김일성종합대학학보
(자연과학)
주체106(2017)년 제63권 제11호

JOURNAL OF **KIM IL SUNG** UNIVERSITY
(NATURAL SCIENCE)
Vol. 63 No. 11 JUCHE106(2017).

2진체에 기초한 몇가지 다항식토대의 흔적스펙트르

김 률

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

《기초과학은 과학기술강국을 떠받드는 주추입니다. 기초과학이 든든해야 나라의 과학기술이 공고한 토대우에서 끊임없이 발전할수 있습니다.》(《조선로동당 제7차대회에서 한 중앙위원회사업총화보고》 단행본 40페지)

우리는 정보통신에서의 암호화와 부호화에 쓰이는 유한체에 기초한 다항식토대의 흔적스펙트르에 대하여 연구하였다. 유한체의 원소의 흔적계산은 안전한 암호방안의 구성과 같은 많은 실천적문제들에서 제기되므로 흔적계산의 고속화를 위하여 유한체의 토대의 흔적스펙트르를 분석하는것은 실천적으로 중요하다.

선행연구[1]에서는 2진체 $\mathbf{F}_2$ 에 기초한 기약3항식 및 기약5항식토대에서 토대원소들의 흔적값과 흔적값이 1인 토대원소의 개수에 대하여 론의하였으며 선행연구[2]에서는 유한체 $\mathbf{F}_{2^n}$ 의 다항식토대의 흔적스펙트르를 분석하여 흔적값이 1인 원소의 개수가 지적된 값을 가지는 다항식토대의 존재성을 밝히고 그 결과를 적용하여 일정한 무게를 가진 기약다항식의 존재성을 증명하였다. 선행연구[3]에서는 유한체 $\mathbf{F}_{2^n}$ 에서 지적된 흔적스펙트르를 가지는 불변토대의 존재성문제를 론의한데 기초하여 지적된 흔적스펙트르를 가진 불변원소의 구성법에 대하여 론의하였다.

우리는 $\mathbf{F}_{2^n}$ 에서의 연산고속화에 리용되는 2진체 $\mathbf{F}_2$ 에 기초한 두가지 형태의 다항식토대의 흔적스펙트르를 분석한다.

정의 $K=\mathbf{F}_q$, $F=\mathbf{F}_{q^m}$, $\alpha\in F$ 라고 할 때 $\alpha+\alpha^q+\alpha^{q^2}+\cdots+\alpha^{q^{m-1}}$ 을 K 에 관한 원소 α 의 흔적이라고 부르고 $\mathrm{Tr}_{F/K}(\alpha)$ 또는 $\mathrm{Tr}_{q^m/q}(\alpha)$ 로 표시한다.

$\mathbf{F}_2$ 에 기초한 n 차다항식이 $f(x)=x^n+a_1x^{n-1}+\cdots+a_n=\sum_{i=0}^{n}a_ix^{n-i}\in\mathbf{F}_2[x]$ 로 주어졌다고 할 때 $f(x)$ 가 기약이면 $f(x)$ 의 항의 개수는 홀수이다.

론문에서는 n 이 3보다 작지 않은 홀수일 때 $\mathbf{F}_2$ 에 기초한 극대무게를 가지는 n 차기약다항식 $F_{n,\,m}=x^n+x^{n-1}+\cdots+x^{m+1}+x^{m-1}+\cdots+1$ 과 $\mathbf{F}_2$ 에 기초한 상수항과 홀수차항전체를 포함하는 n 차기약다항식 $F_n=x^n+x^{n-2}+\cdots+x+1$ 에 대응되는 다항식토대의 흔적스펙트르 즉 토대원소들의 흔적값렬을 분석한다.

일반적으로 유한체연산들은 령아닌 항의 개수가 작을수록 빨라진다.

우에서 지적된 두가지 형태의 다항식의 항의 개수는 작지 않다. 그러나 간단한 변환을 실시하여 주어진 기약다항식대신에 변환된 낮은 무게의 다항식을 리용하여 $\mathbf{F}_{2^n}$ 에서의 연산을 고속화할수 있다.

