김일성종합대학학보
(자연과학)
주체104(2015)년 제61권 제8호

JOURNAL OF **KIM IL SUNG** UNIVERSITY
(NATURAL SCIENCE)
Vol. 61 No. 8 JUCHE104(2015).

한가지 형태의 치환다항식클라스에 대한 보충

태일경, 김광연

위대한 령도자 **김정일**동지께서는 다음과 같이 교시하시였다.

《과학기술을 발전시켜야 나라의 경제를 빨리 추켜세울수 있으며 뒤떨어진 기술을 앞선 기술로 갱신하여 생산을 끊임없이 높여나갈수 있습니다.》(《**김정일**선집》 증보판 제20권 62페지)

치환다항식과 관련하여 제시된 미해명문제들가운데서 하나는 새로운 치환다항식클라스를 찾는 문제이다.

현재 치환다항식에 대한 연구에서 이 문제는 중요한 문제의 하나로 되고있다.

선행연구[2]에서는 $\mathbf{F}_{2^m}$ 에서 클루스터만합에 대한 새로운 항등식을 얻기 위하여 $(X^2-X+\delta)^s+L(X)$ ($L(X)$ 는 선형화다항식이다.)형태의 치환다항식을 연구하였으며 선행연구[3, 4]에서는 $(X^p-X+\delta)^s+L(X)$, $(X^{p^k}-X+\delta)^s+L(X)$ 형태의 치환다항식클라스를 새로 제안하였다.

한편 선행연구[5]에서는 $\mathbf{F}_{2^n}$ 우에서 $(X^{2^k}+X+\delta)^s+X$ 형태의 치환다항식을 찾아냈다. 이와 관련하여 선행연구[1]에서는 $(X^{p^k}+X+\delta)^s+L(X)$ 형태의 새로운 치환다항식클라스를 제안하였다.

우리는 $(X^{p^k}+X+\delta)^s+L(X)$ 형태의 새로운 치환다항식클라스에 속하는 새로운 치환다항식들을 찾는것을 연구목적으로 설정하였다.

앞으로 D_0 을 $\mathbf{F}_{p^n}$ 의 령아닌 평방원소들전체의 모임이라고 하고 D_1 은 $\mathbf{F}_{p^n}$ 의 비평방원소들전체의 모임이라고 하자.

정리 1 p 가 $p\equiv 1 \pmod 4$ 인 홀씨수이고 n 과 k 는 정의옹근수들로서 $n=4k$ 일 때 $\mathbf{F}_{p^n}$ 의 원소 δ 에 대하여 $\delta^{p^{2k}}+\delta\in\mathbf{F}_{p^n}$ 이면 다항식 $(X^{p^k}+X+\delta)^{(p^n-1)/2+p^{2k}}-X^{p^k}+X$ 는 $\mathbf{F}_{p^n}$ 우에서 치환다항식으로 된다.

증명 $\mathbf{F}_{p^n}$ 의 임의의 원소 b에 대하여

$$(X^{p^k}+X+\delta)^{\frac{p^n-1}{2}+p^{2k}}-X^{p^k}+X=b \tag{1}$$

를 만족시키는 원소는 유일하다는것을 증명하자.

이제 X 가 식 (1)을 만족시킨다고 하면 다음의 경우들이 성립된다.

① $X^{p^k}+X+\delta=0$ 인 경우 $-X^{p^k}+X=b$ 이므로

$$X=\frac{b-\delta}{2},\ X^{p^k}=\frac{b^{p^k}-\delta^{p^k}}{2},\ X^{p^k}+X+\delta=\frac{b^{p^k}+b-\delta^{p^k}+\delta}{2}.$$

따라서 식 (1)을 만족시키는 X는 유일하다.

