김일성종합대학학보 주체110(2021)년
수 학 제67권 제3호

유한체우에서 몇가지 치환다항식과 완전치환다항식들의 구성

구철범, 김광연

q를 씨수의 제곱, $\mathbf{F}_q$를 위수가 q인 유한체라고 하자.

이때 다항식 $f(X)\in\mathbf{F}_q[X]$에 대하여 넘기기 $x\mapsto f(x)$가 $\mathbf{F}_q$우에서 우로의 1：1넘기기일 때 $f(X)$를 $\mathbf{F}_q$의 치환다항식이라고 부른다. 그리고 $f(X)$와 $f(X)+X$가 모두 $\mathbf{F}_q$의 치환다항식일 때 $f(X)$를 완전치환다항식이라고 부른다.

선행연구[2]에서는 $q=(q')^n$인 체 $\mathbf{F}_q$우에서 $d=(q-1)/(q'-1)+1$일 때 ax^d형태의 완전치환다항식을 구성하였으며 n이 홀수일 때 충분히 큰 q에 대하여 $\mathbf{F}_q$우의 단항식 aX^d가 완전치환다항식이 되기 위한 필요조건을 제시하였다.

선행연구[4]에서는 표수가 홀수인 유한체우에서 3개의 완전치환단항식클라스를 구성하고 거꿀함수에 해당한 단항식들에 대해서도 연구하였으며 선행연구[1]에서는 AGW판정조건을 리용하여 완전치환3항식들을 구성하였다.

선행연구[5]에서는 $a[\mathrm{Tr}_m^n(X)]^k+u(c+X)(\mathrm{Tr}_m^n(X)+X)+bX$ 형태와 $X^{i(2^{2m}-1)/3+1}+bX$ 형태의 완전치환다항식을 구성하고 b가 1의 원시3차뿌리일 때 $X^{3i(2^m-1)+1}+bX$가 완전치환다항식이기 위한 충분조건을 증명하였으며 선행연구[6]에서는 $(X^{2^m}+X+\delta)^s+bX$ 형태의 치환다항식을 구성하였다.

선행연구들을 보면 흔적을 리용한 치환다항식과 완전치환다항식구성과 관련하여서는 아핀3항식을 리용한 경우에 비해 다항식의 형태가 아직 다양하지 못하며 단항식과 2, 3항식과 관련하여서는 대체로 완전치환다항식으로 되기 위한 충분조건들이 제시되였다.

론문에서는 선행연구[5]의 완전치환2항식구성의 충분조건을 필요충분조건으로 개선하여 다항식클라스를 넓히며 선행연구[3, 6]에서 구성한 흔적을 리용한 치환다항식클라스보다 넓은 다항식클라스들에 속하는 다항식들이 치환다항식으로 되기 위한 조건을 제시하고 새로운 완전치환다항식클라스들을 구성한다.

보조정리 1[1] (AGW판정조건) 유한모임 A, S, $\bar{S}$가 $|S|=|\bar{S}|$를 만족시키고 넘기기 $f:A\to A$, $\bar{f}:S\to\bar{S}$ 및 $\lambda:A\to S$, $\bar{\lambda}:A\to\bar{S}$가 $\bar{\lambda}\circ f=\bar{f}\circ\lambda$를 만족시킨다고 하자.

만일 λ와 $\bar{\lambda}$가 우로의 넘기기이면 다음의 사실들은 동등하다.

① f는 A우의 치환이다.

② $\bar{f}$는 우로의 1：1넘기기이며 모든 $s\in S$에 대하여 f는 $\lambda^{-1}(s)$우에서 1：1이다.

보조정리 2[1] q는 씨수의 제곱, r는 정의옹근수, d는 $q-1$의 정의약수라고 하자.

$h(X)\in\mathbf{F}_q[X]$에 대하여 다항식 $f(X)=X^rh(X^{(q-1)/d})$이 $\mathbf{F}_q$우의 치환다항식이기 위해서는 다음의 조건들이 성립될것이 필요하고 충분하다.

① $\gcd(r,\ (q-1)/d)=1$

② $X^rh(X)^{(q-1)/d}$은 1의 d차뿌리들을 치환한다.

보조정리 3 m, n이 정의옹근수일 때 $2 \nmid (n/\gcd(m, n))$ 이면 $\gcd(2^n-1, 2^m+1)=1$ 이 성립된다.

증명 $2 \nmid (n/\gcd(m, n))$ 이므로 $\gcd(m, n)=\gcd(2m, n)$ 이라는것을 알수 있다. 그리고 $\gcd(2^m+1, 2^n-1)=d$ 는 $\gcd(2^{2m}-1, 2^n-1)$ 을 완제한다.

