김일성종합대학학보
수 학

주체109(2020)년
제66권 제1호

한가지 단항식이 완전치환으로 되기 위한 조건들

신 영 호

위대한 령도자 **김정일**동지께서는 다음과 같이 교시하시였다.

《기초과학을 끊임없이 심화발전시키지 않고서는 첨단과학기술을 연구도입할수도 없고 새로운 높은 수준의 과학기술을 연구개발할수도 없습니다.》(《**김정일**선집》 증보판 제22권 21페지)

론문에서는 유한체우의 한가지 형태의 단항식이 완전치환으로 되기 위한 조건에 대하여 연구하였다.

완전치환다항식은 최근시기 유한체리론분야에서 활발히 연구되고있는 대상중의 하나이다. 그러나 완전치환다항식에 대한 선행연구들은 거의 모두가 다 표수가 2인 유한체우에서 진행되였으며 대부분이 단항식의 형태였다.

선행연구[1]에서는 m이 홀수일 때 ax^{2^m+2}이 $\mathbf{F}_{2^{2m}}$ 우에서 완전치환다항식으로 되는 a를 구하였다. 선행연구[2]에서는 m이 홀수일 때 ax^{3^m+2}이 $\mathbf{F}_{3^{2m}}$ 우에서 완전치환다항식으로 되는 a를 구하였다. 이로부터 어떤 씨수 p에 대하여 ax^{p^m+2}이 $\mathbf{F}_{p^{2m}}$ 우의 완전치환다항식으로 될수 있으며 즉 ax^{p^m+2}이 $\mathbf{F}_{p^{2m}}$ 우의 완전치환다항식으로 되게 하는 p, m, a의 조건을 론의하는 문제가 중요하게 제기된다.

론문에서는 2, 3을 포함한 모든 표수 p에 대하여 ax^{p^m+2}이 $\mathbf{F}_{p^{2m}}$ 우의 완전치환다항식으로 되게 하는 m과 a의 조건을 경우에 따라 갈라 고찰하였다.

유한체 $\mathbf{F}_q$ 우의 다항식 $f(x)$로부터 $\mathbf{F}_q$ 우의 우로의 1：1넘기기가 유도될 때 다항식 $f(x)$를 치환다항식[3], $f(x)+x$도 치환다항식일 때 완전치환다항식[4]이라고 부른다.

$\mathbf{F}_{q^n}$을 $\mathbf{F}_q$로 보내는 흔적넘기기[3] $\mathrm{Tr}_{\mathbf{F}_{q^n}/\mathbf{F}_q}:\mathbf{F}_{q^n}\to\mathbf{F}_q$를 다음과 같이 정의한다.

$$\mathrm{Tr}_{\mathbf{F}_{q^n}/\mathbf{F}_q}(x):=x+x^q+x^{q^2}+\cdots+x^{q^{n-1}}$$

$\mathrm{Tr}_{\mathbf{F}_{q^n}/\mathbf{F}_{q^k}}$를 간단히 $\mathrm{Tr}_{n/k}$라고 쓰기도 한다. 여기서 p는 표수이다. $\mathrm{Tr}_{n/1}$을 절대흔적넘기기라고 부르며 Tr로 표시한다. 흔적넘기기는 선형넘기기이다.

보조정리 1[3] $\mathbf{F}_q$ 우의 단항식 x^d가 치환다항식이기 위해서는 $\gcd(d,\ q-1)=1$일것이 필요하고 충분하다.

보조정리 2[3] $\mathbf{F}_q$ 우의 다항식 $f(x)$가 치환다항식이기 위해서는 령이 아닌 임의의 원소 $\gamma\in\mathbf{F}_q$에 대하여

$$\sum_{x\in\mathbf{F}_q}\omega^{\mathrm{Tr}(\gamma f(x))}=0$$

일것이 필요하고 충분하다. 여기서 $\omega = e^{2\pi i/p}$ 은 1의 원시 p 차뿌리이고 p 는 $\mathbf{F}_q$ 의 표수이다.

보조정리 3[2] $d \mid q-1$인 옹근수 $d>0$ 을 선택하자. ζ 를 $\mathbf{F}_q$ 우에서 1의 원시 d 차뿌리라고 하자. 이때 2항식 $x^{(q-1)/d+1}+ax$ $(a\neq 0)$가 $\mathbf{F}_q$ 우에서 치환이기 위해서는 다음의 두 조건을 만족시킬것이 필요하고 충분하다.

① $(-a)^d \neq 1$

② $0\le i<j\le d-1$인 $i,\ j$에 대하여 다음식이 성립한다.

$$\left(\frac{a+\zeta^i}{a+\zeta^j}\right)^{\frac{q-1}{d}} \neq \zeta^{j-i}$$

표수 p가 $6k+5$형태인 경우에 대하여 보겠다. 먼저 m이 홀수라고 하자.

보조정리 4 다항식 x^2-x+1은 $\mathbf{F}_q$ 우에서 기약이다. 여기서 p 는 씨수이며 어떤 정의 옹근수 k가 있어서 $p=6k+5$이다.

