김일성종합대학학보 주체109(2020)년
수 학 제66권 제1호

유한체우에서 두가지 유리변환을 리용한 k-불변다항식렬의 귀납적구성

김률, 손향심

론문에서는 유한체리론에서 중요한 연구분야의 하나인 k-불변다항식의 구성에 대하여 연구하였다.

k-불변다항식은 유한체의 확대체의 구조를 밝히고 원소들사이의 연산을 고속화하는데서 중요한 다항식이다. 선행연구[4]에서는 일반적인 표수를 가진 유한체우에서 변환 $\left(\dfrac{x^p-x}{x^p-x+\delta}\right)$를 리용하여 k-불변다항식렬을 구성하는 방법을 제기하였으며 선행연구[1]에서는 변환 $\left(\dfrac{x^p-x^{p-1}+1}{-x^{p-1}+1}\right)$을 리용하여 불변다항식렬을 구성하는 방법을 제기하였다.

선행연구[2]에서는 표수 2인 유한체우에서 2차변환 $\left(\dfrac{x^2+x+1}{x^2}\right)$을 리용하여 1-불변다항식렬을 구성하는 방법을 제기하였다.

론문에서는 일반적인 표수를 가진 유한체우에서 변환 $\left(\dfrac{x^p-x^{p-1}+1}{-x^{p-1}+1}\right)$을 리용하여 k-불변다항식들의 렬을 귀납적으로 구성하는 방법을 제기하고 선행연구[2]에서 구성했던 1-불변다항식렬에서 초기다항식이 일반적인 k-불변다항식이면 k-불변다항식렬이 된다는것을 증명하였다.

q를 씨수 p의 s제곱, $\mathbf{F}_q$를 q개의 원소를 가진 유한체, $\mathbf{F}_{q^n}$을 $\mathbf{F}_q$의 n차확대체라고 하자.

정의[1] 원소 $\alpha\in\mathbf{F}_{q^n}$과 옹근수 k $(0\le k<n)$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.

선행연구[3, 5]에서는 기약다항식이 k-불변다항식($k>0$)이 되기 위한 다음의 판정조건을 제기하였다.

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

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

으로 기약인수분해된다고 할 때 매 l $(1\le l<n)$에 대하여 $R_{l,1}(x),\ \cdots,\ R_{l,u_{lk}}(x)$들을 x^n-1의 서로 다른 l차인수전부라고 하면 $u_l>0$인 매 l에 대하여

$$R_{l,j}(x)=\prod_{i=1}^{r}\varphi_i^{t_{ij}},\ l=\sum_{i=1}^{r}\deg(\varphi_i)t_{ij}\ \ (0\le t_{ij}\le t,\ 1\le j\le u_l)$$

로 쓸수 있다.

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

으로 놓고 $L_{\Phi_{l,j}}(x)$를

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

으로 정의된 선형화다항식이라고 하면 다음의 사실이 성립한다.

보조정리 1 [5] $F(x)$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 $k-$불변다항식이기 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.

보조정리 2 어떤 $e\ge 1$에 대하여 $n=n_1p^e$이고 $a,\ b\in\mathbf{F}_q$ $(b\ne 0)$이라고 하고 $0\le k<p^e-1$이라고 가정하자. 이때 원소 α가 $\mathbf{F}_q$에 관한 $\mathbf{F}_{q^n}$의 참$k-$불변원소이기 위해서는 $a+b\alpha$가 $\mathbf{F}_q$에 관한 $\mathbf{F}_{q^n}$의 참$k-$불변원소일것이 필요하고 충분하다.

정리 1 $P(x)=\sum_{i=0}^{n}c_ix^i\in\mathbf{F}_q[x]$ $(n=n_1p^e,\ \gcd(n_1,\ p)=1,\ e\ge 1)$를 모니크 $k-$불변다항식 $(0\le k<p^e-1)$이라고 하자. 이때 다항식

$$F(x)=(-x^{p-1}+1)^nP\left(\frac{x^p-x^{p-1}+1}{-x^{p-1}+1}\right)$$

이 $\mathbf{F}_q$우의 pn차$k-$불변다항식이기 위해서는 $\mathrm{Tr}_{q|p}\left(\frac{P'(1)}{P(1)}\right)\ne 0$일것이 필요하고 충분하다.

유리변환 $\left(\frac{x^p-x^{p-1}+1}{-x^{p-1}+1}\right)$을 리용하여 $k-$불변다항식들의 렬을 구성하는 방법을 제기한다.

