표수가 2인 유한체우에서 4가지 치환3항식클라스들의 구성

김광연, 송억현

위대한 령도자 **김정일**동지께서는 다음과 같이 교시하시였다.

《우리는 현실발전의 요구에 맞게 나라의 과학기술을 빨리 발전시켜야 하겠습니다.》(《**김정일**선집》 증보판 제11권 134페지)

1988년과 1993년에 리들과 뮬렌이 제기한 새로운 치환다항식클라스를 찾는 문제를 해결하기 위하여 연구들이 활발히 진행되고있는데 치환3항식에 대하여서는 그 결과가 많이 알려지지 않았다.

선행연구[2]에서는 $q\equiv 1 \pmod 3$ 인 체 $\mathbf{F}_q$ 에 기초한 $X^r h(X^{(q-1)/3})$ 과 같은 형태의 치환3항식의 특성을 밝혔으며 선행연구[1]에서는 q가 홀씨수의 제곱일 때 $aX+bX^q+X^{2q-1}(\in \mathbf{F}_{q^2}[X])$ 과 같은 형태의 3항식이 치환다항식으로 되기 위한 필요충분조건을 밝혔다.

론문에서는 표수가 2인 유한체우에서 선행연구들에서 얻어지지 않은 4가지 클라스의 새로운 치환3항식들의 구성에 대하여 연구하였다.

정리 1[3] r 는 정의옹근수이고 정의옹근수 d 는 $q-1$ 의 약수이며 $h(X)\in \mathbf{F}_q[X]$ 라고 하자. 이때 $X^r h(X^{(q-1)/d})$ 이 $\mathbf{F}_q$ 우에서의 치환다항식이기 위하여서는 다음의 두가지 조건을 만족시킬것이 필요하고 충분하다.

1) $\gcd\left(r,\ \dfrac{q-1}{d}\right)=1$

2) $X^r h(X)^{(q-1)/d}$ 이 μ_d 의 치환이다.(여기서 μ_d 는 1의 d 차뿌리들전부의 모임이다.)

$\mathbf{F}_q$ 의 대수적폐포를 $\overline{\mathbf{F}}_q$ 로 표기하자.

정리 2 m 이 정의옹근수일 때 다음의 다항식들은 모두 μ_{2^m+1} 에서 뿌리를 가지지 않는다.

$$1+X+X^3,\ 1+X^2+X^3,\ 1+X+X^4,\ 1+X^3+X^4$$

증명 우선 $\alpha(\in \mu_{2^m+1})$ 가 $1+X+X^3$ 의 뿌리라고 가정하자. 즉

$$1+\alpha+\alpha^3=0 \tag{1}$$

이라고 하자. 그러면 α 는 분명히 령이 아니다.

이제 식 (1)의 량변을 2^m 제곱하고 그 식에 α^3 을 곱하면 다음의 식이 얻어진다.

$$1+\alpha^2+\alpha^3=0 \tag{2}$$

이로부터 $\alpha+\alpha^2=0$ 이 얻어지는데 따라서 $\alpha=1$ 이라는것이 얻어진다. 그러나 $\alpha=1$ 은 식 (1)을 만족시키지 않는다. 그러므로 $1+X+X^3$ 은 μ_{2^m+1} 에서 뿌리를 가지지 않는다.

류사한 방법으로 나머지 3개의 다항식들에 대하여서도 주장이 성립한다는것이 증명된다.(증명끝)

넘기기들의 합성에 관한 일반적인 성질로부터 다항식 $g(X)(\in \mathbf{F}_q[X])$ 가 주어졌을 때 $f(X):=ag(bX+c)+d$ (여기서 $a,\ b,\ c,\ d\in \mathbf{F}_q,\ a,\ b\neq 0$ 이다.)가 $\mathbf{F}_q$ 우에서의 치환다항식이

기 위하여서는 $g(X)$ 가 $\mathbf{F}_q$ 우에서의 치환다항식일것이 필요하고 충분하다는것을 알수 있다. 그리고 분명히 치환다항식들전부의 모임은 다항식들의 합성산법에 관하여 하나의 군을 이룬다는것을 알수 있다.

