한가지 유리변환을 리용한 불변다항식렬의 귀납적구성

김룔, 손향심

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

《현시대는 과학기술의 시대이며 과학기술의 발전수준은 나라의 종합적국력과 지위를 규정하는 징표로 됩니다.》(《조선로동당 제7차대회에서 한 중앙위원회사업총화보고》 단행본 38페지)

우리는 유한체리론과 응용에서 매우 중요한 유한체에 기초한 기약다항식과 불변다항식에 대하여 연구하였다.

여기서는 q를 표수 p의 s제곱, $\mathbf{F}_q$를 q개의 원소를 가진 유한체, $\mathbf{F}_{q^n}$을 $\mathbf{F}_q$의 n차 확대체라고 가정한다.

정의[3] 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.

또한 $0-$불변원소, $0-$불변다항식(N_0-다항식)을 보통 불변원소, 불변다항식($N-$다항식)이라고 부른다.

선행연구[3]에서는 표수 2인 유한체우에서 변환 $(x^2+\delta^2)/x$을 리용하여 불변다항식렬을 구성하였으며 선행연구[2]에서는 유한체우에서 변환 $(x^p-x+\delta_0)/(x^p-x+\delta_1)$ $(\delta_1\neq 0)$을 리용한 기약다항식렬의 구성법을 제기하고 $k-$불변다항식렬을 구성하였다.

론문에서는 새로운 형태의 표수차변환을 리용하여 기약다항식렬을 구성하고 초기다항식이 불변다항식일 때 이 기약다항식렬이 불변다항식렬이 된다는것을 보여준다.

보조정리 1 $f(x),\ g(x)\in\mathbf{F}_q[x]$이고 $P(x)\in\mathbf{F}_q[x]$는 n차기약다항식이라고 하자. 이때 다항식 $F(x):=g^n(x)P(f(x)/g(x))$가 $\mathbf{F}_q$우에서 기약이기 위해서는 $P(x)$의 어떤 뿌리 $\alpha\in\mathbf{F}_{q^n}$에 대하여 $f(x)-\alpha g(x)$가 $\mathbf{F}_{q^n}$우에서 기약일것이 필요하고 충분하다.

보조정리 2 $b\in\mathbf{F}_q$일 때 3항식 x^p-x-b가 $\mathbf{F}_q$우에서 기약이기 위해서는 $\mathrm{Tr}_{q^n/p}(b)\neq 0$일것이 필요하고 충분하다.

정리 1 $P(x)=\sum_{i=0}^{n}c_ix^i\in\mathbf{F}_q[x]$가 기약다항식일 때 $F(x)=(-x^{p-1}+1)^n\cdot P\left(\frac{x^p-x^{p-1}+1}{-x^{p-1}+1}\right)$이 $\mathbf{F}_q$우에서 기약다항식이 위해서는 $\mathrm{Tr}_{q/p}(P'(1)/P(1))\neq 0$일것이 필요하고 충분하다.

증명 $F(x)=(-x^{p-1}+1)^n\cdot P\left(\frac{x^p-x^{p-1}+1}{-x^{p-1}+1}\right)$이 $\mathbf{F}_q$우에서 기약이기 위해서는 $P(x)\in\mathbf{F}_q[x]$의 어떤 뿌리 $\alpha\in\mathbf{F}_{q^n}$에 대하여 $g(x):=x^p-x^{p-1}+1-\alpha(-x^{p-1}+1)=x^p-(1-\alpha)x^{p-1}+(1-\alpha)$가 $\mathbf{F}_{q^n}$우에서 기약일것이 필요하고 충분하다.

한편 다항식 $g(x)$의 기약성과 그것의 상반다항식의 상수배인

$$g^*(x)/g(0)=x^p g(1/x)/g(0)=x^p-x-1/(\alpha-1)\in\mathbf{F}_{q^n}[x]$$

의 기약성은 동등하다.[1]

보조정리 2에 의하여 $g^*(x)/g(0)$가 $\mathbf{F}_{q^n}$ 우에서 기약이기 위해서는 $\mathrm{Tr}_{q^n/p}(1/(\alpha-1))\neq 0$ 일것이 필요하고 충분하다.

α가 $P(x)$의 뿌리이므로 $\alpha-1$은 $P(x+1)$의 뿌리, $1/(\alpha-1)$은 $(P(x+1))^*$의 뿌리이다.

