GF(p)의 유한 확장체의 구축을 위한 GF(p) 위에서의 기약 다항식

최 윤 서
고려대학교 대학원

Finding Irreducible Polynomial Over GF(p) For Constructing The Finite Extension Field of GF(p)

Choi, Youn-Seo
Graduate School of Korea University

1, 개요.

p를 솟수라고 가정하고, F를 유한체(finite field) GF(p)로 n을 양의 정수라 하자. 우리가 만약 n차의 기약 다항식을 알고 있다면 F[X]/fF[X]가 유한체이므로 p^n개의 원소를 가진 유한체에 대한 구체적인 정보를 알수 있을 것이다. 반대로 원소의 갯수가 p^n개인 유한체에 대한 구체적인 정보를 알고 있다면 F 위에서 차수가 n인 원소를 주어진 유한체에서 찾을 수 있고 또한 그 원소의 F 위에서의 n 차의 기약 다항식 f를 계산해 낼수 있을 것이다. 따라서 p^n개의 원소를 가진 유한체를 찾는 것과 F[X] 안에서 n 차의 기약 다항식을 구해내는 것과는 동치 관계에 있다. 그리고 그런 기약 다항식은 다양한 방면(coding theory, cryptography, multivariate polynomial factoring, parallel polynomial arithmetic 등)에 사용 되어진다.

따라서 앞으로의 본문 내용은 기약 다항식을 구하는데 필요한 아래의 두 정리를 증명하는 과정으로 되어있다.

(정리 1) n을 나누고 p와는 다른 모든 솟수 q에 대하여, F 위에서의 X^q-1의 분해체(splitting field)와 K 안에서의 q차 비 잉여(nonresidue)가 주어지면 F 위에서의 n차 기약 다항식을 찾을 수 있다.

(정리 2) F 위에서의 n차 기약 다항식을 찾는 것을 F 위에서 다항식의 인수 분해 문제로 제한해서 생각 할수 있다.

추가로, 두 정리를 이용해 program을 짰으나 program의 크기 관계로 본 내용에서는 뺐으나 그 대신 program을 통해 구해낸 간단한 예를 대신 첨가했다. 그리고 그 program은 Fortran어의 link와 commpile 과정의 제약에의해 현재는 70차 이내의 기약 다항식 구할때에 한해서만 작동한다. 현재 그 program상의 문제점을 보완하기위해 수정, 보완중이다.

2, 정리 1의 증명.

(정리 1) n을 나누고 p와는 다른 모든 솟수 q에 대하여, F 위에서의 X^q-1의 분해체(splitting field)와 K 안에서의 q차 비 잉여(nonresidue)가 주어지면 F 위에서의 n차

기약 다항식을 찾을 수 있다.

X^q-1의 분해체는 1의 q차 원시 근(a primitive qth root of unity)을 포함하는 가장 작은 F의 확대체(extension field)이며, m이 q를 법으로 한 위수(order)일때 앞의 분해체는 바로 $GF(p^m)$이 된다. 그리고 우리는 mod GCD algorithm에의해 X^q-1에서 F 위에서의 m차 기약 다항식 f를 얻을 수 있다. 따라서 정리 1의 가정은 F 위에서의 m차 기약 다항식 f와 α가 f의 근일때 $F(\alpha)$안에서 q차 비 잉여 a가 주어진 것을 의미한다.

지금부터 정리 1의 증명을 시작한다. n의 소인수 분해를 $q_1^{e1}\cdots q_r^{er}$이라고 하자. 먼저 모든 $i(=1,\cdots,r)$에대해 F 위에서의 q_i^{ei}차 기약 다항식을 구하고 그 다음에 이 다항식들을 n차의 다항식으로 조합한다.

1 단계 : 솟수 멱차의 기약 다항식을 구한다.

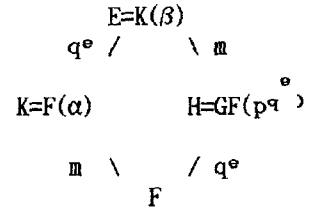
$1\le i\le r$, $q=q_i$,그리고 $e=e_i$라 하자. F[X]안에서 q^e차 기약 다항식을 구하기 위해서 다음의 3가지 경우로 q를 구분하다. (1) q가 2도 p도 아닌 경우, (2) q가 2이고 p가 아닌 경우, 그리고 (3) q가 p인 경우.

(1) q가 2도 p도 아닌 경우.

m을 q를 법으로 했을때의 p의 위수(order)라고 하자. 그리고 가정에 의해서 F 위에서의 m차 기약 다항식 f와 $F(\alpha)$에서의 q차 비 잉여 a가 주어진다.

