通信情報保護學會誌
第2卷 第4號, 1992. 12

유한체 상에서의 순환 다항식과 암호 체계

Permutation Polynomials over Finite Fields and Cryptosystems

고형준* · 윤석임** · 이준복* · 전유봉*

요 약

유한체 상에서의 순환 다항식은 여러 분야, 특히 조합론, 암호학등에 많이 이용되고 있다. 이 논문에서 이항 형태의 순환 다항식에 대해 알아보고 암호체계에서의 그 응용을 알아본다.

1. 서 론

GF(q)를 원소 q의 유한체라 하고, 여기서 q는 소수의 멱 이라 놓자. 주어진 유한체 GF(q) 상에서 순환을 하는 다항식을 순환 다항식(Permutation Polynomial, 이후 PP로 약함)이라 한다. 이를테면, 다항식 $f \in GF(q)[x]$가 GF(q)에서 GF(q)의 1-1 map을 이루면 f를 PP라 한다. PP들은 조합론, 암호학 등과 같은 많은 분야에 응용할 수 있다. 예를 들어, 암호 체계에서 송신자 A가 수신자 B에게 message M을 비밀리에 보내고자 한다. 그러면, 하나의 PP $f \in GF(q)[x]$를 encryption method로서 f^{-1}를 decryption method로 이용할 수 있다. A가 B에게 $f(M) = N$을 보내면 B는 N을 가지고 $f^{-1}(N) = f^{-1}(f(M)) = M$을 복구할 수 있다. 물론 제삼자는 M을 복구할 수 없도록 f는 특수한 성질을 가지고 있어야 한다. 예를들어 f(x)는 f(M)을 쉽게 계산할 수 있는 간단한 형태이고, A와 B만이 알고있는 비밀키가 없이는 $f^{-1}(x)$를 계산하기 어려운(intractable) 형태여서 제삼자는 $f^{-1}(N) = M$을 복구키 어려운 것이어야 한다. 동시에 B는 비밀키를 이용하여 $f^{-1}(x)$를 쉽게 구하여 $f^{-1}(N) = M$을 복구할 수 있다.

주어진 다항식 $f \in GF(q)[x]$가 PP인지 아닌지 f의 계수와 차수에 의해 결정할 수 있는 문제는 매우 어려운 일이다. 많은 학자들이 여러종류의 PP들의 class들을 찾고 PP들의 성질을 연구하여 왔다. 100여년전에 Dickson은 PP의 동치조건인 다음과 같은 Hermite's Criterion을 이용하여 차수가 5 보다 작거나 같은 모든 PP들과 $(6, q) = 1$인 경우의 차수가 6인 PP들을 분류하였다[4](p. 352).

Hermite's Criterion :

GF(q)가 characteristic p를 갖는다 하자. 그러면, $f \in GF(q)[x]$가 GF(q) 상에서 PP라는 사실과 다음 두 조건과는 동치 관계에 있다.

(1.1) f는 GF(q)에서 정확히 하나의 근을 갖는다.

(1.2) $1 \le t \le q-2$와 $t \not\equiv 0 \pmod p$를 만족하는 모든 정수 t에 대해 $f(x)^t \bmod (x^q - x)$의 reduction은

* 연세대학교 이과대학 수학과
** 덕성 여자대학교 자연과학대학 수학과

$q-2$ 보다 작거나 같은 차수를 갖는다.
또한, 여러종류의 잘 알려진 PP들, 예를들면, 다음과 같은 class들이 있다.

(1.3) 분명히 모든 일차 다항식은 PP가 된다.

(1.4) 단항식 x^n이 PP라는 것은 $(n, q-1)=1$과 동치이다.

(1.5) Dickson의 다항식 $D_n(x, a)=\sum_{j=0}^{\lfloor n/2 \rfloor} \frac{n}{n-j}\binom{n-j}{j}(-a)^j x^{n-2j}$이 PP라는 것은 $(n, q^2-1)=1$과 동치이다.(여기서, $\lfloor\ \rfloor$은 greatest integer function 이다)

(1.6) 선형화된 다항식 $L(x)=\sum_{i=0}^{n} a_i x^{p^i} \in GF(q)[x]$가 PP라는 것은 $L(x)$가 오직 0만을 근으로 갖고 있다는 사실과 동치이다.

PP의 개념을 다변수 다항식에서 확장시킬 수 있고 또한 유한체를 갈로아환으로 확장하여 연구할 수 있다.

우리는 여기서 주로 이항에 관한 PP, 즉 ax^i+bx^j+c와 같은 형태와 그 암호 체계에 대해서 알아보기로 하자.

