유한체의 2차확대에서 두가지 치환다항식구성방법

리영성, 김광연

선행연구에 의하여 흔적다항식과 선형화다항식 등을 리용하는 치환다항식구성법들이 여러가지로 연구되였다.

새로운 치환다항식을 구성하기 위한 선행연구과정에 한가지 새로운 판정조건이 얻어졌다.

론문에서는 선행연구에서 밝혀진 치환다항식구성을 위한 한가지 판정조건에 근거하여 $\mathbf{F}_{q^2}$ 우에서

$$(aX^q+X+\delta)^{(q^2-1)/2+1}-aX^q,\ (X^q+aX+\delta)^{(q^2-1)/2+q}-aX$$

형태의 새로운 치환다항식들을 고찰하려고 한다.

보조정리 1[1] A, S 와 $\overline{S}$ 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 하자. 이때 λ 와 $\overline{\lambda}$ 가 다같이 우로의 넘기기라면 다음의 주장들은 서로 동등하다.

① f 는 A의 치환이다.

② h는 1대1이며 f는 임의의 $s\in S$에 대하여 $\lambda^{-1}(s)$ 에서 1대1이다.

선행에서 연구된 적지 않은 치환다항식구성법들이 이 판정조건에 의하여 통합화되며 그런데로부터 치환다항식을 새로 얻기 위하여 이 판정조건을 리용하려는 시도들이 많이 제기되고있다. 선행연구[1]에서는 이 판정조건을 리용하여 $\mathbf{F}_{p^{2m}}$ 에서

$$(X^{p^m}+aX+\delta)^{(p^{2m}-1)/d+1}-aX\ \ (d=2,\ 3,\ 4,\ 6)$$

형태로 새로운 치환다항식들을 얻어냈으며 선행연구[2]에서는 $(X^{p^m}-X+\delta)^s+X$ 형태로 $\mathbf{F}_{p^{2m}}$ 의 치환다항식들을 새롭게 얻었다.

이제 론문에서는 유한체의 2차확대체우에서 새로운 치환다항식들을 구성하게 된다.

α 를 $\mathbf{F}_{q^2}$ 의 원시원소라고 하고 $D_0=<\alpha^2>$, $D_1=\alpha D_0$ 이라고 하자. 그리고 $\mathbf{F}_{q^2}$ 의 원소 a가 $a^{q+1}=1$ 을 만족시킨다고 하자. 그러면 $a=\alpha^{(q-1)t}$ 을 만족시키는 t가 존재한다. 이때 다음의 보조정리가 성립한다.

보조정리 2 $\mathbf{F}_{q^2}$ 의 원소 a와 δ가 $a^{q+1}=1,\ a\delta^q=\delta$ 를 만족시킨다고 하자. 이때

$$\{ax^q+x+\delta\,|\,x\in\mathbf{F}_{q^2}\}=\{ax^q+x-\delta\,|\,x\in\mathbf{F}_{q^2}\}=\alpha^{-t}\mathbf{F}_q$$

가 성립한다.

증명 $(ax^q+x+\delta)^q=a^qx+x^q+\delta^q=(ax^q+x+\delta)/a$ 가 성립한다. 따라서 $ax^q+x+\delta\neq 0$ 일 때

$$(ax^q+x+\delta)^{q-1}=\frac{1}{a}=\alpha^{-(q-1)t}$$

이므로 어떤 $b\in\mathbf{F}_q$ 가 존재하여 $ax^q+x+\delta=\alpha^{-t}b$ 가 성립한다. 즉 $ax^q+x+\delta\in\alpha^{-t}\mathbf{F}_q$ 가 성립한다. 따라서 $q\geq|\{ax^q+x+\delta\,|\,x\in\mathbf{F}_{q^2}\}|$ 이 성립한다.

한편 $|\{ax^q+x\,|\,x\in\mathbf{F}_{q^2}\}|=|\{ax^q+x+\delta\,|\,x\in\mathbf{F}_{q^2}\}|$ 이고 $|\{ax^q+x\,|\,x\in\mathbf{F}_{q^2}\}|\geq q^2/q=q$ 이므로 $|\{ax^q+x+\delta\,|\,x\in\mathbf{F}_{q^2}\}|=q$ 이며 따라서 $\{ax^q+x+\delta\}=\alpha^{-t}\mathbf{F}_q$ 이다. 또한 $a\delta^q=\delta$ 를 만족시키는 임의의 $\delta\in\mathbf{F}_{q^2}$ 에 대하여 $\forall x\in\mathbf{F}_{q^2}$, $a(x-\delta)^q+(x-\delta)+\delta=ax^q+x-\delta$ 가 성립하므로 $\{ax^q+x+\delta\,|\,x\in\mathbf{F}_{q^2}\}=\{ax^q+x-\delta\,|\,x\in\mathbf{F}_{q^2}\}$ 가 성립한다는것도 알수 있다.(증명끝)

정리 1 $\mathbf{F}_{q^2}$ 의 원소 a와 δ 가 $a^{q+1}=1$, $a\delta^q=\delta$ 를 만족시키고 표수는 3이 아닌 홀수라고 하자. 이때 $f(X)=(aX^q+X+\delta)^{(q^2-1)/2+1}-aX^q$ 은 $\mathbf{F}_{q^2}$ 의 치환다항식이다.