그런데 $\gcd(2^{2m}-1, 2^n-1)=2^{\gcd(2m, n)}-1=2^{\gcd(m, n)}-1=\gcd(2^m-1, 2^n-1)$ 이 성립되므로 d 는 $\gcd(2^m+1, 2^m-1)=1$을 완제하며 결국 $d=1$이다.(증명끝)

정리 1 정의옹근수 m이 n의 약수이고 정의옹근수 l, k, s에 대하여 $2 \nmid (n/\gcd(lm, n))$ 이며 $(2^{lm}+1)s \equiv 1 \pmod{2^n-1}$ 이라고 하자. 이때 임의의 $\delta \in \mathbf{F}_{2^n}$과 임의의 $b \in \mathbf{F}_{2^m}^{\times}$에 대하여 다항식 $g(X)=(X^{2^{lm}}+X+\delta)^s+bX$ 는 $\mathbf{F}_{2^n}$ 우의 치환다항식이다.

증명 $g(X)$가 $\mathbf{F}_{2^n}$ 우의 치환다항식이라는것을 증명하기 위하여 임의의 $\gamma \in \mathbf{F}_{2^n}$에 대하여 방정식 $g(x)=\gamma$가 $\mathbf{F}_{2^n}$에서 기껏 1개의 풀이를 가진다는것을 증명하자.

x가 이 방정식의 풀이이면 $g(x)=\gamma$이므로 $(x^{2^{lm}}+x+\delta)^s=bx+\gamma$이다.

이제 이 식의 량변을 $2^{lm}+1$제곱하면 $x^{2^{lm}}+x+\delta=(bx+\gamma)^{2^{lm}+1}$을 얻는다.

여기서 오른변을 전개하면

$$(bx+\gamma)^{2^{lm}+1}=(bx+\gamma)(bx+\gamma)^{2^{lm}}=(bx+\gamma)(bx^{2^{lm}}+\gamma^{2^{lm}})=b^2x^{2^{lm}+1}+b\gamma x^{2^{lm}}+b\gamma^{2^{lm}}x+\gamma^{2^{lm}+1}$$

이므로 다음의 식이 성립된다.

$$b^2x^{2^{lm}+1}+(b\gamma+1)x^{2^{lm}}+(b\gamma^{2^{lm}}+1)x+\gamma^{2^{lm}+1}+\delta=0 \qquad (1)$$

웃식의 왼변을 변형하면

$$b^2x^{2^{lm}+1}+(b\gamma+1)x^{2^{lm}}+(b\gamma^{2^{lm}}+1)x+\gamma^{2^{lm}+1}+\delta=b^2(x+(b\gamma+1)/b^2)^{2^{lm}+1}+(b\gamma^{2^{lm}}+b\gamma+1+b^2\delta)/b^2$$

와 같이 쓸수 있다. 따라서 식 (1)은 다음의 식과 동등하다.

$$(x+(b\gamma+1)/b^2)^{2^{lm}+1}=(b\gamma^{2^{lm}}+b\gamma+1+b^2\delta)/b^4 \qquad (2)$$

그런데 $(2^{lm}+1)s \equiv 1 \pmod{2^n-1}$이므로 식 (2)의 량변을 s제곱하면 $x=(b\gamma+1)/b^2+\Delta^s$이 성립된다. 여기서 $\Delta=(b\gamma^{2^{lm}}+b\gamma+1+b^2\delta)/b^4$이다.

따라서 방정식 $g(x)=\gamma$는 $\mathbf{F}_{2^n}$에서 기껏 1개의 풀이를 가진다.

그러므로 $g(X)$는 $\mathbf{F}_{2^n}$ 우의 치환다항식이다.(증명끝)

따름 정의옹근수 m, n, l, k와 s들이 정리 1의 조건을 만족시킨다고 하면 임의의 $\delta \in \mathbf{F}_{2^n}$와 임의의 $b \in \mathbf{F}_{2^m} \setminus \mathbf{F}_2$에 대하여 다항식 $g(X)=(X^{2^{lm}}+X+\delta)^s+bX$는 $\mathbf{F}_{2^n}$ 우의 완전치환다항식이다.

따름에서 $l=1$로 놓으면 선행연구[6]의 명제 1의 주장이 얻어진다.

정리 2 p는 씨수이고 정의옹근수 m이 정의옹근수 n의 약수라고 하자.

이때 임의의 $b \in \mathbf{F}_{p^m}^{\times}$와 임의의 $h(X) \in \mathbf{F}_{p^m}[X]$, $\gamma \in \mathbf{F}_{p^n}$에 대하여 $k=\mathrm{Tr}_m^n(\gamma) \in \mathbf{F}_{p^m}$이면 다항식 $f(X)=\gamma h(\mathrm{Tr}_m^n(X))+bX$가 $\mathbf{F}_{p^n}$ 우의 치환다항식이기 위해서는 $g(X)=\frac{n}{m}kh(X)+bX$가 $\mathbf{F}_{p^n}$ 우의 치환다항식일것이 필요하고 충분하다.