구체적으로는

$$G_{n,\,m}=F_{n,\,m}\cdot(x+1)=x^{n+1}+x^{m+1}+x^m+1,\ \ G_n=F_n\cdot(x^2+1)=x^{n+2}+x^2+x+1$$

로 $F_{n,\,m}$, F_n을 변환하여 연산고속화를 실현할수 있다.

$G_{n,\,m}$, G_n은 무게가 4이고 중간항들이 이웃하고있으므로 연산고속화에 적합하다.

$f(x)=x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$이 $\mathbf{F}_2$에 기초한 n차기약다항식이고 α를 $\mathbf{F}_{2^n}$에서 $f(x)$의 뿌리라고 하면 $\mathbf{F}_{2^n}$에서 $f(x)$의 뿌리들은 $x_i=\alpha^{2^i},\ 0\le i\le n-1$이다.

$k\ (0\le k\le n-1)$에 대하여 $S_k=\mathrm{Tr}(\alpha^k)$으로 놓으면 $f(x)=\prod_{i=0}^{n-1}(x-x_i),\ S_k=\sum_{i=0}^{n-1}x_i^k$이다.

여기서 Tr는 $\mathrm{Tr}_{2^n/2}$을 의미한다.

뉴톤의 공식에 의하여 $S_k=S_{k-1}a_1+S_{k-2}a_2+\cdots+S_1a_{k-1}+ka_k$가 성립된다.

$\mathbf{F}_{2^n}$의 다항식토대는 $N=\{1,\ \alpha,\ \alpha^2,\ \cdots,\ \alpha^{n-1}\}$이다.

이제 먼저 $F_{n,\,m}$에 대응되는 다항식토대원소들의 흔적값들을 고찰하자.

정리 1 $m=1$일 때 임의의 $k\ (0\le k\le n-1)$에 대하여 $\mathrm{Tr}(\alpha^k)=1$이다.

증명 n이 홀수이므로 $S_0=\mathrm{Tr}(1)=n \bmod 2=1$이다.

$m=1$이므로 $a_1=a_2=\cdots=a_{n-2}=a_n=1,\ a_{n-1}=0$이고 따라서 $S_1=a_1=1$이다.

이제 임의의 $i\ (0\le i\le k,\ 1\le k\le n-1)$에 대하여 $S_i=1$이 성립된다고 가정하자.

이때 뉴톤의 공식으로부터 $k \bmod 2=0$인 경우에는 $ka_k=0$이고 오른변의 령아닌 항의 개수가 홀수이므로 $S_k=1$이며 $k \bmod 2=1$인 경우에는 $ka_k=1$이므로 다시 오른변의 령아닌 항의 개수가 홀수로 되여 $S_k=1$이다.

따라서 임의의 $k\ (0\le k\le n-1)$에 대하여 $\mathrm{Tr}(\alpha^k)=1$이다.(증명끝)

정리 2 $m=1$일 때 임의의 $k\ (0\le k\le n-1)$에 대하여 $S_k=\begin{cases}1, & 3\mid k\\ 0, & 3\nmid k\end{cases}$이다.

증명 $S_0=\mathrm{Tr}(1)=n \bmod 2=1$이고 $m=n-1$이므로 $a_1=0,\ a_2=a_3=\cdots=a_n=1$이다.

또한 $S_1=a_1=0,\ S_2=S_1a_1+2a_2=0$이 성립된다.

이제 임의의 $i\ (0\le i<k,\ 1\le k\le n-1)$에 대하여 정리의 결과가 성립된다고 가정하자.

뉴톤의 공식으로부터 $S_k=S_{k-1}a_1+\cdots+S_1a_{k-1}+ka_k=S_{k-2}+\cdots+S_1+k=\left\lfloor\frac{k-2}{3}\right\rfloor+k$이므로

$$k \bmod 3=0\Rightarrow S_k=\left\lfloor\frac{3k+3-2}{3}\right\rfloor+3k+3=4k+3=1,$$

$$k \bmod 3=1\Rightarrow S_k=\left\lfloor\frac{3k+4-2}{3}\right\rfloor+3k+4=0,$$

$$k \bmod 3=2\Rightarrow S_k=\left\lfloor\frac{3k+5-2}{3}\right\rfloor+3k+5=0$$

이다. 그러므로 임의의 $k\ (0\le k\le n-1)$에 대하여 $S_k=\begin{cases}1, & 3\mid k\\ 0, & 3\nmid k\end{cases}$가 성립된다.(증명끝)

