김일성종합대학학보
수 학

주체110(2021)년
제67권 제2호

유한체의 2차확대체우에서 세가지 형태의 완전치환다항식들의 구성

홍예성, 김광연

일반적으로 다항식 $f(X)\in\mathbf{F}_q[X]$에 의하여 정의되는 넘기기 $f:\mathbf{F}_q\ni x\mapsto f(x)\in\mathbf{F}_q$가 치환이면 $f(X)$를 $\mathbf{F}_q$우에서의 치환다항식이라고 부르고 다항식 $f(X)+X$ 까지도 $\mathbf{F}_q$우에서 치환다항식이면 $f(X)$를 $\mathbf{F}_q$우에서의 완전치환다항식이라고 부른다.

유한체에 대한 연구과정에 치환다항식과 완전치환다항식이 발견되여 연구가 심화되였으며 특히 클루스터만합항등식을 유도하기 위하여 $(X^2+X+\delta)^{-2^l}+X$ 형태의 치환다항식을 리용한것을 계기로 하여 $L(X)$가 선형화다항식일 때 $(X^{p^i}-X+\delta)^s+L(X)$ 형태의 치환다항식 또는 완전치환다항식에 대한 연구는 관심을 끄는 문제의 하나로 되였다.

선행연구[5]에서는 $s=i(p^m\pm1)+p^j$일 때 특정한 a, b에 대하여 다음과 같은 형태의 완전치환다항식을 구성하였다.

$$(X^{p^m}-X+\delta)^s+aX^{p^m}+bX$$

한편 흔적을 리용한 완전치환다항식의 구성도 진행되고있는데 선행연구[1]에서는 $\mathbf{F}_{2^n}$우에서 $X^{2^{k+m}}+(\alpha^{2^m}+1)\mathrm{Tr}(X^{2^k})$ 형태의 완전치환다항식을, 선행연구[4]에서는 $\mathbf{F}_{p^{mn}}$우에서 $a\in\mathbf{F}_{p^m}^{\times}$, $G(X)\in\mathbf{F}_{p^m}[X]$일 때 $aX^{p^r}+X(G(\mathrm{Tr}_{mn/m}(X))-a\mathrm{Tr}_{mn/m}(X)^{p^r-1})$ 형태의 완전치환다항식을 구성하였다.

선행연구[6]에서는 $(X^q-X+\delta)^s+cX$ $(s\in\{(3q^2+2q-1)/4,\ (q+1)^2/4\})$ 형태로 $\mathbf{F}_{q^2}$우에서의 치환다항식들을 구성하였다.

치환다항식들을 구성하기 위한 연구과정에 다음의 판정법들이 얻어졌다.

보조정리 [2] A, S와 $\overline{S}$를 $|S|=|\overline{S}|$인 유한모임들이라고 하고 $f:A\to A$, $\lambda:A\to S$, $\overline{\lambda}:A\to\overline{S}$와 $h:S\to\overline{S}$는 $\overline{\lambda}\circ f=h\circ\lambda$를 만족시키는 넘기기들이라고 할 때 λ와 $\overline{\lambda}$가 다같이 우로의 넘기기라면 다음의 주장들은 서로 동등하다.

① f는 A의 치환이다.

② h는 1:1이며 f는 임의의 $s\in S$에 대하여 $\lambda^{-1}(s)$에서 1:1이다.

정리 1[3] $f(X)\in\mathbf{F}_q[X]$일 때 $f(X)$가 $\mathbf{F}_q$우에서 치환다항식이기 위하여서는 임의의 $a\in\mathbf{F}_q^{\times}$에 대하여 $\sum_{x\in\mathbf{F}_q}\xi_p^{\mathrm{Tr}_{q/p}(af(x))}=0$일것이 필요하고 충분하다. 여기서 $p=\mathrm{char}(\mathbf{F}_q)$이고 $\xi_p=e^{2\pi i/p}$이다.

론문에서는 이 판정법들을 리용하여 유한체의 2차확대체우에서 $(X^q-X+\delta)^i+aX^q$, $(X^q-X+\delta)^i+aX$ 형태의 완전치환다항식을 얻는다. 여기서 i는 짝수이다.

또한 흔적을 리용하여 $X^{2^{k+m}}+(\gamma+\gamma^{2^m}+\gamma^{2^{k+m}}+1)\mathrm{Tr}((\gamma+\gamma^{2^k}+\gamma^{2^{n-m}})X^{2^k})$ 형태로 표수가

2인 유한체우에서 완전치환다항식을 구성한다.