보조 정리 1 : K를 체(field)라하고 d를 2보다 큰 정수라하며, a가 K에 들어가는 0이 아닌 원소라고 하자. 그때 d를 나누는 모든 솟수 t에 대하여 a가 K^t 안에 있지 않을때, 단 d가 4에 의해 나누어질때는 a가 $-4K^4$에 있지 않으면 X^d-a는 K[X] 안에서 기약 다항식이된다.

보조정리 1에 의해 $X^{q^e}-a$는 K[X]에서 기약 다항식이 된다. 그러면 $E=GF(p^{mq^e})$를 $X^{q^e}-a$의 근 β에 의해서 $K(\beta)$로 표현할수있다. 그리고 $H=GF(p^{q^e})$가 E의 부분체(subfield)가 되기 때문에 다음의 관계가 성립된다.



지금부터는 E 안에 있는 F 위에서 q^e차의 원소 ν를 찾는다. 만약 그런 원소를 찾게 되면 우리는 그 원소의 최소 다항식(minimum polynomial)을 구할수 있기 때문이다. 즉

$$Irr(\nu,F)=(X-\nu)(X-\nu^P)\cdots(X-\nu^{P^{q^e-1}}).$$

다행이도 E 안에 있으면서 F 위에서 q^e차인 원소를 찾는것은 쉽다.

T를 E에서 H로 가는 자취(trace)라고 하면· $\nu=T(\beta)$는 F위에서 q^e차의 원소가 된다.

(2) q가 2이고 p가 아닌 경우.

이 경우에서는 2^e차의 기약 다항식을 찾아야한다. 이번에도 경우(1)에서와 같이 보조 정리 1을 사용한다. p가 홀수이기 때문에 p는 4를 법으로해서 +1 또는 -1이 된다. 먼저 p가 4를 법으로해서 1이라고 하자. 그러면 $(-1)^{(p-1)/2}$는 1이되고 -1는 F 안에서 제곱 근을 가진다. 따라서 F 안에서 제곱 근을 갖지 않는 a라는 원소가 존재한다면 a는 F 안에 있는 어떤 원소 b에 의해 $a=-4b^4$의 형태로 나타내지지 않는다. 따라서 보조 정리 1에 의하여 $X^{2^e}-a$는 기약 다항식이다.

이번에는 p가 4를 법으로하여 -1이라고 가정하자. 이 경우 2^e차 기약 다항식은 쉽게 찾아진다. 만약에 e가 1이면 $(-1)^{(p-1)/2}=-1$이기 때문에 -1은 F에서 제곱 근을 갖지 않고 그에 따라서 X^2+1은 기약이다. 또 만약에 e가 1이 아니면 다음과 같다. 자 F(i)를 생각해 보자. 여기서 i는 $i^2=1$인 원소이다. -1은 F(i)에서 제곱 근을 갖기 때문에 제곱 근을 갖지 않는 F(i)의 한 원소 a를 찾으면 $X^{2^{e-1}}-a$는 F(i)[X]에서 기약 다항식이다. $X^{2^{e-1}}-a$의 근을 α라 했을때 $F(i,\alpha)$를 E라하자. 그러면 유한체의 정리에의해 F의 대수적 닫힘(algebraic closure)에서 E는 $F(\alpha)$가 된다. 그러므로 i를 -i로 보내는 F(i)에서의 자기 동형(automorphism) h에 의해서 2^e차 기약 다항식은 $(X^{2^{e-1}}-a)(X^{2^{e-1}}-a^h)$

가 된다. 그래서 지금부터는 위 문제를 F(i)에서 2차 비 잉여류(a quadratic nonresid ue)를 찾는것으로 한정한다. F(i)*는 원소의 갯수가 p^2-1인 순환 군(cyclic group)이며 p^2-1는 홀수 l과 양의 정수 k에의해 12^k로 나타낼수 있다. 만약에 k-2개의 연속적인 i의 제곱 근을 구할수 있으면 F(i)에서 1의 2^k번째 원시 근(a primitive 2^kth root of unity)을 취할수 있으며 그것이 2차 비 잉여류일것이다. 그렇지 않다면 그것의 제곱 근은 F(i)*에서 2^{k-1}의 차수를 가져야하는데 Lagrange's theorem에의해 불가능한 것이다. 따라서 F(i)에서 제곱근을 아래의 방식에 의해서 구하기만 하면 된다.

1) $\alpha^{(p-1)/2}=1$이면 α의 제곱 근은 $(1+\alpha^{(p-1)/2})^{(p-1)/2}\ \alpha^{(p+1)/4}$.

