유한체에서의 원시 정규기저 알고리즘의 구현과 응용에 관한 연구

(AN ALGORITHM FOR PRIMITIVE NORMAL BASIS IN FINITE FIELDS)

임 종인 (고려대학교 자연과학대학 수학과 부교수)
김 용태 (광주교육대학 수학교육과 전임강사)
김 윤경 (동신대학교 수학과 조교수)
서 광석 (서남대학교 수학과 조교수)

A B S T R A C T

GF(2^m) 이론은 switching 이론과 컴퓨터 연산, 오류 정정 부호(error correcting codes), 암호학(cryptography) 등에 대한 폭넓은 응용때문에 주목을 받아 왔다. 특히 유한체에서의 이산 대수(discrete logarithm)는 one-way 함수의 대표적인 예로서 Massey-Omura Scheme을 비롯한 여러 암호에서 사용하고 있다. 이러한 암호 system에서는 암호화 시간을 동일하게 두면 고석 연산은 유한체의 크기를 크게 할 수 있어 비도(crypto-degree)를 향상 시킨다. 따라서 고속 연산의 필요성이 요구된다.

1981년 Massey와 Omura가 정규기저(normal basis)를 이용한 고속 연산 방법을 제시한 이래 Wang, Troung 등 여러 사람이 이 방법의 구현(implementation) 및 곱셈기(Multiplier)의 설계에 힘써왔다.

1988년 Itoh와 Tsujii는 국제 정보 학회에서 유한체의 역원을 구하는 획기적인 방법을 제시했다. 1987년에 H. W. Lenstra와 Schoof는 유한체의 임의의 확대체는 원시정규기저(primitive normal basis)를 갖는다는 것을 증명하였다.

1991년 Stepanov와 Shparlinskiy는 유한체에서의 원시원소(primitive element), 정규기저를 찾는 고속 연산 알고리즘을 개발하였다.

이 논문에서는 원시 정규기저를 찾는 Algorithm을 구현(Implementation)하고 이것이 응용되는 문제들에 관해서 연구했다.

1. 정규기저의 생성

이 절에서는 m,n 이 정수이고 $q = p^m$ 인 경우 $(n, q) = 1$ 일 때 유한체 F_q 위에서 F_{q^n} 의 임의의 기저 $w_1, w_2, \ldots, w_n$ 으로 $(n \log q)^{O(1)}$ 시간 내에 정규 기저 $\alpha_1=\alpha$, $\alpha_2=\alpha^q$, $\cdots$, $\alpha_n=\alpha^{q^{n-1}}$을 생성시키는 과정을 연구했다.

$w_i^q = a_{i,1}w_1 + \ldots + a_{i,n}w_n \quad 1 \le i \le n \quad a_{i,j} \in F_q \quad (1\text{-}1)$

의 계수 행렬을 $A = (a_{i,1})$ 이라 했을 때,

$(w_1^q, \ldots, w_n^q)^t = A(w_1, \ldots, w_n)^t$ 이다.

(1-1)의 양변에 q^{j-1}를 승하면 $a_{i,j}{}^q = a_{i,j}$ 이므로

$$w_i{}^q = a_{i,1}w_1{}^{q^{j-1}} + \ldots + a_{i,n}w_n{}^{q^{j-1}} \quad , \quad 1 \le i \le n$$

$$(w_1{}^{q^j}, \ldots, w_n{}^{q^j})^t = A^j(w_1, \ldots, w_n)^t \qquad (1\text{-}2)$$

모든 $w \in F_{q^n}$ 에 대하여 $w^{q^n} = w$ 이고 $w_1, \ldots, w_n$ 이 F_{q^n} 의 기저이므로 $A^n = I$ 를 얻는다. 따라서 $f(\lambda) = \lambda^n - 1$ 이 A 의 최소 다항식이다.
$(n,q)=1$ 이므로 $f(\lambda)$ 는 중근을 갖지 않는다.

$$f(\lambda) = \prod_{i=1}^{m} f_i(\lambda) \qquad (1\text{-}3)$$

을 F_q위에서 기약 다항식만의 인수분해이고 각각의 차수를 $d_1, \ldots, d_m$ 이라 하자.
$\lambda_{i,1}, \ldots, \lambda_{i,d_i}$ 를 $f(\lambda)$ 의 근으로서 행렬 A의 고유치라 할 때
$\lambda_{i,1}$ 에 대응하는 고유 벡터 $z_{i,1}$ 을 구하기 위해

$$(A - \lambda_{i,1} I)z_{i,1}{}^t = 0 \qquad (1\text{-}4)$$

의 0 이 아닌 해를 유한체 $F_{q^{d_1}}$ 위에서 구한다.
일반적으로 기약 다항식의 근은 한 근의 q승으로 표시되므로

$z_{i,1} = (z_{i,1}(1), \ldots, z_{i,n}(n))$ 이라 할때

$$z_{i,r} = (z_{i,1}(1)^{q^{r-1}}, \ldots, z_{i,1}(n)^{q^{r-1}}) \quad , \quad 1 \le r \le d_i \qquad (1\text{-}5)$$