2. 본 론

이항식 $f(x)=ax^i+bx^j+c$, 여기서 $a, b, c \in GF(q)$, $a\neq 0$, $i>j\geq 1$이라 하자. 모든 다항식은 상수항의 변화와 또는 0이 아닌 원소의 곱에 관계없이 PP의 성질을 유지할 수 있기 때문에 $f(x)$가 PP라는 사실은 $x^i-\alpha x^j$이 PP라는 사실과 동치이며, 여기서 $\alpha=-a^{-1}b$이다.

정리 1. $x^i \in GF(q)[x]$가 PP라는 사실은 $(i, q-1)=1$와 동치이다.

정리 2. $f(x)=x^i-\alpha x^j$, $i>j\geq 1$, $0\neq\alpha\in GF(q)$, $e=(i, j)$, $i'=i/e$, $j'=j/e$라 하자. 그러면, $f(x)$가 PP라는 사실은 $x^{i'}-\alpha x^{j'}$이 PP이고 $(e, q-1)=1$이라는 사실과 동치이다.

증명. $f(x)=(x^e)^{i'}-\alpha(x^e)^{j'}$이 PP라는 사실은 x^e와 $x^{i'}-\alpha x^{j'}$ 둘다 PP라는 사실과 동치이다. 왜냐하면 $f(x)$는 x^e와 $x^{i'}-\alpha x^{j'}$의 합성함수이기 때문이다. 그리고, 정리 1을 이용하여 정리 2의 결과를 얻는다. □

위의 정리 2에 의하여 이항식인 PP는 $f(x)=x^i-\alpha x^j$, $i>j\geq 1$, $0\neq a\in GF(q)$, $(i, j)=1$인 형태만을 연구하기에 충분함을 알 수 있다. 그리고, 잘 알려진 사실로서 모든 $GF(q)$에서 $GF(q)$의 mapping은 차수가 q 보다 작은 유일한 다항식으로 주어질 수 있기 때문에 $i<q$라고 가정하고, 또한 $q\equiv 1 \pmod i$인 경우를 제외시킬 수 있다. 왜냐하면, Hermite's Criterion의 (1.2)를 이용하면 다음의 정리를 얻는다.

정리 3. 만일 $q\equiv 1 \pmod i$, $i>q$이면 차수 i인 다항식 $f\in GF(q)[x]$는 PP가 될 수 없다.

$f(x)=x^i-\alpha x^j=x^j g(x)$, $0\neq\alpha\in GF(q)$이면 $g(x)=x^{i-j}-\alpha$이고 다음 세 조건을 생각하자.

(2.1) $g(x)\in GF(q)[x]$는 PP이다.

(2.2) $(i-j, q-1)=1$.

(2.3) α는 $GF(q)$의 한 원소의 $(i-j)^{th}$ power 이다.

정리 4. 위의 세조건중 하나를 만족하면 $f(x)=x^i-\alpha x^j$는 PP가 아니다.

증명. (2.3)에 의해서 $\alpha=\beta^{i-j}$인 $\beta\in GF(q)$가 존재한다. $\beta\neq 0$이고 $f(0)=f(\beta)=0$이므로 $f(x)$는 PP가 아니다. □

그러나 위의 세 조건은 PP가 되지 않는 필요조건이며 충분조건은 아니다.
예를들어, $f(x)=x^4-3x\in GF(13)[x]$을 생각하자. 분명히 $(4-1, 13-1)=3$, (2.2)를 위배한다. 그러나 $f(5)=f(-3)=-1$이므로 $f(x)$는 PP가 아니다. 또한, $f(x)=x^i-\alpha x^j=x^j g(x)$, $i>j\geq 1$, $0\neq\alpha\in GF(q)$, 그리고 $d=(i-j, q-1)$인 경우에 다음과 같은 $f(x)$가 PP가 되지 않는 특수한 필요조건들을 얻는다.

1) $i=j+1$. (왜냐하면 $g(x)$는 PP가 아니다)
2) $\alpha=1$. (왜냐하면 $f(0)=f(1)=0$)
3) $\alpha=-1$, $i-j$는 홀수. (왜냐하면 $f(0)=f(-1)=0$)
4) $\alpha=-1$, $(q-1)/d$는 홀수
(왜냐하면 $\beta^{i-j}=-1$, $\beta\in GF(q)$와 $(-1)^{(q-1)/d}$

$=1$은 동치이다.)

5) $d=1$ 즉, $(i-j, q-1)=1$.

