김일성종합대학학보 주체107(2018)년
수 학 제64권 제4호

표수 2인 유한체우에서 2차변환을 리용한 1−불변다항식의 구성

손향심, 김률

경애하는 최고령도자 **김정은**동지께서는 다음과 같이 말씀하시였다.

《우리는 과학기술강국건설에 박차를 가하여 짧은 기간에 나라의 과학기술발전에서 새로운 비약을 이룩하며 과학으로 흥하는 시대를 열고 사회주의건설에서 혁명적전환을 가져와야 합니다.》(《조선로동당 제7차대회에서 한 중앙위원회사업총화보고》 단행본 38페지)

유한체의 불변토대와 불변원소, 불변다항식에 대해서는 지금까지 많은 연구가 진행되였으며 선행연구[3]에서 불변원소의 개념을 일반화한 k−불변원소의 개념을 내놓은 후 표수차변환들을 리용한 불변다항식과 k−불변다항식의 구성문제들이 연구되고있다.

정의 q를 씨수의 제곱, $\mathbf{F}_q$를 q개의 원소를 가진 유한체, $\mathbf{F}_{q^n}$을 $\mathbf{F}_q$의 n차확대체라고 하자. 원소 $\alpha\in\mathbf{F}_{q^n}$에 대하여

$$\deg\left(\gcd\left(x^n-1,\ \sum_{i=0}^{n-1}\alpha^{q^i}x^{n-1-i}\right)\right)=k$$

일 때 α를 $\mathbf{F}_q$에 관한 $\mathbf{F}_{q^n}$의 $k-$불변원소라고 부르며 n차기약다항식 $f(x)\in\mathbf{F}_q[x]$의 뿌리들이 $\mathbf{F}_q$에 관한 $k-$불변원소일 때 $f(x)$를 $\mathbf{F}_q$에 관한 $k-$불변다항식 또는 N_k-다항식이라고 부른다.[2, 3] $0-$불변원소, $0-$불변다항식(N_0-다항식)이 바로 불변원소, 불변다항식($N-$다항식)이다.

선행연구[1]에서는 표수 2인 유한체우에서 변환 $(x^2+x+1)/x^2$을 리용한 $N-$다항식렬구성법을 제기하고 선행연구[2]에서는 표수 2인 유한체우에서 변환 $(x^2+\delta^2)/x$을 리용한 N_1-다항식렬구성법을 내놓았다.

론문에서는 선행연구[1]에서 구성한 다항식렬의 초기다항식이 N_1-다항식이면 N_1-다항식렬을 얻을수 있다는것을 밝히고 2차변환 $(x^2+ax+b^2)/cx$을 리용하여 주어진 $N-$다항식으로부터 차수가 2배인 새로운 $N-$다항식을 구성할수 있다는것을 보여준다.

$n=n_1p^e,\ \gcd(n_1,\ p)=1\ (e\geq 0)$이라고 하고 p^e을 t로 표시하자. x^n-1이 $\mathbf{F}_q$에서

$$x^n-1=(x^{n_1}-1)^{p^e}=(\varphi_1(x)\cdots\varphi_r(x))^t \tag{1}$$

로 기약인수분해된다고 하자. 여기서 $\varphi_i(x)$들은 $x^{n_1}-1$의 서로 다른 기약인수들이다. 매 $k\ (1\leq k<n)$에 대하여 $R_{k,1}(x),\cdots,\ R_{k,u_k}(x)$들을 x^n-1의 서로 다른 k차인수전부라고 하면 $u_k>0$인 매 k에 대하여

$$R_{k,j}(x)=\prod_{i=1}^{r}\varphi_i^{t_{ij}},\ k=\sum_{i=1}^{r}\deg(\varphi_i)t_{ij}\ (0\leq t_{ij}\leq t,\ 1\leq j\leq u_k)$$

로 쓸수 있다.

$$\Phi_{k,j}(x)=\frac{x^n-1}{R_{k,j}(x)}=\sum_{m=0}^{n-k}b_{jm}x^m$$

으로 놓고 $L_{\Phi_{k,j}}(x)$를

$$L_{\Phi_{k,j}}(x)=\sum_{m=0}^{n-k}b_{jm}x^{q^m}$$

으로 정의된 선형화다항식이라고 하면 다음의 사실이 성립한다.