② $X^{p^k}+X+\delta\in D_0$인 경우

$$(X^{p^k}+X+\delta)^{\frac{p^n-1}{2}+p^{2k}}-X^{p^k}+X=(X^{p^k}+X+\delta)^{p^{2k}}-X^{p^k}+X=b$$

이므로

$$X^{p^{3k}}+X^{p^{2k}}-X^{p^k}-X=b-\delta^{p^{2k}}=\alpha,\ \ X^{p^{3k}}-X^{p^{2k}}+X^{p^k}+X=\alpha^{p^k},$$
$$-X^{p^{3k}}+X^{p^{2k}}+X^{p^k}+X=\alpha^{p^{2k}},\ \ X^{p^{3k}}+X^{p^{2k}}+X^{p^k}-X=\alpha^{p^{3k}},$$
$$X=\frac{\alpha+\alpha^{p^k}+\alpha^{p^{2k}}-\alpha^{p^{3k}}}{4},\ \ X^{p^k}+X+\delta=\frac{b^{p^{2k}}+b^{p^k}-\delta^{p^{3k}}+\delta}{2}$$

이고 이 경우에도 식 (1)을 만족시키는 X는 유일하다.

③ $X^{p^k}+X+\delta\in D_1$인 경우

$$(X^{p^k}+X+\delta)^{\frac{p^n-1}{2}+p^{2k}}-X^{p^k}+X=-(X^{p^k}+X+\delta)^{p^{2k}}-X^{p^k}+X=b$$

이므로

$$-X^{p^{3k}}-X^{p^{2k}}-X^{p^k}+X=b+\delta^{p^{2k}}=\beta,\ \ -X^{p^{3k}}-X^{p^{2k}}+X^{p^k}-X=\beta^{p^k},$$
$$-X^{p^{3k}}+X^{p^{2k}}-X^{p^k}-X=\beta^{p^{2k}},\ \ X^{p^{3k}}-X^{p^{2k}}-X^{p^k}-X=\beta^{p^{3k}},$$
$$X=\frac{\beta-\beta^{p^k}-\beta^{p^{2k}}-\beta^{p^{3k}}}{4},\ \ X^{p^k}+X+\delta=-\frac{b^{p^{3k}}+b^{p^{2k}}+\delta^{p^k}-\delta}{2}$$

이고 이 경우에도 역시 (1)을 만족시키는 X는 유일하다.

이제 $\alpha:=\frac{b^{p^{2k}}+b^{p^k}-\delta^{p^{3k}}+\delta}{2}$라고 하자.

만일 어떤 X_0, X_1에 대하여 $X_i\in D_i$이고 X_i들이 각각 식 (1)을 만족시킨다면

$$X_0^{p^k}+X_0+\delta=\alpha,\ \ X_1^{p^k}+X_1+\delta=-\alpha^{p^k}.$$

여기서 α는 평방원소이고 -1이 평방원소이므로 $X_1^{p^k}+X_1+\delta=-\alpha^{p^k}$도 평방원소인데 이것은 $-\alpha^{p^k}$이 비평방이라는데 모순된다.

한편 경우 ①이 성립되고 동시에 경우 ②가 성립된다면 $\frac{b^{p^k}+b-\delta^{p^k}+\delta}{2}=0$이고 $\frac{b^{p^{2k}}+b^{p^k}-\delta^{p^{3k}}+\delta}{2}\in D_0$이다.

그런데 $\frac{b^{p^{2k}}+b^{p^k}-\delta^{p^{2k}}+\delta^{p^k}}{2}=0$이므로

$$\frac{b^{p^{2k}}+b^{p^k}-\delta^{p^{3k}}+\delta}{2}=-\frac{\delta^{p^{3k}}-\delta^{p^{2k}}-\delta^{p^k}-\delta}{2}=-\frac{(\delta^{p^{2k}}+\delta)^{p^k}-(\delta^{p^{2k}}+\delta)}{2}$$

이고 가정으로부터 $(\delta^{p^{2k}}+\delta)^{p^k}-(\delta^{p^{2k}}+\delta)=0$이므로 $\frac{b^{p^{2k}}+b^{p^k}-\delta^{p^{3k}}+\delta}{2}=0$.

이것은 $\frac{b^{p^{2k}}+b^{p^k}-\delta^{p^{3k}}+\delta}{2}\in D_0$ 이라는 주장과 모순된다.

