$\sum_{x\in\mathbf{F}_{2^n}}(-1)^{\mathrm{Tr}(\lambda\cdot f(x))}=\sum_{x\in\mathbf{F}_{2^n}}(-1)^{\mathrm{Tr}(\lambda\cdot x^{2^{k+m}}+\lambda(\alpha^{2^m}+1)\mathrm{Tr}(x^{2^k}))}=$$

$$=\begin{cases}\sum_{x\in\mathbf{F}_{2^n}}(-1)^{\mathrm{Tr}(\lambda\cdot x^{2^{k+m}})}, & \mathrm{Tr}(\lambda(\alpha^{2^m}+1))=0\\ \sum_{x\in\mathbf{F}_{2^n}}(-1)^{\mathrm{Tr}(\lambda\cdot x^{2^{k+m}}+x^{2^k})}, & \mathrm{Tr}(\lambda(\alpha^{2^m}+1))=1\end{cases}$$

이 성립한다. $\mathrm{Tr}(\lambda(\alpha^{2^m}+1))=0$ 이면 $\gcd(2^n-1,\ 2^{k+m})=1$ 이므로 $X^{2^{k+m}}$ 은 $\mathbf{F}_{2^n}$ 에서의 치환다항식이기때문에

$$\sum_{x\in\mathbf{F}_{2^n}}(-1)^{\mathrm{Tr}(\lambda\cdot x^{2^{k+m}})}=0$$

이 성립한다. 만일 $\mathrm{Tr}(\lambda\cdot(\alpha^{2^m}+1))=1$ 이면

$$\mathrm{Tr}(\lambda\cdot x^{2^{k+m}}+x^{2^k})=\mathrm{Tr}(\lambda\cdot x^{2^{k+m}}+x^{2^{k+m}})=\mathrm{Tr}((\lambda+1)\cdot x^{2^{k+m}})$$

이다. 이제 $\lambda=1$이면 $1=\mathrm{Tr}(\alpha^{2^m}+1)=\mathrm{Tr}(\alpha+1)=0$ 이므로 $\lambda=1$일수 없다. 즉 $\lambda+1\neq 0$이고 따라서 $(\lambda+1)X^{2^{k+m}}$ 은 $\mathbf{F}_{2^n}$ 에서의 치환다항식이므로

$$\sum_{x\in\mathbf{F}_{2^n}}(-1)^{Tr(\lambda\cdot f(x))}=0$$

이 성립한다. 그러므로 $f(X)$는 $\mathbf{F}_{2^n}$ 에서의 치환다항식이다.

다음으로 $f(X)+X$가 $\mathbf{F}_{2^n}$ 에서의 치환다항식이라는것을 밝히자.

$$\sum_{x\in\mathbf{F}_{2^n}}(-1)^{\mathrm{Tr}(\lambda\cdot(f(x)+x))}=\sum_{x\in\mathbf{F}_{2^n}}(-1)^{\mathrm{Tr}(\lambda\cdot x^{2^{k+m}}+\lambda(\alpha^{2^m}+1)\mathrm{Tr}(x^{2^k})+\lambda\cdot x)}=$$

$$=\sum_{x\in\mathbf{F}_{2^n}}(-1)^{\mathrm{Tr}((\lambda+\lambda^{2^{k+m}})x^{2^{k+m}})+\mathrm{Tr}(\lambda(\alpha^{2^m}+1))\mathrm{Tr}(x^{2^k})}=$$

$$=\begin{cases}\sum_{x\in\mathbf{F}_{2^n}}(-1)^{\mathrm{Tr}((\lambda+\lambda^{2^{k+m}})x^{2^{k+m}})}, & \mathrm{Tr}(\lambda(\alpha^{2^m}+1))=0\\ \sum_{x\in\mathbf{F}_{2^n}}(-1)^{\mathrm{Tr}((\lambda+\lambda^{2^{k+m}}+1)x^{2^{k+m}})}, & \mathrm{Tr}(\lambda(\alpha^{2^m}+1))=1\end{cases}$$

이 성립한다. $\gcd(n,\ k+m)=1$이므로 $\gcd(2^n-1,\ 2^{k+m}-1)=1$이며 따라서 임의의 령이 아닌 원소 $\lambda\in\mathbf{F}_{2^n}$에 대하여 $\lambda^{2^{k+m}-1}\neq 1$ 즉 $\lambda+\lambda^{2^{k+m}}\neq 0$이다.

또한 $\mathrm{Tr}(\lambda+\lambda^{2^{k+m}}+1)=\mathrm{Tr}(1)=1$이므로 역시 임의의 령이 아닌 원소 $\lambda\in\mathbf{F}_{2^n}$에 대하여 $\lambda+\lambda^{2^{k+m}}+1\neq 0$이다. 이로부터 임의의 령이 아닌 원소 $\lambda\in\mathbf{F}_{2^n}$에 대하여 $(\lambda+\lambda^{2^{k+m}})X^{2^{k+m}}$과 $(\lambda+\lambda^{2^{k+m}}+1)X^{2^{k+m}}$은 다같이 $\mathbf{F}_{2^n}$에서의 치환다항식이다. 그러므로

$$\sum_{x\in\mathbf{F}_{2^n}}(-1)^{\mathrm{Tr}(\lambda\cdot f(x)+x)}=0$$

이 성립한다. 따라서 $f(X)+X$는 $\mathbf{F}_{2^n}$에서의 치환다항식이다.(증명끝)

참 고 문 헌

[1] P. Charpin et al.; SIAM J. Discrete Math., 22, 2, 650, 2008.
[2] Z. Tu et al.; Finite Fields Appl., 25, 182. 2014.
[3] B. Wu et al.; Discrete Applied Mathematics, 184, 213, 2015.
[4] G. Wu et al.; Finite Fields Appl., 31, 228, 2015.

주체108(2019)년 9월 15일 원고접수

Construction of Several Complete Permutation Polynomials over Finite Fields

Kim Kwang Yon, Ri Yong Song

In this paper, we construct complete permutation monomials, complete permutation polynomials of the form $X^{2^{k+m}}+(\alpha^{2^m}+1)\mathrm{Tr}(X^{2^k})$ over finite extensions of a finite field of characteristic 2 and complete permutation polynomials of the form $(X^q+X+\delta)^{(q^2-1)/2+q}-X^q$ over quadratic extensions of finite fields of odd characteristic.

Keywords: complete permutation polynomial, permutation polynomial