증명 $S=\overline{S}=\{ax^q+x+\delta\,|\,x\in\mathbf{F}_{q^2}\}=\{ax^q+x-\delta\,|\,x\in\mathbf{F}_{q^2}\}$ 이라고 하고

$$\varphi(x):=ax^q+x+\delta,\ \psi(x):=ax^q+x-\delta,\ h(x):=2x^{(q^2-1)/2+1}-x$$

라고 하자. 그러면 임의의 $x\in\mathbf{F}_{q^2}$ 에 대하여

$$\begin{aligned}\psi\circ f(x)&=a(ax^q+x+\delta)^{((q^2-1)/2+1)q}-x+(ax^q+x+\delta)^{(q^2-1)/2+1}-ax^q-\delta=\\&=a[a^{-1}(ax^q+x+\delta)]^{(q^2-1)/2+1}+(ax^q+x+\delta)^{(q^2-1)/2+1}-(ax^q+x+\delta)=\\&=2(ax^q+x+\delta)^{(q^2-1)/2+1}-(ax^q+x+\delta)\\h\circ\varphi(x)&=2(ax^q+x+\delta)^{(q^2-1)/2+1}-(ax^q+x+\delta)\end{aligned}$$

또한 임의의 $s\in S$ 에 대하여 $f(x)$ 가 $\varphi^{-1}(s)$ 에서 1대1이므로 $f(X)$ 가 $\mathbf{F}_{q^2}$ 의 치환다항식이기 위하여서는 $h:S\to\overline{S}$ 가 1대1일것이 필요하고 충분하다. 그런데 구조적인 특성으로부터 $S\subset D_0\cup\{0\}$ 또는 $S\subset D_1\cup\{0\}$ 이다. 그리고 $x\in D_0\cup\{0\}$ 에 대하여

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

이고 $x\in D_1\cup\{0\}$ 에 대하여

$$h(x)=2x^{(q^2-1)/2+1}-x=-3x$$

이므로 $h:S\to\overline{S}$ 는 1대1이다.(증명끝)

$a^{q+1}=1$, $a\delta^q=\delta$ 를 만족시키는 임의의 a, $\delta\in\mathbf{F}_{q^2}$ 에 대하여 $y=x/a$ 에 의하여

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

이 성립한다는것을 알수 있다. 그러므로 다음과 같은 주장이 성립한다.

따름 $\mathbf{F}_{q^2}$ 의 원소 a와 δ 가 $a^{q+1}=1$, $a\delta^q=\delta$ 를 만족시키고 표수는 3이 아닌 홀수라고 하자. 이때 $f(X)=(X^q+aX+\delta)^{(q^2-1)/2+1}-X^q$ 는 $\mathbf{F}_{q^2}$ 의 치환다항식이다.

정리 2 $\mathbf{F}_{q^2}$ 의 표수는 홀수이고 $\mathbf{F}_{q^2}$ 의 원소 a와 δ 가 $a^{q+1}=1$, $a\delta^q=\delta$ 를 만족시키며 또한 a는 $a+a^{-1}\pm1=0$ 을 만족시키지 않는다고 하자.

이때 $f(X)=(X^q+aX+\delta)^{(q^2-1)/2+q}-aX$ 는 $\mathbf{F}_{q^2}$ 의 치환다항식이다.

증명 $S=\overline{S}=\{x^q+ax+\delta \mid x\in \mathbf{F}_{q^2}\}=\{ax^q+x-\delta \mid x\in \mathbf{F}_{q^2}\}$ 으로 놓고

$$\varphi(x):=x^q+ax+\delta,\ \psi(x):=ax^q+x-\delta,\ h(x):=(a+a^{-1})x^{(q^2-1)/2+1}-x$$

라고 하면 임의의 $x\in \mathbf{F}_{q^2}$ 에 대하여

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

$$h\circ\varphi(x)=(a+a^{-1})(x^q+ax+\delta)^{(q^2-1)/2+1}-(x^q+ax+\delta)$$

$f(x)$ 는 임의의 $s\in S$ 에 대하여 $\varphi^{-1}(s)$ 에서 1대1이다. 따라서 $h:S\to\overline{S}$ 가 1대1이면 $f(X)$ 는 $\mathbf{F}_{q^2}$ 의 치환다항식이다. 그런데 $S\subset D_0\cup\{0\}$ 또는 $S\subset D_1\cup\{0\}$ 이며 $x\in D_0\cup\{0\}$ 에 대하여

$$h(x)=(a+a^{-1})x^{(q^2-1)/2+1}-x=(a+a^{-1}-1)x$$

이고 $x\in D_1\cup\{0\}$ 에 대하여

$$h(x)=(a+a^{-1})x^{(q^2-1)/2+1}-x=-(a+a^{-1}+1)x$$

이므로 $h:S\to\overline{S}$ 는 1대1이다.(증명끝)

따름 $\mathbf{F}_{q^2}$ 의 원소 a와 δ 가 $a^{q+1}=1,\ a\delta^q=\delta$ 를 만족시키고 a가 $a+a^{-1}\pm1=0$ 을 만족시키지 않을 때 $f(X)=(aX^q+X+\delta)^{(q^2-1)/2+q}-X$ 는 $\mathbf{F}_{q^2}$ 의 치환다항식이다.

참 고 문 헌

[1] P. Yuan et al.; Finite Fields Appl., 35, 215, 2015.

[2] Z. Zha et al.; Finite Fields Appl., 40, 150, 2016.

주체107(2018)년 9월 8일 원고접수

The Methods for Constructing Two Kinds of Permutation Polynomials over Quadratic Extension of a Finite Field

Ri Yong Song, *Kim Kwang Yon*

In this paper, new permutation polynomials of the form

$$(aX^q+X+\delta)^{(q^2-1)/2+1}-aX^q,\ (X^q+aX+\delta)^{(q^2-1)/2+q}-aX$$

over $\mathbf{F}_{q^2}$ are constructed.

Key words: finite field, quadratic extension, permutation polynomial