정리 3 다항식 $f(X):=X^4+X^{2^m+3}+X^{3\cdot 2^m+1}(\in \mathbf{F}_{2^{2m}}[X])$ 이 $\mathbf{F}_{2^{2m}}$ 우에서의 치환다항식이기 위하여서는 $\gcd(m,\ 3)=1$ 이 성립할것이 필요하고 충분하다.

증명 다항식 $h(X):=1+X+X^3(\in \mathbf{F}_{2^{2m}}[X])$ 을 생각하면 다항식은 $f(x)$ 를 다음과 같이 쓸수 있다.

$$f(X)=X^4h(X^{2^m-1})$$

그러면 $\gcd(4,\ 2^m-1)=1$ 이므로 정리 1에 의하여 $f(X)$ 가 $\mathbf{F}_{2^{2m}}$ 우에서의 치환다항식이라는것은 다항식 $g(x):=X^4h(x)^{2^m-1}$ 이 μ_{2^m+1} 의 치환이라는 사실과 동등하다. 그러므로 $g(x)$ 가 μ_{2^m+1} 의 치환이기 위하여서는 m 이 3과 서로 소이라는것을 증명하면 충분하다.

우선 충분성을 증명하자.

$\gcd(m,\ 3)=1$ 이라고 하자. 그러면 정리 2에 의하여 $h(X)$ 는 μ_{2^m+1} 에서 뿌리를 가지지 않는다. 그리고 $h(\mu_{2^m+1})\subseteq \mathbf{F}_{2^{2m}}{}^{\times}$ 가 성립하므로 g 는 μ_{2^m+1} 을 μ_{2^m+1} 에로 넘긴다는것을 알수 있다. 그리고 μ_{2^m+1} 이 유한모임이므로 $g(x)$ 가 μ_{2^m+1} 의 치환이라는것은 $g(x)$ 가 μ_{2^m+1} 에서 1대1이라는것과 동등하다.

한편 임의의 $\alpha(\in \mu_{2^m+1})$ 에 대하여

$$g(\alpha)=\alpha^4(1+\alpha+\alpha^3)^{2^m-1}=\frac{\alpha^4(1+\alpha+\alpha^3)^{2m}}{1+\alpha+\alpha^3}=$$

$$=\frac{\alpha^4(1+\alpha^{2m}+(\alpha^{2m})^3)}{1+\alpha+\alpha^3}=\frac{\alpha^4(1+\alpha^{-1}+(\alpha^{-1})^3)}{1+\alpha+\alpha^3}=\frac{\alpha+\alpha^3+\alpha^4}{1+\alpha+\alpha^3}$$

이 성립하므로 $g(x)$ 가 μ_{2^m+1} 에서 1대1이라는것은 $G(x):=(x+x^3+x^4)/(1+x+x^3)$ 이 μ_{2^m+1} 에서 1대1이라는것과 동등하다. 그러므로 $G(x)$ 가 μ_{2^m+1} 에서 1대1이라는것을 밝히자.

어떤 서로 다른 $x,\ y(\in \mu_{2^m+1})$ 에 대하여 $G(x)=G(y)$ 가 성립한다고 하자. 그러면 x 와 y 가운데 적어도 하나가 1이든가 아니면 x 와 y 가운데 어느것도 1이 아니다.

우선 x 또는 y 가 1인 경우에는

$$\frac{x+x^3+x^4}{1+x+x^3}=\frac{y+y^3+y^4}{1+y+y^3}=1$$

이 성립하고 따라서 $x^4+1=y^4+1=0$ 이 성립한다. 그러므로 $x=y=1$ 이 얻어진다.

