김일성종합대학학보
(자연과학)
주체106(2017)년 제63권 제1호

JOURNAL OF **KIM IL SUNG** UNIVERSITY
(NATURAL SCIENCE)
Vol. 63 No. 1 JUCHE106(2017).

유한체의 2차확대체우에서 몇가지 치환다항식들

최수련, 김광연

유한체 $\mathbf{F}_q$에서 결수를 가지는 다항식 $f(X)$로부터 정의되는 넘기기 $f:\mathbf{F}_q\to\mathbf{F}_q$가 $\mathbf{F}_q$의 1:1넘기기일 때 $f(X)$를 $\mathbf{F}_q$의 치환다항식이라고 부른다.

유한체의 치환다항식은 부호리론과 암호리론, 조합설계를 비롯한 수학과 공학의 다른 령역에 널리 응용되고있다.

치환다항식에 대한 연구들가운데서 새로운 치환다항식클라스를 얻기 위한 연구가 가장 활발하게 진행되고있다.

선행연구[4]에서는 유한모임의 치환을 위한 보조정리[1]를 리용하여 $g(X^{p^k}-X+\delta)+L(X)$ 형태의 치환다항식을 얻기 위한 조건들을 얻었으며 선행연구[5]에서도 $b(X^{p^k}+aX+\delta)^{(p^n-1)/d+1}+L(X)$ 형태의 치환다항식클라스들을 연구하였다.

한편 선행연구[2, 3]에서는 이 보조정리를 리용하지 않고 방정식의 풀이개수를 결정하는 방법으로 2차확대체우에서 $(X^{p^m}-X+\delta)^s+L(X)$ 형태의 치환다항식들을 구하였다.

론문에서는 표수가 홀수인 2차확대체우에서 선행연구의 일부 결과들을 일반화하여 $a(X^q-bX+\delta)^s+L(X)$ (q는 홀씨수)형태의 치환다항식들의 판정조건을 얻었다.

보조정리 1[1] $A, S, \overline{S}$는 유한모임들이고 $|S|=|\overline{S}|$이며 넘기기

$$f:A\to A,\ h:S\to\overline{S},\ \lambda:A\to S,\ \overline{\lambda}:A\to\overline{S}$$

들은 $\overline{\lambda}\circ f=h\circ\lambda$를 만족시킨다고 하자.

이때 λ와 $\overline{\lambda}$가 우로의 넘기기이면 다음의 명제들은 동등하다.

① f는 우로의 1:1넘기기이다. 즉 f는 A의 치환이다.

② $h:S\to\overline{S}$는 우로의 1:1넘기기이며 f는 매 $s\in S$에 대하여 $\lambda^{-1}(s)$ 우에서 1:1이다.

보조정리 1에 근거하여 다음의 결과들이 얻어진다.

정리 1 $\delta\in\mathbf{F}_{q^n}$이고 $g(X)$는 $\mathbf{F}_{q^n}$에 기초한 다항식이며 임의의 $x\in\mathbf{F}_{q^n}$에 대하여

$$g^q(x^q-x+\delta)=-g(x^q-x+\delta)$$

라고 하자.

$L(X)\in\mathbf{F}_q[X]$가 선형다항식이라고 할 때 다항식 $f(X)=g(X^q-X+\delta)+L(X)$가 $\mathbf{F}_{q^n}$우의 치환다항식이기 위해서는 $h(x)=-2g(x)+L(x)$가 $\{x\in\mathbf{F}_{q^n}\mid Tr_{q^n/q}(x)=Tr_{q^n/q}(\delta)\}$ 우에서 1:1넘기기이고 $L(X)$가 $\mathbf{F}_q$우의 치환다항식일것이 필요하고 충분하다.

증명 $S=\overline{S}=\{x^q-x\mid x\in\mathbf{F}_{q^n}\}$, $\psi(x)=\overline{\psi}(x)=x^q-x$, $u(x)=-2g(x+\delta)+L(x)$ 라고 하면 ψ와 $\overline{\psi}$는 $\mathbf{F}_{q^n}$을 S로 보내는 우로의 넘기기이고 u는 S를 $\overline{S}$로 보내는 넘기기이며

$\overline{\psi} \circ f(x) = (g(x^q - x + \delta))^q + (L(x))^q - g(x^q - x + \delta) - L(x) = -2g(x^q - x + \delta) + L(x^q) - L(x),$

$u \circ \psi(x) = -2g(x^q - x + \delta) + L(x^q) - L(x)$

이다. 즉 $\overline{\psi} \circ f = u \circ \psi$ 이다.