2) $\alpha^{(p-1)/2}=-1$이면 $i\alpha^{(p+1)/4}$.

(3) q가 p인 경우

지금부터 귀납적인 방법으로 p^e차의 기약 다항식을 찾을 것이다.

먼저 보조 정리 2를 살펴 보자.

보조 정리 2 : 다항식 X^p-X-1은 F[X]에서 기약이다. 더우기 K가 F의 확대체이고 다항식 X^p-X-a가 K[X]에서 기약이며 X^p-X-a의 근 α에 의해 E가 $K(\alpha)$로 표현 될때, 다항식 X^p-X-ab^{p-1}는 E[X]에서 기약이다.

$f_1=X^p-X-1$라 하고 1보다 큰 정수 t에 대해 f_t가 계산되어졌다고 가정하자. 그 다음으로 f_t의 근이 α일때 $K=F(\alpha)$라 하자. 이때에 t=1이면 a를 α^{p-1}라 하고, t가 1이 아니면 $a=(\alpha^p-\alpha)\alpha^{p-1}$라 놓자. 그러면 X^p-X-a는 K위에서 기약이 된다. 그리고, X^p-X-a의 근을 β이라고 한 후 $E=K(\beta)$이라고 하면 유한체 정리에 의해 $E=F(\beta)$이 된다. 따라서 F 위에서 β의 최소 다항식(minimum polynomial)은 $f_{t+1}=\prod_{i=0}^{p^i-1}(X^p-X-a^{p^i})$가 된다. 그리고 다항식 $X^p-X-a\beta^{p-1}=X^p-X-(\beta^{2p-1}-\beta^p)$는 E 위에서 기약이다. 이상의 방법으로 p^e차의 기약 다항식을 계산해낼수 있다.

2 단계 : 솟수 멱차의 기약 다항식들의 합성.

먼저 F 위에서의 $q_1^{e1},\cdots,q_r^{er}$차 기약 다항식들을 구했다고 가정하자. 지금부터는

귀납적인 방법에의해 F 위에서 차수가 $q_1^{e1}, q_1^{e1}q_2^{e2}, \cdots, q_1^{e1}\cdots q_r^{er}=n$가 되는 기약 다항식들을 차례로 구할 것이다. 그러나, 그것은 F[X]에 있는 서로 소인 a,b를 차수로 가진 두 기약 다항식 f,g로부터 차수가 ab인 기약 다항식을 찾는 것만으로도 충분하다. 여기서 보조 정리 3을 보자.

보조 정리 3 : α과 β이 F의 대수적 닫힘에 있고 $[F(\alpha):F]=a$, $[F(\beta):F]=b$, 그리고 $\gcd(a,b)=1$이라고 가정하면 $[F(\alpha,\beta):F]=[F(\alpha+\beta):F]=ab$이다.

만약에 f와 g가 위에서 설명되어진것과 같이 주어지고 α이 f의 근이고 β이 g의 근으로 주어졌을때, 보조 정리 3에 의해서 F가 $F(\alpha)$에 속하고 $F(\alpha)$이 $F(\alpha,\beta)$에 속함을 알 수 있고, 또한 $[F(\alpha):F]=a$인 것과 $[F(\alpha,\beta):F(\alpha)]=b$임을 알수 있다. 결과적으로 F 위에서 $\alpha+\beta$의 최소 다항식은 $(X-(\alpha+\beta))(X-(\alpha+\beta)^p)\cdots(X-(\alpha+\beta)^{p^{ab-1}})$이다. 이 다항식이 F 위에서 차수가 ab인 기약 다항식임은 물론이다.

3, 정리 2의 증명.

(정리 2) F 위에서의 n차 기약 다항식을 찾는 것을 F 위에서 다항식의 인수 분해 문제로 제한해서 생각 할수 있다.

정의 : 체 K가 지표(characteristic)로 p를 갖고 n은 p에 의해서 나눠지지 않는 양의 정수이며 s는 K위에서 1의 n번째 원시 근일때 다항식 $Qn(X)=\prod_{s=1,\gcd(s,n)=1}^{n}(X-\zeta^s)$을 n번째 원분 다항식(cyclotomic polynomial)이라고 한다.

q는 n을 나누고 p와는 다른 솟수라고 하고, m을 q를 법으로 하는 p의 위수(order)라고 하자. 그러면 정리 1에의해 m차의 기약 다항식 f와 f의 근이 α일때 $F(\alpha)$에서 q차의 비 잉여류(qth nonresidue)만 찾으면 충분하다.