정리 2 i는 짝수이고 $\delta\in\mathbf{F}_{q^2}$, $\mathrm{Tr}_{q^2/q}(\delta)=0$이며 $q\geq 4$이라고 하자.

이때 $f(X)=(X^q-X+\delta)^i+aX^q$, $a\in\mathbf{F}_q\setminus\{0,\ 1,\ -1\}$은 $\mathbf{F}_{q^2}$우에서 완전치환다항식이다.

증명 먼저 $f(X)$가 $\mathbf{F}_{q^2}$우에서 치환다항식이라는것을 증명하자.

$T_0:=\{x\in\mathbf{F}_{q^2}\mid \mathrm{Tr}(x)=0\}$으로 놓고 넘기기 φ, h를 $\varphi:\mathbf{F}_{q^2}\to T_0$, $x\mapsto x^q-x$, $h:=-a\cdot id_{T_0}$으로 정의하면 임의의 $x\in\mathbf{F}_{q^2}$에 대하여

$$\varphi\circ f(x)=(x^q-x+\delta)^{iq}+ax-(x^q-x+\delta)^i-ax^q=-a(x^q-x)=h\circ\varphi(x)$$

$$\begin{array}{ccc}\mathbf{F}_{q^2} & \xrightarrow{f} & \mathbf{F}_{q^2}\\ \varphi\downarrow & & \downarrow\varphi\\ T_0 & \xrightarrow{h} & T_0\end{array}$$

가 성립된다. 즉 도식 은 가환도식이다.

h는 분명히 1：1이므로 $f(X)$가 치환다항식이라는것을 밝히자면 임의의 $s\in T_0$에 대하여 $f(x)$가 $\varphi^{-1}(s)$에서 1：1이라는것을 밝히면 충분하다. 그런데 임의의 $s\in T_0$과 $x\in\varphi^{-1}(s)$에 대하여 $f(x)=(s+\delta)^i+ax^q$이므로 $\varphi^{-1}(s)$에서 $f(x)$는 1：1이다.

그러므로 $f(X)$는 $\mathbf{F}_{q^2}$우에서 치환다항식이다.

다음으로 $g(X)=f(X)+X$가 $\mathbf{F}_{q^2}$우에서 치환다항식이라는것을 밝히자.

$\overline{h}=(1-a)id_{T_0}$으로 정의하면 임의의 $x\in\mathbf{F}_{q^2}$에 대하여 $\varphi\circ g(x)=(1-a)(x^q-x)=\overline{h}\circ\varphi(x)$가 성립된다. 따라서 가정으로부터 $1-a\neq 0$이므로 $\overline{h}$는 1：1이다.

임의의 $s\in T_0$과 $x,\ y\in\varphi^{-1}(s)$에 대하여 $g(x)=g(y)$이면 $ax^q+x=ay^q+y$가 성립된다.

한편 $x^q-x=y^q-y$이므로 $(1+a)x=(1+a)y$이고 가정으로부터 $1+a\neq 0$이므로 $x=y$이다. 결과적으로 임의의 $s\in T_0$에 대하여 $\varphi^{-1}(s)$우에서 $g(x)$는 1：1이다.

그러므로 $g(X)$도 역시 $\mathbf{F}_{q^2}$우에서 치환다항식이다.(증명끝)

실례 1 $\mathbf{F}_5$우에서 원시다항식 $p(X)=X^2+X+2$를 택하고 α를 그것의 뿌리라고 하면 $\delta=\alpha^3$, $a=2$으로 택하였을 때 $\mathrm{Tr}(\delta)=0$이며 다항식

$$f(X)=(X^5-X+\delta)^4+2X^5 \tag{1}$$

은 $\mathbf{F}_{25}$우에서 완전치환다항식이다. $f(X)$와 $g(X)=(X^5-X+\delta)^4+2X^5+X$의 다항식값들은 표 1과 같다.