따라서 $\mathrm{Tr}_{q^n/p}(1/(\alpha-1))=\mathrm{Tr}_{q/p}(\mathrm{Tr}_{q^n/q}(1/(\alpha-1)))=-\mathrm{Tr}_{q/p}(P'(1)/P(1))$ 이다. 즉 $F(x)$가 $\mathbf{F}_q$ 우에서 기약다항식이 위해서는 $\mathrm{Tr}_{q/p}(P'(1)/P(1))\neq 0$ 일것이 필요하고 충분하다.(증명끝)

정리 2 $P(x)=\sum_{i=0}^{n}c_ix^i\in\mathbf{F}_q[x]$가 모니크기약다항식이라고 할 때 다항식렬

$$F_1(x)=(-x^{p-1}+1)^n\cdot P\left(\frac{x^p-x^{p-1}+1}{-x^{p-1}+1}\right),\ F_k(x)=(-x^{p-1}+1)^{np^{k-1}}\cdot F_{k-1}\left(\frac{x^p-x^{p-1}+1}{-x^{p-1}+1}\right)\quad(k>1)$$

이 $\mathbf{F}_q$ 우에서 기약다항식렬이기 위해서는 $\mathrm{Tr}_{q/p}(P'(1)/P(1))\mathrm{Tr}_{q/p}(n+P^{*'}(0))\neq 0$ 일것이 필요하고 충분하다.

선행연구[2]에서는 변환 $(x^p-x+\delta_0)/(x^p-x+\delta_1)$ $(\delta_1\neq 0)$을 리용하였지만 정리 2에서는 변환 $(x^p-x^{p-1}+1)/(-x^{p-1}+1)$을 리용하여 선행연구[2]에서의 기약다항식렬과 다른 기약다항식렬을 구성하였다.

정리 2에서의 $F_k(x)$의 상반다항식은 $F_k^*(x)=(x^p-x)^{np^{k-1}}F_{k-1}((x^p-x+1)/(x^p-x))$ 로서 이것도 선행연구[2]에서의 변환으로는 얻을수 없다.

다음으로 우에서 구성한 기약다항식렬에서 초기다항식이 불변다항식일 때 이 기약다항식렬이 불변다항식렬이 된다는것을 보자.

$n=n_1p^e$, $\gcd(n_1,\ p)=1,\ e\geq 0$이라고 하고 p^e을 t로 표시하자.

x^n-1이 $\mathbf{F}_q$에서 $x^n-1=(x^{n_1}-1)^{p^e}=(\varphi_1(x)\cdots\varphi_r(x))^t$로 기약인수분해된다고 하자. 여기서 $\varphi_i(x)$들은 $x^{n_1}-1$의 서로 다른 m_i차기약인수들이다.

$1\leq i\leq r$인 매 i에 대하여 $\Phi_i(x)=\dfrac{x^n-1}{\varphi_i(x)}=\sum_{\upsilon=0}^{m_i}t_{i\upsilon}x^\upsilon$ 으로 놓고 $L_{\Phi_i}(x)$를 $L_{\Phi_i}(x)=\sum_{\upsilon=0}^{m_i}t_{i\upsilon}x^{q^\upsilon}$ 으로 정의된 선형화다항식이라고 하면 다음의 사실이 성립된다.

보조정리 3[3] $F(x)$를 $\mathbf{F}_q$ 우의 n차기약다항식, α를 $\mathbf{F}_{q^n}$에서 $F(x)$의 뿌리라고 할 때 $F(x)$가 $\mathbf{F}_q$ 우의 불변다항식이기 위해서는 모든 $i,\ 1\leq i\leq r$에 대하여 $L_{\Phi_i}(\alpha)\neq 0$ 일것이 필요하고 충분하다.

정리 3 $P(x)=\sum_{i=0}^{n}c_ix^i\in\mathbf{F}_q[x]$ ($n=n_1p^e$, $\gcd(n_1,\ p)=1,\ e\geq 1$)를 모니크불변다항식이라고 할 때 다항식 $F(x)=(-x^{p-1}+1)P((x^p-x^{p-1}+1)/(-x^{p-1}+1))$이 $\mathbf{F}_q$ 우의 pn차불변다항식이

기 위해서는 $\mathrm{Tr}_{q/p}(P'(1)/P(1))\neq 0$ 일것이 필요하고 충분하다.