정리 1 $\mathbf{F}_{p^{2m}}$ 우의 단항식 $v^{-1}x^{p^m+2}$ 은 m 이 홀수이고 $\mathrm{Tr}_{2m/m}(\alpha v)=0$ 혹은 $\mathrm{Tr}_{2m/m}(\alpha^5 v)=0$ $(v\neq 0)$일 때 완전치환다항식이다. 여기서 α는 1의 원시6차뿌리이다.

증명 보조정리 4로부터 다항식 x^2-x+1 은 $\mathbf{F}_p$ 우에서 기약이다. 또한 α 는 다항식 x^2-x+1의 뿌리이다. 이때

$$\alpha^2=\alpha-1,\ \alpha^3=-1,\ \alpha^4=-\alpha,\ \alpha^5=1-\alpha$$

이며 m이 홀수이므로 x^2-x+1은 $\mathbf{F}_{p^m}$ 우에서 기약다항식이다. 즉

$$\mathbf{F}_{p^{2m}}=\mathbf{F}_{p^m}(\alpha)=\{x_0+x_1\alpha \mid x_0,\ x_1\in\mathbf{F}_{p^m}\}$$

이다. 그리고 $\mathrm{Tr}_{2m/m}(\alpha)=1,\ \mathrm{Tr}_{2m/m}(\alpha^2)=-1$ 이다. $v=v_0+v_1\alpha$ 에 대하여 $\mathrm{Tr}_{2m/m}(\alpha v)=0$ 이라는것은

$$\mathrm{Tr}_{2m/m}(\alpha(v_0+v_1\alpha))=\mathrm{Tr}_{2m/m}(v_0\alpha+v_1\alpha^2)=v_0-v_1$$

이므로 $v_0=v_1$임을 의미하며 류사하게 $\mathrm{Tr}_{2m/m}(\alpha^5 v)=0$ 이라는것은 $v_0=-2v_1$ 임을 의미한다.

먼저 $v^{-1}x^{p^m+2}$ 가 $\mathbf{F}_{p^{2m}}$ 우의 치환다항식이라는것을 보자.

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

이므로 보조정리 1로부터 $v^{-1}x^{p^m+2}$ 는 치환다항식이다.

다음으로 $v^{-1}x^{p^m+2}+x$ 다시말하여 $x^{p^m+2}+vx$가 치환다항식이라는것을 보자.

보조정리 2를 리용하겠다. 즉 령이 아닌 임의의 $\gamma\in\mathbf{F}_{p^{2m}}$ 에 대하여

$$\sum_{x\in\mathbf{F}_{p^{2m}}}\omega^{\mathrm{Tr}(\gamma(x^{p^m+2}+vx))}=0$$

이라는것을 밝히겠다. 여기에서 ω는 1의 원시 p 차뿌리이다.

x^{p^m+2} 가 치환다항식이므로 어떤 원소 $\beta \in \mathbf{F}_{p^{2m}}^*$ 이 있어서 $\gamma = \beta^{p^m+2}$ 이다. 따라서

$$\sum_{x\in\mathbf{F}_{p^{2m}}} \omega^{\mathrm{Tr}(\gamma(x^{p^m+2}+vx))} = \sum_{x\in\mathbf{F}_{p^{2m}}} \omega^{\mathrm{Tr}((\beta x)^{p^m+2}+\beta^{p^m+1}v(\beta x))} = \sum_{x\in\mathbf{F}_{p^{2m}}} \omega^{\mathrm{Tr}(x^{p^m+2}+\beta^{p^m}vx)} =$$

$$= \sum_{x\in\mathbf{F}_{p^{2m}}} \omega^{\mathrm{Tr}_{m/1}(\mathrm{Tr}_{2m/m}(x^{p^m+2}+\beta^{p^m+1}vx))} = \sum_{x_0,\,x_1\in\mathbf{F}_{p^m}} \omega^{\mathrm{Tr}_{m/1}(\mathrm{Tr}_{2m/m}((x_0+x_1\alpha)^{p^m+2}+\beta^{p^m+1}(v_0+v_1\alpha)(x_0+x_1\alpha)))}$$

이다. 여기서

$$\begin{aligned}\mathrm{Tr}_{2m/m}((x_0+x_1\alpha)^{p^m+2}) &= \mathrm{Tr}_{2m/m}((x_0+x_1\alpha)^{p^m}(x_0+x_1\alpha)^2) = \\ &= \mathrm{Tr}_{2m/m}((x_0-x_1\alpha^2)(x_0^2+2x_0x_1\alpha+x_1^2\alpha^2)) = \\ &= 2x_0^3+3x_0^2x_1+3x_0x_1^2+x_1^3 = (x_0+x_1)^3+x_0^3\end{aligned}$$

$(\beta^{p^m+1})^{p^{m-1}} = \beta^{p^{2m-1}} = 1$ 이므로 β^{p^m+1} 은 $\mathbf{F}_{p^m}$ 의 원소이고 따라서

$$\beta^{p^m+1}(v_0+v_1\alpha) = u_0+u_1\alpha$$

로 쓸수 있다. 여기에서 $u_i = \beta^{p^m+1}v_i$ 이다. 이로부터

$$\mathrm{Tr}_{2m/m}(\beta^{p^m+1}(v_0+v_1\alpha)(x_0+x_1\alpha)) = (2u_0+u_1)x_0+(u_0-u_1)x_1$$

이라는것을 알수 있다. 따라서

$$\sum_{x\in\mathbf{F}_{p^{2m}}} \omega^{\mathrm{Tr}(\gamma(x^{p^m+2}+vx))} = \sum_{x_0,\,x_1\in\mathbf{F}_{p^m}} \omega^{\mathrm{Tr}_{m/1}((x_0+x_1)^3+x_0^3+(2u_0+u_1)x_0+(u_0-u_1)x_1)} =: A$$

이다.