표 1. 식 (1)의 다항식값들

x	$f(x)$	$f(x)+x$	x	$f(x)$	$f(x)+x$	x	$f(x)$	$f(x)+x$	x	$f(x)$	$f(x)+x$	x	$f(x)$	$f(x)+x$
α	α^4	α^3	α^6	α^{18}	0	α^{11}	α^5	α^{23}	α^{16}	α^{14}	α^{19}	α^{21}	α^{15}	α^9
α^2	α^{23}	α	α^7	α^{17}	α^8	α^{12}	α^6	α^{24}	α^{17}	α^9	α^{13}	α^{22}	α^{16}	α^{10}
α^3	α^7	α^{14}	α^8	α^{13}	α^{21}	α^{13}	α^{21}	α^{17}	α^{18}	0	α^{18}	α^{23}	α	α^4
α^4	α^3	α^{20}	α^9	α^{22}	α^7	α^{14}	α^8	α^2	α^{19}	α^2	α^{16}	α^{24}	α^{24}	α^6
α^5	α^{20}	α^{15}	α^{10}	α^{19}	α^5	α^{15}	α^{11}	α^{22}	α^{20}	α^{10}	α^{11}	0	α^{12}	α^{12}

4는 $i(5\pm1)+5^j$ 형태로 표시되지 않으므로 이 다항식은 선행연구[5]에서 밝힌 형태의 완전치환다항식이 아니다.

정리 3 i는 짝수이고 $\delta\in\mathbf{F}_{q^2}$, $\mathrm{Tr}_{q^2/q}(\delta)=0$이며 $q\geq4$이라고 하자.

이때 $f(X)=(X^q-X+\delta)^i+aX$ $a\in\mathbf{F}_q\setminus\{0,\ -1\}$은 $\mathbf{F}_{q^2}$우에서 완전치환다항식이다.

증명 $T_0:=\{x\in\mathbf{F}_{q^2}\,|\,\mathrm{Tr}(x)=0\}$으로 놓고 넘기기 φ를 $\varphi:\mathbf{F}_{q^2}\to T_0,\ x\mapsto x^q-x$로 정의하고 먼저 $f(X)$가 $\mathbf{F}_{q^2}$우에서 치환다항식이라는것을 밝히자.

$h:=a\cdot id_{T_0}$로 정의하면 임의의 $x\in\mathbf{F}_{q^2}$에 대하여

$$\varphi\circ f(x)=(x^q-x+\delta)^{iq}+ax^q-(x^q-x+\delta)^i-ax=a(x^q-x)=h\circ\varphi(x)$$

가 성립된다. h는 분명히 1：1이다. 그러므로 $f(X)$가 $\mathbf{F}_{q^2}$우에서 치환다항식이기 위하여서는 임의의 $s\in T_0$에 대하여 $f(x)$가 $\varphi^{-1}(s)$에서 1：1일것이 필요하고 충분하다.

그런데 임의의 $s\in T_0$과 $x\in\varphi^{-1}(s)$에 대하여 $f(x)=(s+\delta)^i+ax$이므로 $\varphi^{-1}(s)$에서 $f(x)$는 1：1이다. 따라서 $f(X)$는 $\mathbf{F}_{q^2}$우에서 치환다항식이다.

다음으로 $g(X)=f(X)+X$가 $\mathbf{F}_{q^2}$우에서 치환다항식이라는것을 밝히자.

$\bar{h}=(a+1)\cdot id_{T_0}$으로 정의하면 임의의 $x\in\mathbf{F}_{q^2}$에 대하여 $\varphi\circ g(x)=(a+1)(x^q-x)=\bar{h}\circ\varphi(x)$가 성립된다. 가정에 의하여 $a+1\neq0$이므로 $\bar{h}$는 1：1이다.

그리고 우에서와 마찬가지로 임의의 $s\in T_0$에 대하여 $g(x)$가 $\varphi^{-1}(s)$우에서 1：1이라고 볼수 있다.

그러므로 $g(X)$도 $\mathbf{F}_{q^2}$우에서 치환다항식이다.(증명끝)

정리 4 n은 짝수이고 $q=2^n$이며 k와 m은 정의웅근수들로서 $\gcd(k+m,\ n)=1$이라고 하자. 그리고 $\mathrm{Tr}(\gamma)=1$이라고 하자.

그러면

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

은 $\mathbf{F}_q$우에서 완전치환다항식이다. 여기서 Tr는 $\mathbf{F}_q$의 절대흔적이다.

증명 먼저 $f(X)$가 $\mathbf{F}_q$우에서 치환다항식이라는것을 밝히자.

$f(X)$가 치환다항식이기 위해서는 임의의 $\lambda\in\mathbf{F}_q^\times$에 대하여

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

일것이 필요하고 충분하다.

이 등식을 증명하자.