증명 임의의 $x\in\mathbf{F}_{p^n}$ 에 대하여 $\mathrm{Tr}_m^n(f(x))=\frac{n}{m}kh(\mathrm{Tr}_m^n(x))+b\mathrm{Tr}_m^n(x)=g(\mathrm{Tr}_m^n(x))$ 가 성립한다.

AGW판정조건에 의해 $f(X)$ 가 $\mathbf{F}_{p^n}$ 우의 치환다항식이기 위해서는 $g(X)$ 가 $\mathbf{F}_{p^n}$ 우의 치환다항식이고 임의의 $s\in\mathbf{F}_{p^m}$ 에 대하여 $f(x)$ 가 $\{x\in\mathbf{F}_{p^n}\,|\,\mathrm{Tr}_m^n(x)=s\}$ 우에서 1:1넘기기일것이 필요하고 충분하다. 그런데 임의의 $s\in\mathbf{F}_{p^m}$ 에 대하여 모임 $\{x\in\mathbf{F}_{p^n}\,|\,\mathrm{Tr}_m^n(x)=s\}$ 우에서 $f(x)=h(s)+L(x)$ 이고 $b\neq 0$ 이므로 $f(x)$ 는 이 모임우에서 1 : 1이다.

따라서 $f(X)$ 가 $\mathbf{F}_{p^n}$ 우의 치환다항식이기 위해서는 $g(X)$ 가 $\mathbf{F}_{p^n}$ 우의 치환다항식일것이 필요하고 충분하다.(증명끝)

이 정리로부터 완전치환다항식과 관련하여 다음의 따름이 직접 얻어진다.

따름 p 는 씨수이고 정의옹근수 m 이 정의옹근수 n 의 약수이며 $h(X)\in\mathbf{F}_{p^m}[X]$, $\gamma\in\mathbf{F}_{p^n}$, $k=\mathrm{Tr}_m^n(\gamma)$ 라고 할 때 임의의 $b\in\mathbf{F}_{p^m}\setminus\{0,\,-1\}$ 에 대하여 $f(X)=\gamma h(\mathrm{Tr}_m^n(X))+bX$ 가 $\mathbf{F}_{p^n}$ 우의 완전치환다항식이기 위해서는 $g(X)=\frac{n}{m}kh(X)+bX$ 가 $\mathbf{F}_{p^n}$ 우의 완전치환다항식일것이 필요하고 충분하다.

정리 2에서 $m=1$, $\gamma=b=1$로 놓으면 선행연구[3]의 따름 7에서 구성한 치환다항식이 얻어진다. 선행연구 [5]의 명제 1에서는 보조정리 2를 리용하여 특정한 b 에 대하여 $X^{i(2^{2m}-1)/3+1}+bX$ (여기서 $i\in\{1,\,2\}$)가 $\mathbf{F}_{2^{2m}}$ 우의 완전치환다항식이라는것을 증명하였다.

보조정리 2를 리용한 $\mathbf{F}_{2^{2m}}$ 우에서 새로운 완전치환3항식구성에 대하여 보자.

정리 3 정의홀수 m 과 임의의 $b\in\mathbf{F}_{2^m}\setminus\mathbf{F}_2$ 에 대하여 $X^{2(2^{2m}-1)/3+1}+X^{(2^{2m}-1)/3+1}+bX$ 는 $\mathbf{F}_{2^{2m}}$ 우의 완전치환다항식이다.

증명 m 이 홀수이므로 $3\,|\,2^m+1$ 이다.

ω 를 $\mathbf{F}_{2^{2m}}$ 에서 1의 원시3차뿌리라고 하면 $g(X)=X(X^{2(2^{2m}-1)/3}+X^{(2^{2m}-1)/3}+b)$ 이므로 보조정리 2에 의하여 $g(X)$ 가 $\mathbf{F}_{2^{2m}}$ 우의 치환다항식이기 위해서는 $h(x)=x(x^2+x+b)^{(2^{2m}-1)/3}$ 이 $\{1,\,\omega,\,\omega^2\}$ 을 치환할것이 필요하고 충분하다.

그런데 $h(x)=x[(x^2+x+b)^{2^m-1}]^{(2^m+1)/3}$ 이므로

$$h(1)=[(1^2+1+b)^{2^m-1}]^{(2^m+1)/3}=(b^{2^m-1})^{(2^m+1)/3}=1^{(2^m+1)/3}=1$$

$$h(\omega)=\omega[(\omega^2+\omega+b)^{2^m-1}]^{(2^m+1)/3}=\omega[(1+b)^{2^m-1}]^{(2^m+1)/3}=\omega\cdot 1^{(2^m+1)/3}=\omega$$

$$h(\omega^2)=\omega^2[(\omega^4+\omega^2+b)^{2^m-1}]^{(2^m+1)/3}=\omega^2[(1+b)^{2^m-1}]^{(2^m+1)/3}=\omega^2\cdot 1^{(2^m+1)/3}=\omega^2$$

이다. 따라서 $g(X)$ 는 $\mathbf{F}_{2^{2m}}$ 우의 치환다항식이다.