증명 $P(x)$ 가 $\mathbf{F}_q$ 우의 n 차기약다항식일 때 $F(x)$ 가 $\mathbf{F}_q$ 우에서 기약이기 위해서는 정리 1로부터 $\mathrm{Tr}_{q/p}(P'(1)/P(1))\neq 0$ 일것이 필요하고 충분하므로 필요성은 분명하고 충분성만 증명하면 된다.

조건 $\mathrm{Tr}_{q/p}(P'(1)/P(1))\neq 0$ 을 만족시킬 때 $F(x)$ 는 $\mathbf{F}_q$ 우에서 기약이다.

α 를 $\mathbf{F}_{q^n}$ 에서 불변다항식 $P(x)$ 의 뿌리라고 하면 보조정리 3에 의하여 모든 $i,\ 1\leq i\leq r$ 에 대하여 $L_{\Phi_i}(\alpha)\neq 0$ 이다. 그리고 $x^n-1=(x^{n_1}-1)^{p^e}=(\varphi_1(x)\cdots\varphi_r(x))^t$ 으로부터 $x^{pn}-1$ 은 $x^{pn}-1=(\varphi_1(x)\cdots\varphi_r(x))^{pt}$ 으로 기약인수분해된다.

$H_i(x)=\dfrac{x^{pn}-1}{\varphi_i(x)},\ 1\leq i\leq r$ 로 놓자.

그러면 $H_i(x)=\dfrac{x^{pn}-1}{\varphi_i(x)}=\dfrac{(x^n-1)}{\varphi_i(x)}\left(\sum\limits_{j=0}^{p-1}x^{jn}\right)=\Phi_i(x)\left(\sum\limits_{j=0}^{p-1}x^{jn}\right)=\sum\limits_{\upsilon=0}^{m_i}t_{i\upsilon}\left(\sum\limits_{j=0}^{p-1}x^{jn+\upsilon}\right)$ 이다.

$F^*(x)$ 의 $\mathbf{F}_{q^{np}}$ 에서의 뿌리를 α_1 이라고 하면 $\beta_1=1/\alpha_1$ 은 $F(x)$ 의 뿌리이다.

$F^*(x)=x^{np}F\left(\dfrac{1}{x}\right)=(-x+x^p)^nP\left(\dfrac{1-x+x^p}{-x+x^p}\right)$ 이므로 $\dfrac{1-\alpha_1+\alpha_1^p}{-\alpha_1+\alpha_1^p}$ 은 $P(x)$ 의 뿌리이다. 따라서 $\alpha=\dfrac{\alpha_1^p-\alpha_1+1}{\alpha_1^p-\alpha_1}$ 로 놓으면 $\alpha_1^p-\alpha_1=\dfrac{1}{\alpha-1}$ 이며 량변을 q^n 제곱하면 $(\alpha_1^p-\alpha_1)^{q^n}=\dfrac{1}{\alpha-1}$ 이다.

이로부터 $(\alpha_1^{p^{sn}}-\alpha_1)^p=\alpha_1^{p^{sn}}-\alpha_1$ 이므로 $\theta:=\alpha_1^{p^{sn}}-\alpha_1\in\boldsymbol{F}_p$ 이다.

그러면 $\alpha_1^{p^{sn}}=\alpha_1+\theta,\ \alpha_1^{p^{2sn}}=(\alpha_1^{p^{sn}})^{p^{sn}}=(\alpha_1+\theta)^{p^{sn}}=\alpha_1^{p^{sn}}+\theta=\alpha_1+2\theta$ 이고 마찬가지로 $\alpha_1^{p^{jsn}}=\alpha_1+j\theta\ \ (0\leq j\leq p-1)$ 이다.

선행연구[2]에 의하여 $\sum\limits_{j=0}^{p-1}\dfrac{1}{\alpha_1+j\theta}=-\dfrac{1}{\alpha_1{}^p-\alpha_1}$ 이며 따라서 다음의 식이 성립된다.

$$L_{H_i}(\beta_1)=\sum_{\upsilon=0}^{m_i}t_{i\upsilon}\left(\sum_{j=0}^{p-1}\beta_1{}^{p^{s(jn+\upsilon)}}\right)=\sum_{\upsilon=0}^{m_i}t_{i\upsilon}\left(\sum_{j=0}^{p-1}\left(\frac{1}{\alpha_1}\right)^{p^{sjn}}\right)^{p^{s\upsilon}}=\sum_{\upsilon=0}^{m_i}t_{i\upsilon}\left(\sum_{j=0}^{p-1}\left(\frac{1}{\alpha_1+j\theta}\right)\right)^{p^{s\upsilon}}=$$

$$=\sum_{\upsilon=0}^{m_i}t_{i\upsilon}\left(-\frac{1}{\alpha_1{}^p-\alpha_1}\right)^{p^{s\upsilon}}=\sum_{\upsilon=0}^{m_i}t_{i\upsilon}(-(\alpha-1))^{p^{s\upsilon}}=\sum_{\upsilon=0}^{m_i}t_{i\upsilon}(1-\alpha)^{p^{s\upsilon}}=L_{\Phi_i}(1-\alpha)$$