6) $i-j$는 GF(q)의 characteristic의 멱.

(왜냐하면 $i-j=p^n$, $q=p^m$, $m>n$이라 하자. 그러면 $g(x)=(x-\alpha^{p^{m-n}})^{p^n}$)

정리 5. $f(x)=x^{p^s}-\alpha x^{p^r}$, $s>r\geq 0$, $0\neq\alpha\in GF(q)$, $q=p^n$. 그러면,

a) $f(x)$는 PP라는 사실은 α가 GF(q)의 한 원소의 $(p^s-p^r)^{th}$ power가 아니라는 것과 동치이다.

b) $p=2$와 $(s-r, n)=1$이 아닌 경우에 α가 GF(q)의 원시근(primitive root)이면 $f(x)$는 PP이다.

증명. a) 분명히, α가 GF(q)의 한 원소의 $(p^s-p^r)^{th}$ power이면 $f(x)$는 PP가 아니다. 반면에 $f(x)$가 PP가 아니면 $f(\beta)=f(\gamma)$인 $\beta\neq\gamma$가 GF(q)에 존재한다. 즉, $\beta^{p^s}-\alpha\beta^{p^r}=\gamma^{p^s}-\alpha\gamma^{p^r}$. 그러면, $(\beta-\gamma)^{p^s}=\alpha(\beta-\gamma)^{p^r}$ 즉, $\alpha=(\beta-\gamma)^{p^s-p^r}$

b) 만일 $(p^s-p^r, p^n-1)=1$이 아니면 α는 $(p^s-p^r)^{th}$ power가 아니다. $(p^s-p^r, p^n-1)=(p^r(p^{s-r}-1), p^n-1)=p^{(s-r,n)}-1$ 그러므로 $(p^s-p^r, p^n-1)=1$과 $p=2$, $(s-r, n)=1$은 동치이다. 그리고 a)를 이용하여 그 결과를 얻는다. □

$f(x)=x^i-\alpha x^j$가 PP인지 아닌지 완전히 결정할 수는 없다. 그러나, 주어진 $f(x)=x^i-\alpha x^j$가 GF(q)에서 PP이면 q는 충분히 클 수 없음을 다음 정리(보조정리 7,[6])로 알 수 있다.

정리 6. $f(x)=x^i-\alpha x^j$, $0\neq\alpha\in GF(q)$, $1<j<i$, $(i, j)=1$이라 하자. 그러면, 상수 $C=C(i)$가 존재하여 $q>C$이면 f는 PP가 아니다.

또한, Turnward[8]는 좀더 구체적인 다음 정리를 증명하였다.

정리 7. $f(x)=x^i-\alpha x^j$, $0\neq\alpha\in GF(q)$, $1\leq j<i$, $(i, j)=1$이라 하자. 그러면, $f(x)$가 PP이면 $q\leq(i-2)^4+4i-4$, 또는 $i=jp^r$ $(r\geq 1)$.

특히 $f(x)=ax^{(q+1)/2}+bx$, $a, b\in GF(q)$, q는 홀수,와 같은 형태는 많은 PP들을 포함하고 있음을 다음 정리(정리 5,[6])는 보여준다.

정리 8. q는 홀수, $f(x)=x^{(q+1)/2}+bx\in GF(q)[x]$라 하자. 그러면, $f(x)$가 PP라는 사실과 b^2-1은 GF(q)에서 0이 아닌 제곱수인 것과는 동치이다.

암호학에서 잘 알려진 다항식은 $y\equiv x^e \pmod{q-1}$으로 주어진 다항식 x^e이다. 단항식 x^e은 RSA 체계의 기본을 이루고 있다. 주어진 message x, $1<x<q$에 대해서 encryption method와 decryption method는 $y\equiv x^e \pmod{q-1}$와 $x\equiv y^d \pmod{q-1}$으로 주어진다. 여기서, $(e, q-1)=1$, $ed\equiv 1 \pmod{q-1}$. $f(x)=ax^{(q+1)/2}+bx\in GF(q)[x]$, q는 홀수,는 합성의 연산에 의해 닫혀있다. $f_i(x)=a_ix^{(q+1)/2}+b_ix$, $i=1, 2$. $(f_1\circ f_2)(x)=f_1(f_2(x))\equiv(a_1c+b_1a_2)x^{(q+1)/2}+(a_1d+b_1b_2)x \pmod{(x^q-x)}$ 여기서 $c+d=(a_2+b_2)^{(q+1)/2}$, $c-d=(b_2-a_2)^{(q+1)/2}$. 그래서 주어진 $f(x)$의 역 $g(x)$를 $f(x)\circ g(x)=x$, $g(x)\circ f(x)=x$로 부터 구할 수 있다. 정리 8에 의해서 $f(x)=x^{(q+1)/2}+bx\in GF(q)[x]$가 PP라는 사실과 b^2-1은 GF(q)에서 0이 아닌 제곱수인 것과는 동치이다. 그리고, 제곱수 $s\in GF(q)$에 대해 $f(s)=(a+b)s$이고 비 제곱수 $t\in GF(q)$에 대해 $f(t)=(b-a)t$이므로 위의 이항식 $f(x)$에 의해 결정되는 GF(q)에서 GF(q)의 mapping은 간단하다. 그래서 RSA type 암호 체계에서 단항식 x^e 대신에 이항식 (mod n)을 연구하여 이용하는 것도 흥미로울 것이다.