그러므로 보조정리 1로부터 f가 $\mathbf{F}_{q^n}$ 우의 치환다항식이기 위해서는 u가 우로의 1：1넘기기이고 매 $s \in S$에 대하여 f가 $\psi^{-1}(s)$ 우에서 1：1일것이 필요하고 충분하다.

그런데 임의의 $x \in \psi^{-1}(s)$에 대하여 $f(x) = g(s + \delta) + L(x)$ 이므로 f의 $\psi^{-1}(s)$ 우에서의 1：1성은 $L(X)$의 $\psi^{-1}(s)$ 우에서의 1：1성과 동등하다.

임의의 $x,\ y \in \psi^{-1}(s)$에 대하여 $s = x^q - x = y^q - y$ 이므로 $x - y \in \mathbf{F}_q$ 이다. 즉 임의의 $x \in \psi^{-1}(s)$에 대하여 $\psi^{-1}(s) = \{x + z \mid z \in \mathbf{F}_q\}$ 이다.

그러므로 $L(X)$의 $\psi^{-1}(s)$ 우에서의 1：1성은 $\mathbf{F}_q$에서의 1：1성과 동등하다.

한편 $Tr_{q^n/q}(x) = Tr_{q^n/q}(\delta)$ 이기 위하여서는 $Tr_{q^n/q}(x - \delta) = 0$ 일것이 즉 $x - \delta \in S$ 일것이 필요하고 충분하다. 따라서 $S + \delta = \{x \in F_{q^n} \mid Tr_{q^n/q}(x) = Tr_{q^n/q}(\delta)\}$ 가 성립된다.

그러므로 $u(x) = h(x + \delta) - L(\delta)$ 가 S 우에서 1：1이기 위해서는 $h(x) = -2g(x) + L(x)$ 가 $\{x \in \mathbf{F}_{q^n} \mid Tr_{q^n/q}(x) = Tr_{q^n/q}(\delta)\}$ 우에서 1：1일것이 필요하고 충분하다.

이로부터 정리의 주장이 성립된다.(증명끝)

따름 1 t는 홀수이고 $Tr_{q^2/q}(\delta) = 0\ (\delta \in \mathbf{F}_{q^2})$이라고 하자.

$L(X) \in \mathbf{F}_q[X]$가 선형화다항식이라고 할 때 다항식 $f(X) = (X^q - X + \delta)^t + L(X)$가 $\mathbf{F}_{q^2}$ 우의 치환다항식이기 위해서는 $h(x) = -2x^t + L(x)$가 $\{x \in \mathbf{F}_{q^2} \mid Tr_{q^2/q}(x) = 0\}$ 우에서 1：1넘기기이고 $L(X)$가 $\mathbf{F}_q$ 우의 치환다항식일것이 필요하고 충분하다.

이제 q는 홀씨수의 제곱이고 α를 $\mathbf{F}_{q^2}$의 원시원소라고 하자.

$a \in \mathbf{F}_{q^2}^{\times}$, $b \in \mathbf{F}_{q^2}$이 $b^{1+q} = 1$, $b\delta^q = \delta\ (\delta \in \mathbf{F}_{q^2})$를 만족시킨다고 가정하자.

그러면 어떤 $t\ (0 \le t \le q)$가 있어서 $b = \alpha^{(q-1)t}$ 으로 된다.

이때 다음의 결과들이 성립된다.

보조정리 2[5] $b,\ \delta \in \mathbf{F}_{q^2}$이 $b^{1+q} = 1$, $b\delta^q = \delta$를 만족시킨다고 하자.

이때 $b = \alpha^{(q-1)t}\ (0 \le t \le q)$이라고 하면 다음의 식이 성립된다.

$$\mathrm{Im}(x^q + bx) = \mathrm{Im}(bx^q + x) = \mathrm{Im}(x^q + bx \pm \delta) = \mathrm{Im}(bx^q + x \pm \delta) = \{\alpha^{-t} y \mid y \in \mathbf{F}_q\}$$

정리 2 $a \in \mathbf{F}_{q^2}^{\times}$, $s \in \boldsymbol{N}$이고 $b \in \mathbf{F}_{q^2}$이 $b^{1+q} = 1$을 만족시킨다고 하자.

이때 다항식 $f(X) = a(X^q + bX)^s + X^q - bX$ 가 $\mathbf{F}_{q^2}$의 치환다항식이기 위해서는 $\gcd(s,\ q-1) = 1$이고 $a^{q-1} + b^{s-1} \ne 0$을 만족시킬것이 필요하고 충분하다.