마찬가지로 $g(X)+X$ 도 치환다항식이며 결국 $g(X)$ 는 완전치환다항식이다.(증명끝)

정리 4 m 은 $3\nmid m$ 인 정의홀수이고 i 는 부아닌 옹근수이며 $b\in\mathbf{F}_{2^{2m}}$ 은 1의 원시3차뿌리라고 하면 $f(X)=X^{3i(2^m-1)+1}+bX$ 가 $\mathbf{F}_{2^{2m}}$ 우의 완전치환다항식이기 위해서는 $\gcd(3i-1,\,(2^m+1)/3)=1$ 일것이 필요하고 충분하다.

증명 $h_0(X)=X^i+b$ 로 놓으면 $f(X)=Xh_0(X^{3(2^m-1)})$ 로 표시할수 있다. 그리고 m 이 홀수이므로 $3|(2^m+1)$ 이다. 따라서 보조정리 2에서 $d=(2^m+1)/3$ 으로 놓을 때 $f(X)$ 가 $\mathbf{F}_{2^{2m}}$ 우의 치환다항식이기 위해서는 $h(x)=xh_0(x)^{3(2^m-1)}$ 이 1의 d 차뿌리모임 μ_d 우의 치환일것이 필요하고 충분하다.

먼저 임의의 $x\in\mu_d$ 에 대하여 $x^i+b\neq 0$ 이라는것을 강조해둔다.

만일 어떤 $x\in\mu_d$ 에 대하여 $b=x^i$ 라고 가정하면 $b^d=1$ 이므로 $3|d$ 이며 따라서 $9|(2^m+1)$ 이다. 그런데 $3\nmid m$ 이므로 이것은 모순이다.

다음으로 임의의 $x\in\mu_d$ 에 대하여 $x^{2^m}=x^{-1}x^{3d}=x^{-1}$ 이고 $b^{2^m}=b^{-1}$ 이므로

$$h(x)=x\left(\frac{(x^i+b)^{2^m}}{x^i+b}\right)^3=x\left(\frac{x^{2^m i}+b^{2^m}}{x^i+b}\right)^3=x\left(\frac{x^{-i}+b^{-1}}{x^i+b}\right)^3=x(b^{-1}x^{-i})^3=b^{-3}x^{1-3i}=x^{1-3i}$$

이다. 따라서 $f(X)$ 가 $\mathbf{F}_{2^{2m}}$ 우의 치환다항식이기 위해서는 $h(x)=x^{1-3i}$ 가 μ_d 우의 치환일것이 필요하고 충분하다. 그런데 이것은 $\gcd(3i-1,\ (2^m+1)/3)=1$ 이라는것과 동등하다.

한편 $b+1=b^2$ 도 1의 원시3차뿌리이므로 $f(X)+X$ 에 대해서도 같은 주장을 할수 있다. 즉 $f(X)$ 는 완전치환다항식이다.(증명끝)

선행연구[5]의 명제 2에서는 정리 4와 같은 형태의 다항식이 완전치환다항식이 되기 위한 충분조건으로 $\gcd(1-3i,\ 2^{2m}-1)=1$ 을 제시하였다. 정리 4에서는 이런 형태의 다항식이 완전치환다항식이 되기 위한 필요충분조건을 밝힘으로써 b 와 m 이 주어졌을 때 선행의 완전치환2항식클라스를 최대로 넓혔다.

참 고 문 헌

[1] A. Akbary et al.; Finite Fields Appl., 17, 51, 2011.
[2] D. Bartoli et al.; Finite Fields Appl., 41, 132, 2016.
[3] J. Marcos; Finite Fields Appl., 17, 105, 2011.
[4] X. Guangkui et al.; Finite Fields Appl., 31, 228, 2015.
[5] L. Li et al.; Finite Fields Appl., 55, 177, 2019.
[6] X. Xu et al.; Finite Fields Appl., 57, 309, 2019.

주체110(2021)년 3월 5일 원고접수

Construction of Some Permutation and Complete Permutation Polynomials over Finite Fields

Ku Chol Bom, Kim Kwang Yon

We present necessary and sufficient conditions for some binomials and trinomials permute finite fields $\mathbf{F}_{2^n}$ and polynomials of the form $\gamma h(\mathrm{Tr}_m^n(X))+bX$ to be permutation polynomials over finite fields $\mathbf{F}_{p^n}$.

Keywords: permutation polynomial, binomial, trace