다음으로 x 도 y 도 1이 아닌 경우에 등식

$$G(x)=\frac{x+x^3+x^4}{1+x+x^3}=G(y)=\frac{y+y^3+y^4}{1+y+y^3}$$

의 량변에 1을 더하면

$$\frac{1+x^4}{1+x+x^3}=\frac{1+y^4}{1+y+y^3}$$

이 성립하고 따라서 등식

$$\frac{(x+1)^3+x^2}{(x+1)^4}=\frac{(y+1)^3+y^2}{(y+1)^4}$$

이 얻어진다. 그리고 이 식을 변형하면 다음과 같다.

$$\frac{1}{1+x}+\left(1+\frac{1}{1+x}\right)^2\left(\frac{1}{1+x}\right)^2=\frac{1}{1+y}+\left(1+\frac{1}{1+y}\right)^2\left(\frac{1}{1+y}\right)^2$$

그러므로

$$u:=\frac{1}{1+x},\ v:=\frac{1}{1+y}$$

로 놓으면 다음의 식이 얻어진다.

$$(u+v)^4+(u+v)^2+(u+v)=0 \tag{3}$$

만일 $x\neq y$ 즉 $u+v\neq 0$ 이라고 하면 $u+v(\in \mathbf{F}_{2^{2m}})$ 는 $1+X+X^3(\in \mathbf{F}_{2^{2m}}[X])$ 의 뿌리이다. 그런데 $1+X+X^3$ 은 $\mathbf{F}_2$ 우에서 기약이고 또한 $\gcd(3,\ 2m)=1$ 이라고 가정하였기때문에 $1+X+X^3$ 은 여전히 $\mathbf{F}_{2^{2m}}$ 우에서도 기약이다. 따라서 $\mathbf{F}_{2^{2m}}$ 의 원소들은 $1+X+X^3$ 의 뿌리로 될수 없다. 이것은 $u+v$ 가 $1+X+X^3$ 의 뿌리라는 사실에 모순된다.

다음으로 필요성을 증명하자.

$\beta(\in \overline{\mathbf{F}}_2)$ 를 $X^{2^m}+X+1(\in \mathbf{F}_2[X])$ 의 뿌리라고 하자. 그러면

$$\beta^{2^{2m}}=\left(\beta^{2^m}\right)^{2^m}=(\beta+1)^{2^m}=\beta^{2^m}+1=\beta$$

즉 $\beta\in \mathbf{F}_{2^{2m}}$ 이 성립한다.

이제 $\alpha(\in \mathbf{F}_{2^3})$ 가 $1+X+X^3$ 의 뿌리라고 하자. 이때 만일 $\gcd(m,\ 3)=3$ 이라면 $\alpha\in \mathbf{F}_{2^m}$ 이고

$$\begin{aligned}f(\alpha+\beta)&=(\alpha+\beta)^4+((\alpha+\beta)^{2^m})^3(\alpha+\beta)=\\&=(\alpha+\beta)^4+(\alpha+\beta+1)(\alpha+\beta)^3+(\alpha+\beta+1)^3(\alpha+\beta)=\\&=(\beta^4+\beta^2+\beta)+(\alpha^4+\alpha^2+\alpha)=\beta^4+\beta^2+\beta=f(\beta)\end{aligned}$$

가 성립한다. 그런데 $\alpha\neq 0$ 이므로 $\alpha+\beta\neq\beta$ 이고 따라서 이것은 $f(X)$ 가 $\mathbf{F}_{2^{2m}}$ 우에서의 치환다항식이라는 가정에 모순된다.(증명끝)

표. 다항식값

x	$f(x)$	x	$f(x)$
α	α^8	α^9	α^7
α^2	α	α^{10}	α^{10}
α^3	α^{14}	α^{11}	α^3
α^4	α^2	α^{12}	α^{11}
α^5	α^5	α^{13}	α^9
α^6	α^{13}	α^{14}	α^{12}
α^7	α^6	1	1
α^8	α^4	0	0