보조정리[2] $F(x)$를 $\mathbf{F}_q$ 우의 n차기약다항식, α를 $\mathbf{F}_{q^n}$에서 $F(x)$의 뿌리라고 하자. 이때 $F(x)$가 $\mathbf{F}_q$ 우의 N_k − 다항식이기 위해서는 어떤 $j\ (1\le j\le u_k)$가 있어서 $L_{\Phi_{k,j}}(\alpha)=0$이고 $u_l>0$인 매 $l\,(k<l<n)$과 모든 $j\ (1\le j\le u_l)$에 대하여 $L_{\Phi_{l,j}}(\alpha)\ne 0$일것이 필요하고 충분하다.

정리 1 n을 짝수, $P(x)=\sum_{i=0}^{n}c_ix^i\in\mathbf{F}_{2^s}[x]$를 N_1 − 다항식, $P(x+1)$은 자기상반다항식이라고 하자. 이때 다항식 $F(x)=x^{2n}P((x^2+x+1)/x^2)$이 $\mathbf{F}_{2^s}$ 우의 $2n$차 N_1 − 다항식이기 위해서는 $Tr_{2^s|2}(c_{n-1}/c_n)\ne 0$일것이 필요하고 충분하다.

증명 $P(x)$가 $\mathbf{F}_{2^s}$ 우의 n차기약다항식일 때 $F(x)$가 $\mathbf{F}_{2^s}$ 우에서 기약이기 위해서는 $Tr_{2^s|2}(c_{n-1}/c_n+n)\ne 0$ 일것이 필요하고 충분[1]하므로 n이 짝수라는데로부터 필요성은 분명하고 조건 $Tr_{2^s|2}(c_{n-1}/c_n)\ne 0$을 만족시킬 때 $F(x)$는 $\mathbf{F}_{2^s}$ 우에서 기약이다.

α를 $\mathbf{F}_{2^{sn}}$에서 N_1 − 다항식 $P(x)$의 뿌리라고 하면 보조정리에 의하여 어떤 $j\,(1\le j\le u_1)$가 있어서 $L_{\Phi_{1,j}}(\alpha)=0$이고 $u_l>0$인 매 $l\,(1<l<n)$과 모든 $j\,(1\le j\le u_l)$에 대하여 $L_{\Phi_{l,j}}(\alpha)\ne 0$이다. 식 (1)로부터 $x^{2n}-1$은 $x^{2n}-1=(\varphi_1(x)\cdots\varphi_r(x))^{2t}$으로 기약인수분해되고 매 $k'\,(1\le k'<2n)$에 대하여 $R'_{k',1}(x),\ \cdots,\ R'_{k',u'_{k'}}(x)$들을 $x^{2n}-1$의 서로 다른 k'차인수전부라고 하면 $u'_{k'}>0$인 매 k'에 대하여

$$R'_{k',j'}(x)=\prod_{i=1}^{r}\varphi_i^{t'_{ij'}}(x),\ k'=\sum_{i=1}^{r}\deg(\varphi_i)t'_{ij'}\ \ (0\le t'_{ij'}\le 2t,\ 1\le j'\le u'_{k'})$$

로 쓸수 있다.

$$H'_{k',j'}(x)=\frac{x^{2n}-1}{R'_{k',j'}(x)}\ \ (1\le j'\le u'_{k'})$$

로 놓자. 그리고 $k\ (1\le k<n)$와 $j\,(1\le j\le u_k)$에 대하여

$$H_{k,j}(x)=\frac{x^{2n}-1}{R_{k,j}(x)}=\frac{(x^n+1)(x^n-1)}{R_{k,j}(x)}=(x^n+1)\sum_{m=0}^{n-k}b_{jm}x^m=\sum_{m=0}^{n-k}b_{jm}(x^{n+m}+x^m)$$

이고 $F(x)$의 $\mathbf{F}_{2^{2sn}}$에서의 뿌리 α_1에 대하여

$$L_{H_{k,j}}(\alpha_1)=\sum_{m=0}^{n-k}b_{jm}(\alpha_1^{2^{sn}}+\alpha_1)^{2^{sm}}$$

이다.