기본적인 착상은 m차의 기약 다항식을 포함하고 있는 원분 다항식 $Qq(X)=X^{q-1}+\cdots+1$을 인수 분해하는 것이다. 이 착상은 $GF(p^m)$과 $GF(p^m)$에서 q번째 원시 근 ζ을 얻개해

준다. $GF(p^m)^*$는 원소의 갯수가 p^m-1개인 순환 군이며 원소의 갯수 p^m-1은 q와 서로 소인 l에 의해 lq^k로 나타낼수있다. 만약, k-1번 연속적으로 s의 q차 근(qth root)을 구할수 있다면, $GF(p^m)$안에서 1(unity)의 q^k번째 원시 근을 구할수 있으며 그것은 q차의 비 잉여류일 것이다. 따라서 $GF(p^m)$ 위에서 X^q-c 형태의 다항식의 근을 찾는 것으로 문제를 축소해서 생각할수 있으며 그것에 Berlekamp가 제시한 방법(참고 문헌 [3])을 적용하겠다.

앞으로 귀납적인 방법에 의해 1의 q^i번째 원시 근들을 근들로 갖는 F[X]에서의 m차 다항식 $f^{(i)}$을 $f^{(1)}$에서 $f^{(k)}$까지 정의 할 것이다. 먼저 $f^{(1)}$는 $\Phi_q(x)$의 어느 한 기약 인수로 정의한다. 물론 $f^{(1)}$의 근들은 1의 q번째 원시 근들이다. 그리고 i=2,···,k인 경우에 대해서는 $f^{(i)}$를 $f^{(i-1)}(X^q)$의 임의의 한 기약 인수로 정의 한다. $f^{(i-1)}$의 근들이 1의 q^{i-1}번째 원시 근들이기 때문에 $f^{(i)}$의 근들은 1(unity)의 q^i번째 원시 근임에 틀림없다. 이와 같이 $f^{(1)},\cdots,f^{(k)}$를 계산해내기 위해서는 q-1차의 다항식과 m^q차의 다항식들을 인수 분해해야 하지만 mod GCD algorithm을 사용한다면 쉽게 해결수 있다. 그리고 m이 q^i(i는 1과 k사이)를 법으로 한 p의 위수이기 때문에 모든 $f^{(1)},\cdots,f^{(k)}$는 m차의 서로 다른 기약 다항식들의 적(product)이다. 또한 f를 $f^{(k)}$라 하면 f의 모든 근 α은 $F(\alpha)$ 안에 있는 q번째 비 잉여류가된다. 이로써 정리 2의 증명을 마친다.

4, 간단한 예제.

이미 개요에서 언급했던 Fortran어를 이용해 짠 program을 수행시켜서 얻은 간단한 예제를 소개하겠다. Fortran어에서 충분한 space가 제공된다면 보다 높은 차수에서도 수행이 되리라 여겨진다.

program상에서는 주어진 다항식의 근을 companion matrix로 표현하여 모든 근들 사이의 연산을 matrix 연산으로 대체했다.

(예제)

p가 3이고 n이 30인 경우. 즉, GF(3) 위에서 차수가 30인 기약 다항식을 찾는 문제.

(1) p=3,n=30=2x3x5

(2) GF(3) 위에서 차수가 2인 기약 다항식 $f_1 = X^2+1$

(3) GF(3) 위에서 차수가 3인 기약 다항식 $f_2 = X^3+2X+2$

(4) GF(3) 위에서 차수가 5인 기약 다항식 $f_3 = X^5+2X^3+2X^2+X+1$

(5) GF(3) 위에서 차수가 6인 기약 다항식 $f_{12} = X^6+X^4+X^3+X^2+2X+2$

(6) GF(3) 위에서 차수가 30인 기약 다항식

$f_{123} = X^{30}+2X^{28}+2X^{27}+X^{21}+2X^{19}+X^{13}+X^{12}+2X^{11}+2X^{10}+X^5+X^4+X^3+2X^2+2X+2$

5, 참고 문헌.

[1] Rudolf Lidl and Harald Niederreiter : Introduction to finite fields and their applications. Cambridge University Press. (1986)

[2] Serge Lang : Algebra. 2nd ed., Addison-Wesley. (1984)

[3] E. Berlekamp : Facroting polynomials over large finite fields. Math. Comp 24. PP 713-735. (1970)

[4] E. Berlekamp : Algebraic coding theory. McGraw-Hill. (1968)

[5] B. van der Waerden : Algebra. Vol 1, 7th ed., Ungar. (1970)

[6] J. H. Loxton : Number theory and Cryptography. Cambridge University Press PP 76-85. (1990)

[7] Leonard M. Adleman and Andrew M. Odlyzko : Irreducibility testing and factorization of polynomials. Vol 41, Number 164. PP 699-709. (1983)