실례 1 원시다항식 $X^4+X+1(\in \mathbf{F}_2[X])$ 을 리용하여 4차확대체 $\mathbf{F}_{2^4}$ 우에서 정리 3의 조건에 맞는 치환3항식을 보기로 하자. 이때 3항식의 형태는 $X^4+X^{2^m+3}+X^{3\cdot 2^m+1}$ 으로 된다. 이 다항식의 값들을 보면 다음과 같다.(표)

표를 보면 이 3항식은 $\mathbf{F}_{2^4}$ 우에서 치환다항식이라는것을 알수 있다.

정리 4 다항식 $f(X):=X^2+X^{2\cdot 2m}+X^{3\cdot 2m-1}(\in \mathbf{F}_{2^{2m}}[X])$ 이 $\mathbf{F}_{2^{2m}}$ 우에서의 치환다항식이기 위하여서는 $\gcd(m,\ 3)=1$ 이 성립할것이 필요하고 충분하다.

증명 다항식 $f(X)$ 를 다항식 $h(X):=1+X+X^3$ 을 리용하여 다음과 같이 쓸수 있다.

$$f(X)=X^2h(X^{2^m-1})$$

그런데 $\gcd(2,\ 2^m-1)=1$ 이므로 정리 1에 의하여 $f(X)$ 가 $\mathbf{F}_{2^{2m}}$ 우에서의 치환다항식이라는것은 다항식 $g(x):=X^2h(x)^{2^m-1}$ 이 μ_{2^m+1} 의 치환이라는것과 동등하다. 정리 2에 의하여 $h(X)$ 는 μ_{2^m+1} 에서 뿌리를 가지지 않는다. 그러므로 $h(\mu_{2^m+1})\subseteq \mathbf{F}_{2^{2m}}{}^{\times}$ 와 $g(\mu_{2^m+1})\subseteq \mu_{2^m+1}$ 이 성립한다. 그리고 $g(x)$ 가 μ_{2^m+1} 의 치환이라는것은 $g(x)$ 가 μ_{2^m+1} 에서 1대1이라는것과 동등하다.

한편 임의의 $\alpha(\in \mu_{2^m+1})$ 에 대하여 앞에서와 류사한 방법으로

$$g(\alpha)=\frac{1+\alpha+\alpha^3}{\alpha+\alpha^3+\alpha^4}$$

이 성립한다는것을 밝힐수 있다. 따라서 $g(x)$ 가 μ_{2^m+1} 에서 1대1이라는것은 $G(x):=(1+x+x^3)/(x+x^3+x^4)$ 이 μ_{2^m+1} 에서 1대1이라는것과 동등하다. 그리고 정리 3의 증명에서의 $G(x)$ 를 $G_1(x)$ 로 표시하면 임의의 $\alpha(\in \mu_{2^m+1})$ 에 대하여 $G(\alpha)=1/G_1(\alpha)$ 이 성립하므로 결국 $g(x)$ 가 μ_{2^m+1} 에서 1대1이라는것은 $1/G(x)$ 이 μ_{2^m+1} 에서 1대1이라는것 즉 $G_1(x)$ 가 μ_{2^m+1} 에서 1대1이라는것과 동등하다. 그러므로 $g(x)$ 가 μ_{2^m+1} 에서 1대1이기 위하여서는 $\gcd(m,\ 3)=1$ 이 성립할것이 필요하고 충분하다.(증명끝)

정리 5 다항식 $f(X):=X^5+X^{2m+4}+X^{4\cdot 2m+1}(\in \mathbf{F}_{2^{2m}}[X])$ 이 $\mathbf{F}_{2^{2m}}$ 우에서의 치환다항식이기 위하여서는 m 이 홀수일것이 필요하고 충분하다.