한편 $(\alpha_1^2+\alpha_1+1)/\alpha_1^2$ 은 $P(x)$ 의 뿌리이므로 $P(x)$ 의 어떤 뿌리 α 에 대하여 $(\alpha_1^2+\alpha_1+1)/\alpha_1^2=\alpha$ 이고 따라서

$$\frac{1}{\alpha_1}+\frac{1}{\alpha_1{}^2}=1+\alpha \tag{2}$$

이다. 량변을 2^{sn} 제곱하면

$$\frac{1}{\alpha_1{}^{2^{sn}}}+\frac{1}{\alpha_1{}^{2^{sn+1}}}=1+\alpha \tag{3}$$

이다. 식 (2), (3)으로부터

$$\frac{1}{\alpha_1}+\frac{1}{\alpha_1{}^{2^{sn}}}=\left(\frac{1}{\alpha_1}+\frac{1}{\alpha_1{}^{2^{sn}}}\right)^2$$

이 나온다. $1/\alpha_1$ 은 $\mathbf{F}_{2^s}$ 우의 $2n$ 차기약다항식의 상반다항식의 뿌리이므로 $1/\alpha_1+1/\alpha_1^{2^{sn}}\neq 0$ 이고 따라서 웃식으로부터 $1/\alpha_1+1/\alpha_1^{2^{sn}}=1$ 즉 $\alpha_1{}^{2^{sn}}=\alpha_1/(1+\alpha_1)$ 이다. 이로부터

$$\alpha_1{}^{2^{sn}}+\alpha_1=\frac{\alpha_1}{1+\alpha_1}+\alpha_1=\frac{\alpha_1+\alpha_1+\alpha_1{}^2}{1+\alpha_1}=\frac{\alpha_1{}^2}{1+\alpha_1}=\frac{1}{1+\alpha}$$

이고

$$L_{H_{k,j}}(\alpha_1)=\sum_{m=0}^{n-k}b_{jm}(\alpha_1{}^{2^{sn}}+\alpha_1)^{2^{sm}}=\sum_{m=0}^{n\text{-}k}b_{jm}\left(\frac{1}{1+\alpha}\right)^{2^{sm}}=L_{\Phi_{k,j}}\left(\frac{1}{1+\alpha}\right)$$

이다.

$P(x)$ 의 차수가 짝수이므로 선행연구[2]의 정리 3.1의 증명과정으로부터 $L_{\Phi_{k,j}}(\alpha)=L_{\Phi_{k,j}}(1+\alpha)$ 이고 $P(1+x)$ 가 자기상반기약다항식이므로 $1/(1+\alpha)$ 은 $1+\alpha$ 의 공액원소이다.

가정에 의하여 $L_{\Phi_{1,j}}(\alpha)=0$ 이므로 $L_{\Phi_{1,j}}(1+\alpha)=0$ 이고 $L_{\Phi_{1,j}}(1/(1+\alpha))=L_{H_{1,j}}(\alpha_1)=0$ 이다. 이로부터 $L_{H'_{1,j}}(\alpha_1)=L_{H_{1,j}}(\alpha_1)=0$ 이다.

또한 $1<k<n,\ 1\le j\le u_k$ 에 대하여 $L_{\Phi_{k,j}}(\alpha)=L_{\Phi_{k,j}}(1+\alpha)\neq 0$ 이므로 $L_{\Phi_{k,j}}(1/(1+\alpha))=L_{H_{k,j}}(\alpha_1)\neq 0$ 이다. 이제 $u'_{k'}>0$ 인 때 $k'\ (1<k'<2n)$ 에 대하여 $L_{H'_{k',j'}}(\alpha_1)\neq 0\ (1\le j'\le u'_{k'})$ 을 증명하면 된다.