정리 3 $m=n-2$인 경우 임의의 $k\ (0\le k\le n-1)$에 대하여 다음의 식이 성립된다.

$$\mathrm{Tr}(\alpha_k)=\begin{cases}1, & k=0 \ \vee \ k \bmod 7=1,\ 2,\ 4\\ 0, & k\geq 1 \ \wedge \ k \bmod 7=0,\ 3,\ 5,\ 6\end{cases}$$

정리 4 $1<m<n-2$인 경우 임의의 $k\ (0\leq k\leq n-m)$에 대하여 $\mathrm{Tr}(\alpha^k)=1$이 성립된다.

증명 $1<m<n-2$인 경우 $a_1=a_2=\cdots=a_{n-m-1}=a_{n-m+1}=\cdots=a_n=1,\ a_{n-m}=0$이 성립되며 이때 $S_1=a_1=1$이고 $S_2=S_1a_1+2a_2=1$이 성립된다.

이제 임의의 $i\ (0\leq i<k,\ 1\leq k\leq n-m)$에 대하여 $S_i=1$이라고 가정하자.

뉴톤의 공식을 써서 계산하면 $k \bmod 2=0$일 때 $S_k=1$이 나온다.

$k \bmod 2=1$인 경우에도 역시 같은 방법으로 $S_k=1$을 얻을수 있다.

따라서 임의의 $k\ (0\leq k\leq n-m)$에 대하여 $\mathrm{Tr}(\alpha^k)=1$이 성립된다.(증명끝)

우의 정리들의 결과를 보면 $\mathbf{F}_2$에 기초한 극대무게를 가지는 다항식에 대응되는 다항식토대에서 흔적이 1인 원소가 그리 적지 않다. 이것은 극대무게를 가진 기약다항식이 유한체의 다른 산수연산들에는 적합하지만 흔적계산을 포함하는 체계들에서는 적합하지 않다는것을 보여준다.

그러나 다음의 정리는 F_n이 곱하기연산과 흔적계산에 둘 다 적합하다는것을 보여준다.

정리 5 F_n에 대응되는 다항식토대에서 흔적값이 1인 원소는 오직 1개뿐이다.

증명 이 경우 $a_0=a_2=\cdots=a_{n-1}=0,\ a_1=a_3=\cdots=a_{n-2}=0$이고 따라서 $\mathrm{Tr}(1)=n \bmod 2=1$이다. 또한 $S_1=a_1=0$이다.

임의의 $i\ (0\leq i<k,\ 1\leq k\leq n-1)$에 대하여 $S_i=0$이라고 가정하자.

이때 뉴톤의 공식으로부터 $S_k=k\cdot a_k$이므로 $k \bmod 2=0$이면 $S_k=0$이고 $k \bmod 2=1$인 경우에도 $S_k=0$이 나온다.

따라서 F_n에 대응되는 다항식토대에서 흔적값이 1인 원소는 오직 1개뿐이다.(증명끝)

참 고 문 헌

[1] O. Ahmadi et al.; Des. Codes Cryptogr., 37, 493, 2005.

[2] O. Ahmadi; Appl. Algebra Engrg. Comm. Comput., 18, 391, 2007.

[3] X. Zhang et al.; Finite Fields Appl., 35, 284, 2015.

주체106(2017)년 7월 5일 원고접수

The Trace Spectra of Some Polynomial Bases over a Binary Field

Kim Ryul

We analyze the trace spectra of polynomial bases over a binary field $\mathbf{F}_2$ derived by irreducible polynomials of maximum weight $F_{n,\ m}=x^n+x^{n-1}+\cdots+x^{m+1}+x^{m-1}+\cdots+1$ and irreducible polynomials $F_n=x^n+x^{n-2}+\cdots+x+1$ containing all of a constant term and odd degree term.

These polynomials all are of odd degree.

Key words: binary field, trace spectra