증명 $h(X):=1+X+X^4(\in \mathbf{F}_{2^{2m}}[X])$ 으로 놓고 다항식 $f(X)$ 를 $X^5h(X^{2^m-1})$ 으로 표시하자. 그러면 정리 1에 의하여 $f(X)$ 가 $\mathbf{F}_{2^{2m}}$ 우에서의 치환다항식이기 위하여서는 $\gcd(5,\ 2^m-1)=1$ 이 성립하고 $g(x):=x^5h(x)^{2^m-1}$ 이 μ_{2^m+1} 우에서의 치환일것이 필요하고 충분하다.

충분성을 밝히기 위하여 m 이 홀수라고 가정하자. 그러면 $\gcd(5,\ 2^m-1)=1$ 이다. 그리고 정리 2로부터 알수 있는것처럼 μ_{2^m+1} 의 그 어떤 원소도 $h(X)$ 의 뿌리는 아니므로 $g(\mu_{2^m+1})\subseteq \mu_{2^m+1}$ 이 성립한다.

한편 임의의 $\alpha(\in \mu_{2^m+1})$ 에 대하여

$$g(\alpha)=\frac{\alpha+\alpha^4+\alpha^5}{1+\alpha+\alpha^4}$$

이 성립한다는것을 밝힐수 있다.

이제

$$G(x):=\frac{x+x^4+x^5}{1+x+x^4} \tag{4}$$

으로 정의하고 $G(x)$가 μ_{2^m+1}에서 1대1이라는것을 밝히자.

서로 다른 어떤 $x,\ y(\in\mu_{2^m+1})$에 대하여 $G(x)=G(y)$라고 가정하자. 그러면 식 (4)로부터 다음의 식이 성립한다.

$$(x+x^4+x^5)(1+y+y^4)+(y+y^4+y^5)(1+x+x^4)=0$$

즉

$$(x^5+y^5)+xy(x^4+y^4)+x^4y^4(x+y)+(x^4+y^4)+(x+y)=0$$

한편

$$x^5+y^5=(x+y)^5+x^2y^2(x+y)+xy(x+y)^3$$

이라는 사실을 리용하면 다음의 식이 얻어진다.

$$\frac{1}{(x+y)^4}+\left(\frac{xy}{x+y}\right)^5+\frac{1}{x+y}+\frac{xy}{x+y}+\left(\frac{xy}{(x+y)^2}\right)^2+\frac{xy}{(x+y)^2}+1=0$$

그러면

$$a:=\frac{1}{x+y},\ b:=a^2=\frac{xy}{x+y}$$

로 놓음으로써 웃식을 다음과 같이 쓸수 있다.

$$(a+b)^4+a+b+a^2b^2+ab+1=0 \tag{5}$$

물론 $a,\ b\in\mathbf{F}_{2^m}$이지만 $a+b,\ ab\in\mathbf{F}_{2^m}$이라는 사실을 리용하면 다음의 식이 얻어진다.

$$Tr_1^m((a+b)^4)+Tr_1^m(a+b)+Tr_1^m((ab)^2)+Tr_1^m(ab)+1=0 \tag{6}$$

그런데

$$Tr_1^m((a+b)^4)=Tr_1^m(a+b),\ \ Tr_1^m((ab)^2)=Tr_1^m(ab)$$

가 성립하므로 식 (6)으로부터 1=0이라는 모순이 나온다.