증명 $\varphi(x) = x^q + bx$, $\psi(x) = bx^q + x$라고 하자.

그러면 보조정리 2로부터 $\mathrm{Im}(\varphi) = \mathrm{Im}(\psi)$ 라는것을 알수 있다.

$S = \mathrm{Im}(\varphi) = \mathrm{Im}(\psi)$, $g(x) = (a^q / b^{s-1} + a)x^s$ 이라고 하면

$$\psi(f(x)) = b(a^q(x+b^q x^q)^s + x - b^q x^q) + a(x^q + bx)^s + x^q - bx = \\ = ba^q(b^{-1}x^q + x)^s + a(x^q + bx)^s = \\ = (a^q / b^{s-1} + a)(x^q + bx)^s = (a^q / b^{s-1} + a)(\varphi(x))^s = g(\varphi(x)).$$

또한 임의의 $z \in S$ 에 대하여 $x \in \varphi^{-1}(z)$ 일 때 $f(x) = (az^s + z) - 2bx$ 이므로 $f(x)$ 가 $\varphi^{-1}(z)$ 우에서 1 : 1이라는것을 알수 있다. 그러므로 $f(X)$ 가 $\mathbf{F}_{q^2}$ 의 치환다항식이기 위해서는 $g(x)$ 가 S 의 치환일것이 필요하고 충분하다.

$b^{1+q} = 1$ 이므로 어떤 $t\,(0 \le t \le q)$ 가 있어서 $b = \alpha^{(q-1)t}$ 으로 된다.

보조정리 1로부터 $S = \{\alpha^{-t} y \mid y \in \mathbf{F}_q\}$ 이므로 $g(x)$ 가 S 의 치환이기 위해서는 $\mathbf{F}_q$ 의 치환일것이 필요하고 충분하다. 그런데 $g(x)$ 가 $\mathbf{F}_q$ 의 치환이기 위해서는 $a^q / b^{s-1} + a \ne 0$ 이고 $\gcd(s, q-1) = 1$ 일것이 필요하고 충분하므로 정리의 결과가 성립된다.(증명끝)

따름 2 $a \in \mathbf{F}_q^{\times}$, $s \in \boldsymbol{N}$ 이고 $b \in \mathbf{F}_{q^2}$ 이 $b^{1+q} = 1$ 을 만족시킨다고 하자.

이때 $b = \alpha^{(q-1)t}\,(0 \le t \le q)$ 이라고 하면 다항식 $f(X) = a(X^q + bX)^s + X^q - bX$ 가 $\mathbf{F}_{q^2}$ 의 치환다항식이기 위해서는 $\gcd(s, q-1) = 1$ 이고 $q+1 \nmid (s-1)t - \dfrac{q+1}{2}$ 일것이 필요하고 충분하다.

일반적으로 2차확대체우에서 $f(X) = u(vX^q + wX + \delta)^s + vX^q - wX$ 형태의 다항식이 주어졌을 때 $Y = v^q X$ 로 놓으면 이 다항식은 $g(Y) = u(Y^q + cY + \delta)^s + Y^q - cY\,(c = w/v^q)$ 형태로 되며 $f(X)$ 의 치환성과 $g(Y)$ 의 치환성은 서로 동등하다.

그리고 $c^{1+q} = 1\,(c \in \mathbf{F}_{q^2})$, $c\delta^q = \delta$ 인 경우에는 $c = \alpha^{(q-1)l}$ 인 $0 \le l \le q$ 가 존재하며 따라서 어떤 $y \in \mathbf{F}_q$ 가 있어서 $\delta = \alpha^{-l} y$ 가 성립되며 $\delta = \beta^q + c\beta$ 인 $\beta \in \mathbf{F}_{q^2}$ 이 존재한다. 그러므로

$$g(Y) = u(Y^q + cY + \delta)^s + Y^q - cY = u((Y+\beta)^q + c(Y+\beta))^s + Y^q - cY\,.$$

이때 $Z = Y + \beta$ 로 놓으면 $g(Y) = u(Z^q + cZ)^s + Z^q - cZ - (\beta^q - c\beta)$ 로 되므로 $g(Y)$ 의 치환성은 $h(Z) = u(Z^q + cZ)^s + Z^q - cZ$ 의 치환성과 동등하다. 즉 우의 가정밑에서 $f(X)$ 와 $g(Y)$, $h(Z)$ 들은 아핀동등한 다항식들이므로 그중 어느 한 다항식이 치환다항식이면 나머지 두 다항식도 치환다항식으로 된다.