① $v_0 = v_1$ 즉 $u_0 = u_1$ 인 경우

$$\sum_{x_0,\,x_1\in\mathbf{F}_{p^m}} \omega^{\mathrm{Tr}_{m/1}((x_0+x_1)^3+x_0^3+3u_0x_0)} = \sum_{x_0\in\mathbf{F}_{p^m}} \omega^{\mathrm{Tr}_{m/1}(x_0^3+3u_0x_0)} \sum_{x_1\in\mathbf{F}_{p^m}} \omega^{\mathrm{Tr}_{m/1}((x_0+x_1)^3)}$$

고정된 x_0 에 대하여 $(x_0+x_1)^3$ 은 치환다항식이므로 $\sum_{x_1\in\mathbf{F}_{p^m}} \omega^{\mathrm{Tr}_{m/1}((x_0+x_1)^3)} = 0$ 이다. 따라서

$$A = 0$$

② $v_0 = -2v_1$ 즉 $u_0 = -2u_1$ 인 경우

$$A = \sum_{x_0,\,x_1\in\mathbf{F}_{5^m}} \omega^{\mathrm{Tr}_{m/1}((x_0+x_1)^3+x_0^3-3u_1(x_0+x_1))}$$

$y := x_0+x_1$ 로 변수치환을 하면

$$A = \sum_{x_0,\,y\in\mathbf{F}_{5^m}} \omega^{\mathrm{Tr}_{m/1}(y^3+x_0^3-3u_1y)} = \sum_{y\in\mathbf{F}_{5^m}} \omega^{\mathrm{Tr}_{m/1}(y^3-3u_1y)} \sum_{x_0\in\mathbf{F}_{5^m}} \omega^{\mathrm{Tr}_{m/1}(x_0^3)}$$

이다. 고정된 y 에 대하여 x_0^3 은 치환다항식이므로 $\sum_{x_0\in\mathbf{F}_{5^m}} \omega^{\mathrm{Tr}_{m/1}(x_0^3)} = 0$ 이다. 따라서

$$A = 0$$

이로부터 $x^{p^m+2}+vx$는 치환다항식이다.(증명끝)

m이 짝수인 경우에는 x^{p^m+2}자체가 치환다항식이 아니다. 사실

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

이므로 보조정리 1로부터 x^{p^m+2}는 치환다항식이 아니다.

표수 p가 $6k+3$형태인 경우에 대하여 보자. 이러한 조건을 만족시키는 표수 p는 오직 3뿐이다. m이 홀수인 경우에 대하여서는 선행연구[2]에서 연구되였다.

m이 짝수인 경우에 대하여 고찰하자.

정리 2 $\mathbf{F}_{3^{2m}}$우의 단항식 $v^{-1}x^{3^m+2}$는 m이 짝수이고 $\mathrm{Tr}_{2m/m}(v)=0,\ v\neq 0$일 때 완전 치환다항식이다.

기타 경우의 표수 p에 대하여 보자.

표수 p가 $6k+1$형태인 경우에는 m의 짝홀성에 관계없이 x^{p^m+2}자체가 치환다항식이 아니다. 사실

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

이므로 보조정리 1로부터 x^{p^m+2}은 치환다항식이 아니다.

$6k+2$형태인 표수 p는 오직 2뿐이다. m이 홀수일 때에는 이미 연구되였다. m이 짝수일 때에는 x^{2^m+2}자체가 치환다항식이 아니다. 사실

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

이므로 보조정리 1로부터 x^{2^m+2}은 치환다항식이 아니다.

$6k+4$형태인 표수 p는 없다.

참 고 문 헌

[1] P. Charpin, G. M. Kyureghyan; SIAM J. Discrete Math., 22, 2, 650, 2008.
[2] X. Guangkui, X. Cao; Finite Fields Appl., 31, 228, 2015.
[3] R. Lidl, et al.; Finite Fields, Encyclopedia Math. Appl., 20, 67, 1997.
[4] G. Wu et al.; Finite Fields Appl., 28, 148, 2014.

주체108(2019)년 9월 15일 원고접수

Some Conditions for a Kind of Monomial to be Complete Permutation

Sin Yong Ho

In this paper, we discuss when a monomial ax^{p^m+2} can be a complete permutation over $\mathbf{F}_{p^{2m}}$ for different p and m.

Keywords: monomial, complete permutation