$R'_{k',j'}(x)=\prod_{i=1}^{r}\varphi_i^{t'_{i,j'}}(x)$ 에서 $t'_{i,j'}>t$ 인 $t'_{i,j'}$ 들을 $t'_{i,j'}=t$ 라고 할 때 얻어지는 다항식을 $R_{k_0,j_0}(x)$ 로 놓으면 $1<k_0\le n,\ 1\le j_0\le u_{k_0}$ 이다. 그러면 $R_{k_0,j_0}(x)$ 가 $R'_{k',j'}(x)$ 를 완제하므로 $H'_{k',j'}(x)$ 는 $H_{k_0,j_0}(x)$ 를 완제하고 선형다항식의 성질에 의하여 $L_{H'_{k',j'}}(x)$ 는 $L_{H_{k_0,j_0}}(x)$ 를 완제한다. $k_0<n$ 이면 우에서 본것처럼 $L_{H_{k_0,j_0}}(\alpha_1)=L_{\Phi_{k_0,j_0}}(1/(1+\alpha))\neq 0$ 이고 $k_0=n$ 이면 $H_{k_0,j_0}(x)=x^n-1$, $L_{H_{k_0,j_0}}(\alpha_1)=\alpha_1^{2^{sn}}-\alpha_1\neq 0$ 이므로 $L_{H'_{k',j'}}(\alpha_1)\neq 0$ 이다.(증명끝)

정리 1의 결과를 리용하면 N_1-다항식들의 반복구성법을 다음과 같이 얻을수 있다.

정리 2 $P(x)=\sum_{i=0}^{n}c_i x^i \in \mathbf{F}_{2^s}[x]$ 가 짝수차 N_1- 다항식이고 $P(x+1)$ 이 자기상반다항식이라고 하자. 이때 다항식렬

$$F_1(x)=x^{2n}P\left(\frac{x^2+x+1}{x^2}\right)$$

$$\cdots$$

$$F_k(x)=x^{n2^k}F_{k-1}\left(\frac{x^2+x+1}{x^2}\right)$$

이 $\mathbf{F}_{2^s}$ 에서 N_1- 다항식렬이기 위해서는 $Tr_{2^s|2}\left(\frac{c_{n-1}}{c_n}\right)Tr_{2^s|2}\left(\frac{P'(1)}{P(1)}\right)\neq 0$ 일것이 필요하고 충분하다.

증명 $P(x)$ 가 기약다항식일 때 이 다항식렬이 기약다항식렬이기 위해서는 $Tr_{2^s|2}\left(\frac{c_{n-1}}{c_n}\right)Tr_{2^s|2}\left(\frac{P'(1)}{P(1)}\right)\neq 0$ 일것이 필요하고 충분[1]하므로 이 조건을 만족시킬 때 N_1- 다항식렬이라는것을 증명하면 된다.

정리 1에 의하여 $F_1(x)$ 는 N_1- 다항식이다. 이제 $F_k(x)$ $(k\geq 1)$ 가 N_1- 다항식이라고 가정하고 $F_{k+1}(x)=x^{n2^{k+1}}F_k\left(\frac{x^2+x+1}{x^2}\right)$ 이 N_1- 다항식이라는것을 증명하자. $F_k(x+1)$ 은 분명히 자기상반다항식이므로 $F_{k+1}(x)$ 가 N_1- 다항식이기 위해서는 $Tr_{2^s|2}\left(\frac{F_k^{*\prime}(0)}{F_k^*(0)}\right)\neq 0$ 일것이 필요하고 충분하다. 여기서 $F_k^*(x)$ 는 $F_k(x)$ 의 상반다항식이다.