따름 3 $a, c \in \mathbf{F}_{q^2}^{\times}$, $s \in \boldsymbol{N}$ 이고 $b, c, \delta \in \mathbf{F}_{q^2}$ 이 $b^{1+q} = c^{1+q}$, $b\delta^q = c^q \delta$ 를 만족시킨다고 할 때 다항식 $f(X) = a(cX^q + bX + \delta)^s + cX^q - bX$ 가 $\mathbf{F}_{q^2}$ 의 치환다항식이기 위해서는 $\gcd(s, q-1) = 1$ 이고 $a^{q-1}c^{q(s-1)} + b^{s-1} \ne 0$ 일것이 필요하고 충분하다.

따름 3에서 $s = (q^2 - 1)/d + 1\,(d > 1,\ q - 1 \equiv 0 (\mathrm{mod}\ d))$, $c = 1$ 로 놓으면 선행연구[5]의 결과들이 나오며 $a = 1$, $b = -1$ 로 놓으면 다음의 결과가 성립된다.

따름 4 $s \in \boldsymbol{N}$, $Tr_{q^2/q}(\delta) = 0\,(\delta \in \mathbf{F}_{q^2})$ 이라고 하면 $f(X) = (X^q - X + \delta)^s + X^q + X$ 가 $\mathbf{F}_{q^2}$ 우의 치환다항식이기 위해서는 $\gcd(s, q-1) = 1$ 이고 $2 \nmid s$ 일것이 필요하고 충분하다.

따름 4에서 $s = i(q+1) + 1$ 로 놓으면 선행연구[3]의 결과가 얻어지며

$$s=(q^2-1)/2+q,\ (q^2-1)/3+1$$

로 놓으면 선행연구[2]의 결과가 나온다.

실례 $q=5,\ s=21,\ b=\alpha^4$ 으로 놓으면 다항식 $f(X)=(X^5+bX)^{21}+X^5-bX$ 는 $\mathbf{F}_{25}$ 우의 치환다항식이다. 또한 $b\delta^5=\delta$ 인 임의의 $\delta\in\mathbf{F}_{25}$ 에 대하여서도 $g(X)=(X^5+bX+\delta)^{21}+X^5-bX$ 는 $f(X)$ 와 아핀동등한 치환다항식이다.

선행연구[3, 5]에서는 $s=i(q+1)+1\ (0<i<q-1)$ 또는 $s=(q^2-1)/d+1\ (d>1),\ (q^2-1)/2+q$ 형태로 취하였다. $q=5$ 인 이 경우에 그런 s 는 5, 7, 9, 13, 17, 19이다. $s=21$ 로 놓으면 이것은 그런 형태가 아닌것으로 된다.

그리고 $b=\alpha^4$ 으로 놓으면 $\{x^5+bx\,|\,x\in\mathbf{F}_{25}\}=\{x^5+bx+\delta\,|\,x\in\mathbf{F}_{25}\}=\{\alpha^{-1}y\,|\,y\in\mathbf{F}_5\}$ 로 된다.

다항식을 $h(X)=(X^5+bX)^s+X^5-bX$ 라고 하면 $x^5+bx=\alpha^{-1}\alpha^6=\alpha^5$ 인 $x\in\mathbf{F}_{25}$ 에 대하여 $f(x)\neq h(x)$ 이므로 $f(X)$ 는 선행결과들과 동등하지 않다. 즉 다항식 $f(X)$ 는 선행결과들로는 얻을수 없는 치환다항식이다.

이상과 같이 론문에서는 표수가 홀수인 2차확대체우에서 $a(X^q-bX+\delta)^s+L(X)$ 형태의 선행연구들에서보다 넓은 클라스의 치환다항식들을 구성하였다.

참 고 문 헌

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

[2] T. Helleseth et al.; Finite Fields Appl., **22**, 16, 2013.

[3] Z. Tu et al.; Finite Fields Appl., **34**, 20, 2015.

[4] P. Yuan et al.; Finite Fields Appl., **27**, 88, 2014.

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

주체105(2016)년 9월 5일 원고접수

Some Permutation Polynomials over Quadratic Extensions of Finite Fields

Choe Su Ryon, Kim Kwang Yon

The permutation polynomials over finite fields are applied in many aspects of mathematics and engineering including the coding theory, cryptography, combinational design, etc.

We derive permutation polynomials of the form $a(X^q-bX+\delta)^s+L(X)$ over the finite field $\mathbf{F}_{q^2}$ of odd characteristic.

Key word: permutation polynomial