경우 ②, ③이 동시에 성립될수 없다는것도 마찬가지방법으로 증명된다.(증명끝)

정리 2 p가 $p\equiv 1 \pmod 4$ 인 홀씨수이고 n과 k는 정의옹근수들이라고 할 때 $\mathbf{F}_{p^n}$의 임의의 원소 δ에 대하여 다항식 $(X^{p^k}+X+\delta)^{\frac{p^n-1}{2}+1}-X^{p^k}+X$는 $\mathbf{F}_{p^n}$ 우에서 치환다항식으로 된다.(증명생략)

정리 3 p가 $p\equiv 1 \pmod 4$ 인 홀씨수이고 n과 k는 $n|2k$를 만족시키는 정의옹근수들일 때 $\mathbf{F}_{p^n}$의 임의의 원소 δ에 대하여 다항식 $(X^{p^k}+X+\delta)^{\frac{p^n-1}{2}+p^{2k}}-X^{p^k}+X$는 $\mathbf{F}_{p^n}$ 우에서 치환다항식으로 된다.

증명 $\mathbf{F}_{p^n}$의 임의의 원소 b에 대하여

$$(X^{p^k}+X+\delta)^{\frac{p^n-1}{2}+p^k}-X^{p^k}+X=b \tag{2}$$

를 만족시키는 원소는 유일하다는것을 증명하자.

이제 X가 식 (2)를 만족시킨다고 하면 다음의 경우들이 성립된다.

① $X^{p^k}+X+\delta=0$인 경우 $-X^{p^k}+X=b$이므로

$$X=\frac{b-\delta}{2},\ X^{p^k}=\frac{b^{p^k}-\delta^{p^k}}{2},\ X^{p^k}+X+\delta=\frac{b^{p^k}+b-\delta^{p^k}+\delta}{2}$$

이고 이 경우 (2)를 만족시키는 X는 유일하다.

② $X^{p^k}+X+\delta\in D_0$인 경우

$$(X^{p^k}+X+\delta)^{\frac{p^n-1}{2}+p^k}-X^{p^k}+X=(X^{p^{2k}}+X^{p^k}+\delta^{p^k})-X^{p^k}+X=2X+\delta^{p^k}=b$$

이므로 $X=\frac{b-\delta^{p^k}}{2},\ X^{p^k}=\frac{b^{p^k}-\delta}{2},\ X^{p^k}+X+\delta=(b^{p^k}+b-\delta^{p^k}+\delta)$ 이고 이 경우에도 식 (2)를 만족시키는 X는 유일하다.

③ $X^{p^k}+X+\delta\in D_1$인 경우

$$(X^{p^k}+X+\delta)^{\frac{p^n-1}{2}+p^k}-X^{p^k}+X=-(X^{p^{2k}}+X^{p^k}+\delta^{p^k})-X^{p^k}+X=-2X^{p^k}-\delta^{p^k}=b$$

이므로 $X^{p^k}=-\frac{b+\delta^{p^k}}{2},\ X=-\frac{b^{p^k}+\delta}{2},\ X^{p^k}+X+\delta=-\frac{b^{p^k}+b+\delta^{p^k}-\delta}{2}$ 이고 이 경우에도 역시 식 (2)를 만족시키는 X는 유일하다.

이제 $\alpha:=\frac{b^{p^k}+b-\delta^{p^k}+\delta}{2}$라고 하면 $\frac{b^{p^k}+b+\delta^{p^k}-\delta}{2}=-\alpha^{p^k}$이므로 분명히 경우 ①이 성립되면 경우 ② 또는 경우 ③이 성립되지 않는다.

만일 어떤 X_0, X_1에 대하여 $X_i\in D_i$이고 X_i들이 각각 식 (2)를 만족시킨다면

$$X_0^{p^k}+X_0+\delta=\alpha,\ X_1^{p^k}+X_1+\delta=-\alpha^{p^k}$$

이다. α 와 -1 이 평방원소이므로 $X_1^{p^k}+X_1+\delta=-\alpha^{p^k}$ 도 평방원소인데 이것은 $-\alpha^{p^k}$ 이 비평방이라는데 모순된다.(증명끝)

정리 4 p가 $p\equiv 1 \pmod 4$ 인 홀씨수이고 n과 k는 $n|3k$를 만족시키는 정의옹근수들일 때 $\mathbf{F}_{p^n}$의 임의의 원소 δ에 대하여 다항식

$$(X^{p^k}+X+\delta)^{\frac{p^n-1}{2}+p^{2k}}-X^{p^k}+X$$

는 $\mathbf{F}_{p^n}$ 우에서 치환다항식으로 된다.

증명 $\mathbf{F}_{p^n}$의 임의의 원소 b에 대하여

$$(X^{p^k}+X+\delta)^{\frac{p^n-1}{2}+p^{2k}}-X^{p^{2k}}+X=b \tag{3}$$

를 만족시키는 원소는 유일하다는것을 증명하자.