선행연구[3]에 의하여 $n=n_1p^e,\ \gcd(n_1,\ p)=1,\ e\geq 1$ 일 때 α 와 $1-\alpha$ 의 불변성은 동등하고 조건에 의하여 모든 $i,\ 1\leq i\leq r$ 에 대하여 $L_{\Phi_i}(\alpha)\neq 0$ 이므로 $L_{\Phi_i}(1-\alpha)=L_{H_i}(\beta_1)\neq 0$ 이다. 따라서 보조정리 3에 의하여 $F(x)$ 는 $\mathbf{F}_q$ 에서 불변다항식이다.(증명끝)

정리 4 $P(x)=\sum\limits_{i=0}^{n}c_ix^i\in\mathbf{F}_q[x]$ 가 모니크불변다항식이고 $n=n_1p^e,\ \gcd(n_1,\ p)=1,\ e\geq 1$ 이라고 하자.

이때 다항식렬

$$F_1(x)=(-x^{p-1}+1)^n\cdot P\left(\frac{x^p-x^{p-1}+1}{-x^{p-1}+1}\right),\ F_k(x)=(-x^{p-1}+1)^{np^{k-1}}\cdot F_{k-1}\left(\frac{x^p-x^{p-1}+1}{-x^{p-1}+1}\right)\quad (k>1)$$

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

$$\mathrm{Tr}_{q/p}(P'(1)/P(1))\mathrm{Tr}_{q/p}(P^{*'}(0))\neq 0$$

일것이 필요하고 충분하다.

증명 우선 정리 2에 의하여 초기다항식의 차수가 표수의 배수일 때 $F_k(x)\ (k\geq 1)$ 가 기약다항식렬이기 위해서는 $\mathrm{Tr}_{q/p}(P'(1)/P(1))\mathrm{Tr}_{q/p}(P^{*'}(0))\neq 0$ 일것이 필요하고 충분하므로 이 조건을 만족시킬 때 불변다항식렬이 된다는것을 증명하면 된다.

정리 3에 의하여 $F_1(x)$ 는 불변다항식이다.

이제 $F_m(x)\ (1\leq m\leq k-1)$ 가 불변다항식일 때 $F_k(x)$ 가 불변다항식이 된다는것을 증명하자.

정리 3에 의하여 $F_k(x)$ 가 불변이기 위해서는 $\mathrm{Tr}_{q/p}(F'_{k-1}(1)/F_{k-1}(1))\neq 0$ 일것이 필요하고 충분하며 정리 2에 의하여 $F_{k-1}(1)=1$, $F'_{k-1}(1)=(-1)^{k-3}(p-1)(n+P^{*'}(0))$ 이고 $n=p^e n_1$, $e\geq 1$ 이므로 $\mathrm{Tr}_{q/p}(F'_{k-1}(1)/F_{k-1}(1))=(-1)^{k-3}(p-1)\mathrm{Tr}_{q/p}(P^{*'}(0))$ 이다.

정리의 가정에 의하여 $\mathrm{Tr}_{q/p}(P^{*'}(0))\neq 0$ 이므로 $F_k(x)$ 는 불변다항식이다.(증명끝)

참 고 문 헌

[1] 김률; 유한체, **김일성**종합대학출판사, 34～56, 주체100(2011).

[2] M. Alizadeh et al.; arXiv:1610.05684v1, 2016.

[3] M. K. Kyuregyan; Finite Fields Appl., 10, 323, 2004.

주체107(2018)년 9월 8일 원고접수

Recursive Construction of a Sequence of Normal Polynomials using a Rational Transformation

Kim Ryul, Son Hyang Sim

In this paper, a recursive method for constructing the irreducible polynomials of higher degree from a given irreducible polynomial over a finite field using a simple rational transformation is proposed. And when the initial polynomial is a normal one, we construct a sequence of normal polynomials.

Key words: finite field, irreducible polynomial, normal polynomial