끝으로 (1. 4)에서 정의된 Dickson의 다항식도 암호 체계에 응용할 수 있다. Dickson의 다항식이 합성의 연산에 의해 닫혀져 있는 경우는 오직 $a=0, \pm 1$인 경우임은 잘 알려져 있다(정리 7.22,[4]). $a\neq 0$인 경우에 $D_e(x, \pm 1)$, $(e, q^2-1)=1$을 encryption method로서 $D_e^{-1}(x, \pm 1)=D_d(x, \pm 1)$, $de\equiv 1 \bmod(q^2-1)$을 decryption method로서 이용할 수 있다.

이항식과 Dickson의 다항식에서와 같이 합성의 연산에 대한 닫힘성은 공개키 체계에서 비밀을 유지하는데 매우 중요하다. 왜냐하면 주어진 하나의 다항식의 역을 구하는 것보다 여러 다항식들의 합성한 다항식의 역을 구하는데는 특별한 지식이 없이는 매우 어렵기 때문이다.

참 고 문 헌

1. R. Lidl : On cryptosystems based on polynomials and finite fields, Advances in Cryptology-EUROCRYPT 84, Lecture Notes in Computer Science, V.209, Springer-Verlag, Berlin, (1985), pp.10-15.

2. R. Lidl, G.L. Mullen : When does a polynomial over a finite field permute the elements of the field ?, Amer.Math.Mon., 95(1988), pp. 243-246.

3. R. Lidl, W.B. Müller : Permutation polynomials in RSA-cryptosystems, Advances in Cryptology-CRYPTO '83(D. Chaum, ed.) Plenum Press, New York(1984), pp.293-301.

4. R. Lidl, H. Niederreiter : Finite Fields, Encyclo. Math. and Appls. V.20, Addison-Wesley, Reading, MA(1983).

5. R.A. Mollin, C. Small : On permutation polynomials over finite fields, Internat. J. Math. & Math. Sci., 10(1987), pp.535-544.

6. H. Niederreiter, K.H. Robinson : Complete mappings of finite fields, J. Austral. Math. Soc. (Ser. A), 33(1982), pp.197-212.

7. C. Small : Permutation binomials. Internat. J. Math. & Math. Sci., 13(1990), pp.337-342.

8. G. Turnward : Permutation polynomials of binomial type, Contributions to General Algebra 6, Velag Hölder-pichler-Tempsky, Wien(1988), pp.281-286.

9. V. Varadharajan : Cryptosystems based on permutation polynomials, Internat. J. Computer Math. 23(1988), pp.187-209.

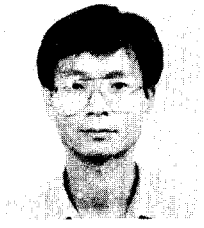
□ 著者紹介

고 형 준(정회원)

제주대학교 수학교육과(학사)
연세대학교 수학과(석사)
미국 Brandeis 대학교(Ph.D)
미국 Purdue 대학교 조교수
현재 : 연세대학교 이과대학 수학과 부교수

윤 석 임

성균관대학교 수학과(학사)
연세대학교 수학과(석사)
불란서 Montpellier II 대학교(박사)
현재 : 덕성여자대학교 자연대학 수학과 부교수



이 준 복

연세대학교 이과대학 수학과(학사)
연세대학교 수학과(석사)
미국 아리조나 대학교(Ph.D)
미국 아리조나 대학교 Post Doc.

전 유 봉

연세대학교 이과대학 수학과(학사)
연세대학교 수학과(석사)
연세대학교 수학과(박사)
현재 : 연세대학교 이과대학 수학과 교수