정리 2 $P(x)=\sum_{i=0}^{n}c_ix^i\in\mathbf{F}_q[x]$ $(n=n_1p^e,\ \gcd(n_1,\ p)=1,\ e\ge 1)$를 모니크 $k-$불변다항식 $(0\le k<p^e-1)$이라고 하자. 이때 다항식렬

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

$$F_u(x)=(-x^{p-1}+1)^{np^{u-1}}\cdot F_{u-1}\left(\frac{x^p-x^{p-1}+1}{-x^{p-1}+1}\right)\ (u>1)$$

이 $\mathbf{F}_q$ 우에서 차수가 np^u 인 k-불변다항식렬이기 위해서는

$$\mathrm{Tr}_{q|p}\left(\frac{P'(1)}{P(1)}\right)\mathrm{Tr}_{q|p}(P^{*\prime}(0))\neq 0$$

일것이 필요하고 충분하다.

정리 3 $P(x)=\sum_{i=0}^{n}c_ix^i\in\mathbf{F}_{2^s}[x]$ $(n=n_12^e=n_1t,\ \gcd(n_1,\ 2)=1,\ e\geq 1)$ 가 k- 불변다항식 $(0\leq k<p^e-1)$ 이고 $P(x+1)$ 이 자기상반다항식이라고 하자. 이때 다항식

$$F(x)=(x^2+b^2)^nP\left(\frac{x^2+ax+b^2}{x^2+b^2}\right)$$

이 k-불변다항식이기 위해서는

$$\mathrm{Tr}_{2^s|2}\left(\frac{bc_{n-1}}{ac_n}\right)\neq 0$$

일것이 필요하고 충분하다. 여기서 $a,\ b\in\mathbf{F}_{2^s}^*$ 이다.

정리 4 $P(x)=\sum_{i=0}^{n}c_ix^i\in\mathbf{F}_{2^s}[x]$ 를 k-불변다항식 $(0\leq k<p^e-1)$, $P(x+1)$ 은 자기상반다항식이라고 하자. 이때 다항식

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

이 $\mathbf{F}_{2^s}$ 우의 $2n$ 차 k-불변다항식이기 위해서는

$$\mathrm{Tr}_{2^s|2}\left(\frac{c_{n-1}}{c_n}\right)\neq 0$$

일것이 필요하고 충분하다.

정리 4를 리용하면 선행연구[1]에서 구성하였던 1-불변다항식렬에서 초기다항식이 k-불변다항식일 때 일반적인 k-불변다항식렬이 된다는것을 알수 있다.

정리 5 $P(x)=\sum_{i=0}^{n}c_ix^i\in\mathbf{F}_{2^s}[x]$ $(n=n_12^e=n_1t,\ \gcd(n_1,\ 2)=1,\ e\geq 1)$ 가 k- 불변다항식 $(0\leq k<p^e-1)$ 이고 $P(x+1)$ 이 자기상반다항식이라고 하자.

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

$$\cdots\quad\cdots\quad\cdots$$

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

일 때 $\{F_u(x)\}_{u\geq 0}$ 과 $\{F_u(x+1)\}_{u\geq 0}$ 이 각각 $\mathbf{F}_{2^s}$ 에 관한 $k-$불변다항식 및 자기상반 $k-$불변다항식렬이기 위해서는

$$\mathrm{Tr}_{2^s|2}\left(\frac{c_{n-1}}{c_n}\right)\mathrm{Tr}_{2^s|2}\left(\frac{P'(1)}{P(1)}\right)\neq 0$$

일것이 필요하고 충분하다.

참 고 문 헌

[1] 김일성종합대학학보 수학, 65, 1, 80, 주체108(2019).

[2] 김일성종합대학학보 수학, 64, 4, 54, 주체107(2018).

[3] S. Abrahamyan et al.; Finite Fields Appl., 18, 738, 2012.

[4] M. Alizadeh et al.; Italian Journal of Pure and Applied Mathematics, 39, 451, 2018.

[5] M. Alizadeh; J. Algebra Appl., 16, 1, 11, 2017.

주체108(2019)년 9월 15일 원고접수

The Recursive Method for Constructing Sequences of $k-$Normal Polynomials Using Two Rational Transformations over Finite Fields

Kim Ryul, *Son Hyang Sim*

In this paper, we present the method for constructing the sequence of the $k-$normal polynomials using a rational transformation $\left(\frac{x^p - x^{p-1}+1}{-x^{p-1}+1}\right)$ over finite fields. And we construct the infinite sequence of $k-$normal polynomials using the transformation $\left(\frac{x^2+x+1}{x^2}\right)$ starting from the suitable $k-$normal polynomial over finite field of characteristic 2.

Keywords: finite field, $k-$normal polynomial