$$F_k^*(x)=x^{n2^k}F_k\left(\frac{1}{x}\right)=x^{n2^k}\frac{1}{x^{n2^k}}F_{k-1}\left(\frac{x^{-2}+x^{-1}+1}{x^{-2}}\right)=F_{k-1}(x^2+x+1)$$

이므로 $F_k^*(0)=F_{k-1}(1),\ F_k^{*\prime}(0)=F'_{k-1}(1)$ 이고

$$F_{k-1}(x)=x^{n2^{k-1}}F_{k-2}\left(\frac{x^2+x+1}{x^2}\right)$$

이므로 $F_{k-1}(1)=F_{k-2}(1)$ 이며

$$F'_{k-1}(x)=x^{n2^{k-1}-2}F'_{k-2}\left(\frac{x^2+x+1}{x^2}\right)$$

이므로 $F'_{k-1}(1)=F'_{k-2}(1)$ 이다. 여기서 $F_0(x)=P(x)$ 이다. 이로부터

$$Tr_{2^s|2}\left(\frac{F_k^{*\prime}(0)}{F_k^*(0)}\right)=Tr_{2^s|2}\left(\frac{P'(1)}{P(1)}\right)$$

이고 가정에 의하여 $Tr_{2^s|2}\left(\frac{P'(1)}{P(1)}\right)\neq 0$ 이다. 따라서 $F_{k+1}(x)$ 는 N_1- 다항식이다.(증명끝)

실례로 $P(x)=x^6+\alpha x^5+x^4+\alpha x^3+x^2+\alpha x+\alpha \in \mathbf{F}_{2^2}[x]$ 는 정리 2의 조건을 만족시키는

초기다항식이다. 여기서 α 는 $\alpha^2+\alpha+1=0$ 을 만족시키는 $\mathbf{F}_{2^2}$ 의 원소이다.

$$P(x+1)=x^6+\alpha x^5+\alpha x^4+\alpha x^3+\alpha x^2+\alpha x+1\in\mathbf{F}_{2^2}[x]$$

는 자기상반다항식이며

$$Tr_{2^2|2}(\alpha)Tr_{2^2|2}\left(\frac{P'(1)}{P(1)}\right)=(\alpha+\alpha^2)Tr_{2^2|2}(\alpha)=(\alpha+\alpha+1)(\alpha+\alpha+1)=1$$

이고 $P(x)$ 가 N_1-다항식이라는것을 보조정리의 판정법을 써서 확인할수 있다.

다음으로 표수 2인 유한체에서 주어진 $N-$다항식으로부터 어떤 2차변환에 의하여 새로운 $N-$다항식을 얻는 방법을 보자.

정리 3 $P(x)=\sum_{i=0}^{n}c_ix^i\in\mathbf{F}_{2^s}[x]$ 가 $N-$다항식이고 $a,\ b,\ c(\neq 0)\in\mathbf{F}_{2^s}$ 이라고 하자. 이때 다항식 $F(x)=x^nP\left(\frac{x^2+ax+b^2}{cx}\right)$이 $N-$다항식이기 위해서는

$$\left(na+c\frac{c_{n-1}}{c_n}\right)Tr_{2^s|2}\left(\frac{bP'(a/c)}{cP(a/c)}\right)\neq 0$$

일것이 필요하고 충분하다.

참 고 문 헌

[1] M. Alizadeh et al.; Turkish J. Math., 39, 259, 2015.

[2] M. Alizadeh; J. Algebra Appl., 16, 1, 1750006, 2017.

[3] S. Huczynska; Finite Fields Appl., 24, 170, 2013.

주체107(2018)년 6월 5일 원고접수

Construction of 1-Normal Polynomials using a Quadratic Transformation over Finite Fields of Characteristic 2

Son Hyang Sim, Kim Ryul

In this paper, we construct an infinite sequence of 1-normal polynomials using a certain quadratic transformation and present another quadratic transformation by which can obtain a new normal polynomial from a given one over a finite field of characteristic 2.

Key words: irreducible polynomial, normal polynomial