가 f_i에 대한 고유벡터이다. 그러면

$$z_i = z_{i,1} + \ldots + z_{i,d_i} \quad , \quad 1 \le r \le m \qquad (1\text{-}6)$$

의 각 성분은 F_q 의 원소이고

$$x = (x_1, \ldots, x_n) = z_1 + \ldots + z_m \qquad (1\text{-}7)$$

의 각 성분도 F_q 의 원소이다.

$$\alpha = x_1w_1 + \ldots + x_nw_n \qquad (1\text{-}8)$$

이라 놓으면 다음 보조정리를 얻는다.
정리 1.1 (1-1), (1-3)-(1-8)에서 정의된 α 가 F_q위에서 F_{q^n}의 정규기저를 생성하고 n 과 q 의 polynomial time내에서 계산된다.

(증명) (1-2)와 (1-8)에서 다음을 얻는다.

$$\alpha^{q^j} = xA^j(w_1, \ldots, w_n)^t \quad , \quad 0 \le j \le n-1.$$

$\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}$이 F_{q^n} 의 정규기저가 됨을 증명하기 위해서는 $w_1, \ldots, w_n$ 이 기저이므로 $x, xA, \ldots, xA^{n-1}$ 이 F_q 위에서 일차 독립임을 보이면 된다.
(1-7) 에서 쌍마다 다른 고유치 $\mu_1, \ldots, \mu_n$ 에 대응하는 A 의 고유벡터가 $y_1, \ldots, y_n$ 일때 $x = y_1 + \ldots + y_n$ 이고
$xA^j = \mu_1{}^j y_1 + \ldots + \mu_n{}^j y_n$, $0 \le j \le n-1$, 그러면 $\mu_i \ne \mu_j$ $(i \ne j)$ 이므로 $\mu_1, \ldots, \mu_n$ 의 Vandermonde 행렬식이 0 이 아님을 이용하면 $x, xA, \ldots, xA^{n-1}$ 은 F_q 의 정규기저를 생성한다.
(1-1)(1-3)-(1-8) 의 계산은 n 과 q의 polynomial time 내에서 실행된다. ([2],[3] 참조). Q.E.D.

2. 원시 정규기저의 생성

θ는 F_{q^n} 의 고정된 한 원시근이다. 위에서의 기저 $w_1,\ldots,w_n$ 에 관한 표현을 $\theta = u_1w_1+\ldots+u_nw_n$ 이라 하자.

θ^k 로 생성되는 원시정규기저를 찾고자 한다.

$\theta^k,\theta^{kq},\ldots,\theta^{kq^{n-1}}$ 이 원시정규기저이기 위한 필요 충분 조건은

$(k,q^{n-1})=1$ 이고 $\theta^k,\theta^{kq},\ldots,\theta^{kq^{n-1}}$ 이 일차독립인 것이다.

모든 계산은 $(n \log q)^{O(1)}$ 이다. 우선

$$w_i = w^{q^i} , \quad 0\le i\le n-1 , \quad (2\text{-}1)$$

을 F_q 위에서 F_{q^n} 의 원시정규기저라 하자.

$u_0(k),\ldots,u_{n-1}(k)$ 를 이 기저에 대한 θ^k 의 좌표라 하면

$$\theta^k = \sum_{i=0}^{n-1} u_i(k)w_i , \quad k = 1,2,\ldots \qquad (2\text{-}2)$$

(2-1) 과 (2-2) 에서

$$\theta^{kq^t} = \sum_{i=0}^{n-1} u_{i-t}(k)w_i , \quad 0\le t\le n-1$$

단 j 0 이면 $u_j = u_{j+n}(k)$

$A(k)$는 순환 행렬 $A(k) = (u_{i-t}(k))$ $0\le t\le n-1$ 이다.

그러면 $\theta^k,\theta^{kq},\ldots,\theta^{kq^{n-1}}$ 이 정규기저가 될 필요 충분 조건은

$$\det A(k) \neq 0 \qquad (2\text{-}3)$$

θ^k 가 원시근일 필요충분조건은

$$(k,q^n-1) = 1 \qquad (2\text{-}4)$$

$h(x) = x^n + a_{n-1}x^{n-1}+\ldots+a_0$ 를 F_q 위에서 θ 의 최소다항식이라 하자.

보조 정리 2.1 $i=0,1,\ldots,n-1$ 에 대해서 수열 $\{u_i(k)\}$ $k=1,2,\ldots$ 는 다음의 순환관계를 만족한다.

$$u_i(k+n) + a_{n-1}u_i(k+n-1) +\ldots+ a_0u_i(k) = 0 , \quad k= 1,2\ldots$$

(증명) 생략.