필요성을 밝히기 위하여 m이 짝수라고 가정하자. 그러면 $5|(2^m-1)$ 즉 2^m-1 또는 2^m+1가운데서 적어도 하나가 5로 완제된다. 만일 $5|(2^m-1)$이면 정리 1에 의하여 $f(X)$는 치환다항식이 아니다. 반면에 $5|(2^m+1)$이면 단위원소의 원시5차뿌리 $\zeta(\in\mu_{2^m+1})$에 대하여 $g(\zeta)=(1+\zeta+\zeta^4)^{2^m-1}=g(\zeta^4)$ 이고 $g(\zeta^2)=(1+\zeta^2+\zeta^3)^{2^m-1}=g(\zeta^3)$ 이 성립하므로 $g(x)$는 μ_{2^m+1}의 치환이 아니며 따라서 $f(X)$가 $\mathbf{F}_{2^{2m}}$ 우에서의 치환다항식이라는 가정에 모순되는 결과가 얻어진다.(증명끝)

실례 2 $\mathbf{F}_{2^6}$을 생각하면 $m=3$으로서 m은 홀수이다. 이때 3항식 $X^5+X^{2^m+4}+X^{4\cdot 2^m+1}$은 정리 5의 조건을 만족시키는 다항식으로서 실지 $\mathbf{F}_{2^6}$ 우에서의 치환다항식이다.

정리 6 다항식 $f(X):=X^3+X^{3\cdot 2^m}+X^{2^{m+2}-1}(\in\mathbf{F}_{2^{2m}}[X])$이 $\mathbf{F}_{2^{2m}}$ 우에서의 치환다항식이기 위하여서는 m이 홀수일것이 필요하고 충분하다.

증명 $h(X):=1+X^3+X^4(\in\mathbf{F}_{2^{2m}}[X])$으로 놓고 다항식 $f(X)$를 $X^5h(X^{2^m-1})$으로 표시하자. 그러면 정리 1에 의하여 $f(X)$가 $\mathbf{F}_{2^{2m}}$ 우에서의 치환다항식이기 위하여서는 $\gcd(3,\ 2^m-1)=1$이 성립하고 $g(X):=x^3h(X)^{2^m-1}$이 μ_{2^m+1}우에서의 치환다항식일것이 필요

하고 충분하다. 그런데 $\gcd(3,\ 2^m-1)=1$ 이라는것은 m 이 홀수라는것과 동등하므로 m 이 홀수이면 $g(x)$ 가 μ_{2^m+1} 에서의 치환이라는것만을 밝히면 된다.

m 이 홀수라고 하자. 그러면 정리 2에 의하여 $h(X)$ 는 μ_{2^m+1} 에서 뿌리를 가지지 않는다.

한편 임의의 $\alpha(\in\mu_{2^m+1})$ 에 대하여

$$g(\alpha)=\frac{1+\alpha+\alpha^4}{\alpha+\alpha^4+\alpha^5}$$

이 성립하므로 $g(x)$ 가 μ_{2^m+1} 의 치환이기 위하여서는 $G(x):=(1+x+x^4)/(x+x^4+x^5)$ 이 μ_{2^m+1} 에서 1대1일것이 필요하고 충분하다. 정리 5의 증명에서의 $G(x)$ 를 $G_2(x)$ 로 표시하면 임의의 $\alpha(\in\mu_{2^m+1})$ 에 대하여 $G(\alpha)=1/G_2(\alpha)$ 이 성립한다는것을 알수 있다. 그리고 m 이 홀수이므로 정리 5의 증명과정으로부터 $G_2(x)$ 는 μ_{2^m+1} 에서 1대1이며 따라서 $G(x)$ 는 μ_{2^m+1} 에서 1대1이라는것을 알수 있다.(증명끝)

참 고 문 헌

[1] X. Hou; Finite Fields Appl., 35, 16, 2015.

[2] J. B. Lee, Y. H. Park; Acta Math. Sci., 17, 250, 1997.

[3] M. Zieve; Int. J. Number Theory, 4, 851, 2008.

주체107(2018)년 3월 10일 원고접수

Constructing Four Classes of Permutation Trinomials over Finite Fields of Characteristic 2

Kim Kwang Yon, Song Ok Hyon

In this paper, we show properties of roots of four trinomials over finite fields with characteristic 2. Using this result, we construct four new classes of permutation trinomials.

Key words: characteristic, trinomial, permutation polynomial