$\mathrm{Tr}(\lambda(\gamma+\gamma^{2^m}+\gamma^{2^{k+m}}+1))=0$인 경우에는 $\sum_{x\in\mathbf{F}_q}(-1)^{\mathrm{Tr}(\lambda\cdot f(x))}=\sum_{x\in\mathbf{F}_q}(-1)^{\mathrm{Tr}(\lambda x^{2^{k+m}})}$이 성립된다.

그런데 $\gcd(k+m,\ n)=1$이므로 $\lambda x^{2^{k+m}}$은 $\mathbf{F}_q$우에서 치환다항식이다.

따라서 $\sum_{x\in\mathbf{F}_q}(-1)^{\mathrm{Tr}(\lambda\cdot f(x))}=0$이 성립된다.

$\mathrm{Tr}(\lambda(\gamma+\gamma^{2^m}+\gamma^{2^{k+m}}+1))=1$ 인 경우에는 $\sum_{x\in\mathbf{F}_q}(-1)^{\mathrm{Tr}(\lambda\cdot f(x))}=\sum_{x\in\mathbf{F}_q}(-1)^{\mathrm{Tr}((\lambda+\gamma^{2^m}+\gamma^{2^{k+m}}+\gamma)x^{2^{k+m}})}$ 이 성립된다.

이때 $\lambda+\gamma^{2^m}+\gamma^{2^{k+m}}+\gamma=0$ 이라고 하면 $\mathrm{Tr}(\lambda(\gamma+\gamma^{2^m}+\gamma^{2^{k+m}}+1))=\mathrm{Tr}(\lambda^2+\lambda)=0$ 이므로 이것은 모순이다. 따라서 $\lambda+\gamma^{2^m}+\gamma^{2^{k+m}}+\gamma\neq 0$ 이고 $(\lambda+\gamma^{2^m}+\gamma^{2^{k+m}}+\gamma)x^{2^{k+m}}$ 은 $\mathbf{F}_q$ 우에서 치환다항식이며 $\sum_{x\in\mathbf{F}_{2^n}}(-1)^{\mathrm{Tr}(\lambda\cdot f(x))}=0$ 이 성립된다.

그러므로 $f(X)$ 는 $\mathbf{F}_q$ 우에서 치환다항식이다.

다음 $f(X)+X$ 가 $\mathbf{F}_q$ 우에서 치환다항식이라는것을 밝히자.

역시 임의의 $\lambda\in\mathbf{F}_q^{\times}$에 대하여

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

이라는것을 증명하자.

$\mathrm{Tr}(\lambda(\gamma+\gamma^{2^m}+\gamma^{2^{k+m}}+1))=0$ 인 경우에는 $\sum_{x\in\mathbf{F}_q}(-1)^{\mathrm{Tr}(\lambda\cdot(f(x)+x))}=\sum_{x\in\mathbf{F}_q}(-1)^{\mathrm{Tr}((\lambda+\lambda^{2^{k+m}})x^{2^{k+m}})}$ 이 성립된다.

만일 $\lambda+\lambda^{2^{k+m}}=0$ 이면 $\lambda\neq 0$ 이므로 $\lambda^{2^{k+m}-1}=1$ 이 성립한다.

그런데 $\gcd(k+m,\ n)=1$ 이므로 $\gcd(2^{k+m}-1,\ 2^n-1)=1$ 이고 따라서 $X^{2^{m+k}-1}$ 은 $\mathbf{F}_q$ 우에서 치환다항식이므로 $\lambda=1$ 이다.

그러면 $\mathrm{Tr}(\lambda(\gamma+\gamma^{2^m}+\gamma^{2^{m+k}}+1))=\mathrm{Tr}(\gamma)+\mathrm{Tr}(1)=\mathrm{Tr}(\gamma)=1$ 이 성립되는데 이것은 가정에 모순이다. 그러므로 $\lambda+\lambda^{2^{k+m}}\neq 0$ 이고 $(\lambda+\lambda^{2^{k+m}})X^{2^{k+m}}$ 은 $\mathbf{F}_q$ 우에서 치환다항식이며 따라서 $\sum_{x\in\mathbf{F}_q}(-1)^{Tr(\lambda\cdot(f(x)+x))}=0$ 이 성립된다.