수열$\{\delta_l\}$ 을 순환관계로 정의 하자.

$\delta_2 = 1$: $\delta_l = \delta_{[(l+2)/2]} / [(l+2)/2]$, $l=3,4,\ldots$.

임의의 체 L에서 수열 $\{v(x)\}$ 를 다음과 같이 정의 하자.

$$v(x) = \alpha_1\mu_1^x + \ldots + \alpha_l\mu_l^x , \quad x = 1,2,\ldots$$

단 $l\ge 2$, $\alpha_1,\ldots,\alpha_l$ $\mu_1,\ldots,\mu_l$ $(\neq 0)\in L$.

보조 정리 2.2 $v(x)=0$, $1\le x\le N$ 의 해의 갯수는

$2lN(N^{-1}+T^{-1})\delta_l$ 이하이다.

단 T는 $1\le i,j\le l$ 에 대하여 $\mu_i^T = \mu_j^T$ 가 되는 최소의 자연수이다.

(증명) 생략.

또한 $\theta_i = \theta^{q^{i-1}}$, $1\le i\le n$ 이라 놓으면 아래와 같은 T의 하한을 얻는다.

([4] 참조)

보조 정리 2.3 $1 \le i < j \le l$ 에 대하여 T 가 $\theta_i^T = \theta_j^T$ 를 만족하는 최소의 자연수이면 $T \ge q$.
(증명) 생략.

정리 2.4 양수 c_1, c_2 에 대해서
$N \ge \max\{\exp(\exp(c_1 \log^2 n)), c_2 n \log q)\}$ 이면 $\theta, \theta^2, \ldots, \theta^N$ 중에 적어도 하나가 F_q 위에서 F_{q^n} 의 원시 정규기저를 생성한다.
(증명) $\nu(k)$ 를 정수 $k \ge 3$ 의 소인수의 갯수라 하자.
[5] 에 의하여 다음을 얻는다. $\nu(k)=O(\log k/\log\log k)$, 소인수정리에 의하여 c_2 가 상당히 큰 수이고 $n \ge c_2 n \log q$ 이면 구간 [1,N] 안에

$$R = N/2\log N \qquad (2\text{-}5)$$

개의 q^{n-1} 과 서로 소이고 서로 다른 숫수가 존재한다.
$\rho_1, \ldots, \rho_n$ 이 F_q 의 대수적 폐포에서 n 차 단위 근이라면 순환 행렬 A(k) 의 행렬식 $\det A(k) = v_1(k) \ldots v_n(k)$, $k=1,2,\ldots$
(단 $v_i(k) = u_0(k) + \rho_i u_i(k) + \ldots + \rho_i^{n-1} u_{n-1}(k)$, $1 \le i \le n$.
F_q 위의 F_{q^n} 의 정규기저가 존재하므로, 각 수열
$\{v(k)\}$, $k=1,2,\ldots$, $1 \le i \le n$, 은 0 이 아니다. 보조 정리 2.1에 의하여
$i=1,2,\ldots,n$ 에 대하여
$\alpha_{i,1}, \ldots, \alpha_{i,n}$ 중 적어도 0 이 아닌 원소가 있어

$$v_i(k) = \sum_{j=i}^{n} \alpha_{i,j}\, \theta_j^k \quad , \quad k = 1,2,\ldots \quad ([1] \text{ 참조})$$

보조 정리 2.2와 보조 정리 2.3에 의하여
$k=1,\ldots,N$ 중에서 $\det A(k)=0$ 이 되는 k 의 갯수는

$$2n^2 N(N^{-1}+T^{-1})\delta_n \qquad (2\text{-}6)$$

이하이다.
$N \ge c_2 n \log q$ 이고 $q \ge \exp\exp(c_1 \log^2 n)$, 또 c_1 이 충분히 크면 (2-6)은 (2-5)보다 작다. 따라서 $R - 2n^2 N(N^{-1}+T^{-1})$개의 원시 정규기저를 생성하는 $\theta^{k^{q^i}}$ 들이 있다. Q.E.D.

참고 문헌

[1] R. Lidl and H. Niederreiter, Introduction to Finite Fields and their Applications, Cambridge Univ. Press, Cambridge 1986.
[2] V. I. Solodovnikov, Upper bounds on complixity of solving system of linear equations, Zapiski Nauchn. Semin. LOMI Akad. Nauk. SSSR 118(1982), 159-187.
[3] D. Yu. Grigoriev, Factoring polynomials over a finite field and solving systems of algebraic equations, Zapiski Nauchn. Semin. LOMI Akad. Nauk SSSR 137(1984), 20-79.
[4] I. E. Shparlinskiy, On arithmetical properties of recurring sequences and some applications, Kand. dissert., M., Moscow State Pegagogical Inst., 1980.
[5] A. G. Postnikov, An introduction to analytic number theory, Moscow, Nauka, 1971.