이제 X가 식 (3)을 만족시킨다고 하면 다음의 경우들이 성립된다.

① $X^{p^k}+X+\delta=0$인 경우 $-X^{p^{2k}}+X=b$이므로 $X^{p^k}-X=b^{p^k}$이다.

따라서 $X=\dfrac{b^{p^k}+\delta}{2}$, $X^{p^k}=\dfrac{b^{p^k}+\delta^{p^k}}{2}$, $X^{p^k}+X+\delta=-\dfrac{b^{p^{2k}}+b^{p^k}+\delta^{p^k}-\delta}{2}$이고 이 경우 식 (3)을 만족시키는 X는 유일하다.

② $X^{p^k}+X+\delta\in D_0$ 인 경우 $(X^{p^k}+X+\delta)^{\frac{p^n-1}{2}+p^{2k}}-X^{p^{2k}}+X=2X+\delta^{p^{2k}}=b$ 이므로 $X=\dfrac{b-\delta^{p^{2k}}}{2}$, $X^{p^k}=\dfrac{b^{p^k}-\delta}{2}$, $X^{p^k}+X+\delta=\dfrac{b^{p^k}+b-\delta^{p^{2k}}+\delta}{2}$이고 이 경우에도 식 (3)을 만족시키는 X는 유일하다.

③ $X^{p^k}+X+\delta\in D_1$인 경우

$$(X^{p^k}+X+\delta)^{\frac{p^n-1}{2}+p^{2k}}-X^{p^{2k}}+X=-2X^{p^{2k}}-\delta^{p^{2k}}=b$$

이므로

$$X^{p^{2k}}=-\frac{b+\delta^{p^{2k}}}{2},\ X=-\frac{b^{p^k}+\delta}{2},\ X^{p^k}=-\frac{b^{p^{2k}}+\delta^{p^k}}{2},\ X^{p^k}+X+\delta=-\frac{b^{p^{2k}}+b^{p^k}+\delta^{p^k}-\delta}{2}$$

이고 이 경우에도 역시 식 (3)을 만족시키는 X는 유일하다.

이제 $\alpha:=\dfrac{b^{p^k}+b-\delta^{p^{2k}}+\delta}{2}$라고 하면 $-\dfrac{b^{p^{2k}}+b^{p^k}+\delta^{p^k}-\delta}{2}=-\alpha^{p^k}$이므로 분명히 경우 ①이 성립되면 경우 ② 또는 경우 ③이 성립되지 않는다.

만일 어떤 X_0, X_1에 대하여 $X_i\in D_i$이고 X_i들이 각각 식 (3)을 만족시킨다면

$$X_0^{p^k}+X_0+\delta=\alpha,\ X_1^{p^k}+X_1+\delta=-\alpha^{p^k}.$$

α와 -1이 평방원소이므로 $X_1^{p^k}+X_1+\delta=-\alpha^{p^k}$ 도 평방원소인데 이것은 $-\alpha^{p^k}$이 비평방이라는데 모순된다.(증명끝)

참 고 문 헌

[1] 김광연 등; 수학, **4**, 42, 주체103(2014).

[2] T. Helleseth et al.; Finite Fields Appl., **9**, 187, 2003.

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

[4] J. Yuan et al.; Finite Fields Appl., **17**, 560, 2011.

[5] X. Zheng et al.; Appl. Algebra Comm. Comput., **21**, 145, 2010.

주체104(2015)년 4월 5일 원고접수

The Complement for a Class of Permutation Polynomials

Thae Il Gyong, Kim Kwang Yon

We find several new permutation polynomials in a class of permutation polynomials of the form $(X^{p^k}+X+\delta)^s+L(X)$ that were newly proposed already.

A new class of permutation polynomials of the form $(X^{p^k}+X+\delta)^s+L(X)$ is constructed by making permutation polynomials $(X^{p^k}+X+\delta)^{(p^n-1)/2+p^{ik}}+X^{p^{jk}}-X$.

We find complementary permutation polynomials of the form

$$(X^{p^k}+X+\delta)^{(p^n-1)/2+p^{ik}}-X^{p^{jk}}+X$$

in this class to extend this class more widely.

Key word: permutation polynomial