$\mathrm{Tr}(\lambda(\gamma+\gamma^{2^m}+\gamma^{2^{k+m}}+1))=1$ 인 경우에는

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

이 성립된다. 만일 $\lambda+\gamma^{2^m}+\gamma^{2^{k+m}}+\gamma+\lambda^{2^{k+m}}=0$ 이면

$$0=\mathrm{Tr}(\lambda+\lambda^{2^{k+m}}+\gamma+\gamma^{2^m}+\gamma^{2^{k+m}})=\mathrm{Tr}(\gamma+\gamma^{2^m}+\gamma^{2^{k+m}})=\mathrm{Tr}(\gamma)$$

가 얻어지는데 이것은 가정에 모순이다.

그러므로 $\lambda+\gamma^{2^m}+\gamma^{2^{k+m}}+\gamma+\lambda^{2^{k+m}}\neq 0$ 이고 $(\lambda+\gamma^{2^m}+\gamma^{2^{k+m}}+\gamma+\lambda^{2^{k+m}})X^{2^{k+m}}$ 은 $\mathbf{F}_q$ 우에서 치환다항식이며 따라서

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

이 성립한다. 그러므로 $f(X)+X$ 는 $\mathbf{F}_q$ 우에서 치환다항식이다.(증명끝)

선행연구[1, 4]에서는 각각 n이 홀수일 때 $\mathbf{F}_{2^n}$ 우에서 $X^{2^{k+m}}+(\alpha^{2^m}+1)\mathrm{Tr}(X^{2^k})$, 일반적인 $\mathbf{F}_{p^{mn}}$ 우에서 $aX^{p^r}+X(G(\mathrm{Tr}_{mn/m}(X))-a\mathrm{Tr}_{mn/m}(X)^{p^r-1})$ 형태의 완전치환다항식들을 론의하였는데 론문에서는 n이 홀수이고 흔적은 절대흔적이며 결수가 붙은 X^{2^k} 에 대한 절대흔적인 것으로 하여 선행연구[1, 4]에서 론의한 형태의 완전치환다항식은 아니라는것을 알수 있다.

실례 2 $\mathbf{F}_2$ 우에서 원시다항식 $p(X)=X^4+X+1$을 택하고 α를 그것의 뿌리라고 하자. 그리고 $\gamma=\alpha^3$, $m=2$, $k=3$으로 택하였을 때 $\mathrm{Tr}(\gamma)=1$이며 다항식

$$f(X)=X^{2^{k+m}}+(\gamma+\gamma^{2^m}+\gamma^{2^{k+m}}+1)\mathrm{Tr}((\gamma+\gamma^{2^k}+\gamma^{2^{n-m}})X^{2^k}) \qquad (2)$$

는 $\mathbf{F}_{16}$ 우에서 완전치환다항식이다.

$f(X)$ 와 $g(X)=X^{2^{k+m}}+(\gamma+\gamma^{2^m}+\gamma^{2^{k+m}}+1)\mathrm{Tr}((\gamma+\gamma^{2^k}+\gamma^{2^{n-m}})X^{2^k})+X$ 의 다항식값들은 표 2와 같다.

표 2. 식 (2)의 다항식값들

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

참 고 문 헌

[1] **김일성**종합대학학보 수학, 66, 1, 9, 주체109(2020).

[2] A. Akbary et al.; Finite Fields Appl., 17, 51, 2011.

[3] L. Li et al.; Finite Fields Appl., 55, 177, 2019.

[4] A. Tuxanidy et al.; Discrete Appl. Math., 217, 318, 2017.

[5] X. Xu et al.; Finite Fields Appl., 57, 309, 2019.

[6] D. Zheng et al.; Finite Fields Appl., 56, 1, 2019.

주체109(2020)년 12월 5일 원고접수

Construction of Three Classes of Complete Permutation Polynomials over the Quadratic Extension of a Finite Field

Hong Ye Song, Kim Kwang Yon

We propose two classes of complete permutation polynomials with the form $(x^{p^m}-x+\delta)^i+ax^q$ and $(x^{p^m}-x+\delta)^i+ax$ over $\mathbf{F}_{p^{2m}}$ by the AGW criterion for even i.

Also a class of complete permutation polynomial with the form

$$X^{2^{m+k}}+(\gamma+\gamma^{2^m}+\gamma^{2^{m+k}}+1)\mathrm{Tr}((\gamma+\gamma^{2^k}+\gamma^{2^{n-m}})X^{2^k})$$

over $\mathbf{F}_{2^n}$ is constructed.

Keywords: complete permutation polynomial, AGW criterion