通信情報保護學會誌
第2卷 第4號, 1992.12

유한체 위에 정의된 함수의 대수적 표준형식
The Algebraic Normal Form of Functions over Finite Fields

李敏燮*, 申鉉容**, 李俊烈***

스위치 이론이나 디지탈 공학[2], 정보보호학[6,8]등의 분야에서 자주 사용되는 많은 함수들은 유한체 $GF(q)^n$에서 $GF(q)$의 값을 취하는 함수들이다. 이러한 함수 f에서 함수값에 따라 독립변수들이 취하는 값을 표현하는 형식을 생각할 수 있다. 특히, $q=2$인 경우에 함수 f는 쉽게 진리표에 의해 표현된다. 본 글에서는 유한체 위에서 성립하는 행렬 구조를 갖는 대수적 표준형식 변환에 대하여 알아보고, 변환의 계산을 점화적으로 이행해보며, 난수함수의 복잡도에 관한 확률분포를 살펴본다. 대수적 표준형식은 함수의 비선형 위수나 복잡도에 관한 판단에 유용하게 응용할 수 있다.

1. 대수적 표준형식

함수 $f: GF(q)^n \to GF(q)$를 전사함수라고하자. 이때, 함수 f의 유한체 $GF(q)$에서의 대수적 표준형식(ANF Algebraic Normal Form)은

$$\begin{aligned} f(x_1,x_2,\cdots,x_n) &= a_0 + a_1x_1 + a_2x_2 + \cdots + a_nx_n \\ &+ a_{11}x_1^2 + a_{12}x_1x_2 + \cdots + a_{nn}x_n^2 \\ &+ a_{111}x_1^3 + a_{112}x_1^2x_2 + a_{123}x_1x_2x_3 + \cdots + a_{nnn}x_n^3 \\ &\vdots \\ &+ a_{11\cdots12\cdots2\cdots n\cdots n}x_1^{q-1}x_2^{q-1}\cdots x_n^{q-1} \end{aligned}$$

으로 정의된다. ANF의 각 곱셈항의 위수는 그 항에 있는 모든 변수들의 지수의 합으로 정의한다. 위의 표준식에서 최대위수는 $n(q-1)$이고 서로 다른 변수의 모든 차수를 고려할 때 q^n개의 서로 다른 항이 있게 된다. 따라서 f는 q^n개의 $GF(q)$에서 값을 취하는 계수 $a_{i\cdots j}$에 의해 결정된다. 따라서 이 계수들을 정함으로써 함수값을 계산하거나 논리회로를 구성할 수 있게 된다.

함수값이 주어졌을 때 ANF의 계수 $a_{i\cdots j}$를 어떻게 결정하는가는 스위치이론에서 Benjauthrit와 Reed[1]에 의하여 일반화된 Boole 대수 축차식에 의해 연구되었다. 여기서는 행렬변환에 의한 대수적 구조에 초점을 맞추어 본다.

일차독립인 q^n개의 곱셈항 $x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$, $i_j \in \{0,1,2,\cdots,q-1\}$, $j=1,\cdots,n$은 $GF(q)$위에서 n개의 변수를 갖는 q^{q^n}개의 함수 집합의 기저를 이룬다. 따라서 $x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$에 대한 기본벡터는 $GF(q)$위에서 q^n-차원 벡터가 된다.

먼저, 변수의 곱셈항 $x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$에 순서를 주는 방법을 생각하자.

정의 1.1. n개 변수 $x_1,x_2,\cdots,x_n$을 갖는 함수 $f: GF(q)^n \to GF(q)$의 대수적 표준형식 ANF에서 각 곱셈항은 다음의 순서를 갖는다.

* 단국대학교 자연과학대학 수학과 교수
** 한국교원대학교 제3대학 수학과 부교수
*** 강원대학교 사범대학 수학과 부교수

$$1, x_1, x_1^2, x_1^3, \cdots, x_1^{q-1}, x_2, x_1x_2, x_1^2x_2, \cdots, x_1^{q-1}x_2^{q-1},$$
$$\cdots, x_1^{q-1}x_2^{q-1}x_3^{q-1}\cdots x_n^{q-1}$$

위의 순서는 앞에 있는 곱셈항을 다음 변수와 곱하면서 복제하는 점화적 순서이다. 이 순서에 따라 점화적으로 얻어지는 특별한 행렬 구조가 얻어진다.

정의 1.2. 대수적 표준형식 ANF의 곱셈항이 정의 1.1에 의한 순서를 갖는다면, $GF(q)$계수벡터를 함수값의 벡터로 옮겨가는 $GF(q)$위에서의 일차변환 A_n은 다음의 점화관계를 만족한다.

$$A_0=1,$$
$$A_n=\begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \alpha & \alpha^2 & \cdots & \alpha^{(q-2)} \\ 0 & 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{(2(q-2))} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 1 & \alpha^{(q-2)} & \alpha^{2(q-2)} & \cdots & \alpha^{(q-2)^2} \\ 0 & 1 & 1 & 1 & \cdots & 1 \end{bmatrix} \otimes A_{n-1}$$
$$n=1,2,\cdots$$

단, α는 법 $q-1$에 관한 원시근이고, $\otimes$는 행렬의 Kronecker 곱이다.

증명. 변환행렬의 행벡터는 n변수 $x_1, x_2, \cdots, x_n$의 함수값의 모든 조합에 의한 곱셈으로 얻어진다. ANF의 곱셈항의 순서를 고려하여 A_n을 구한다.

보기 1. $q=2$, n=4인 경우

1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
x_1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
x_2	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
x_3	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1
x_4	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
x_1x_2	0	0	0	0	0	1	0	1	0	0	0	0	0	1	0	1
x_1x_3	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1
x_1x_4	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
x_2x_3	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
x_2x_4	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	1
x_3x_4	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	1
$x_1x_2x_3$	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1
$x_1x_2x_4$	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1
$x_1x_3x_4$	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1
$x_2x_3x_4$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
$x_1x_2x_3x_4$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

이 때, $A_n=\begin{bmatrix} A_{n-1} & A_{n-1} \\ O_{n-2} & A_{n-1} \end{bmatrix}$, $n=1,2,3,\cdots$,

$$=\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \otimes A_{n-1}$$

단, O_{n-2}는 $q^{(n-2)}\times q^{(n-2)}$차원의 0항 행렬이다.

이제 함수값을 나타내는 벡터가 주어졌을 때 ANF계수벡터를 얻기 위한 선형변화의 역에 대하여 알아보자. 먼저 정리 1.2에서

$$A_1=\begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \alpha & \alpha^2 & \cdots & \alpha^{(q-2)} \\ 0 & 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{(2(q-2))} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \\ 0 & 1 & \alpha^{(q-2)} & \alpha^{2(q-2)} & \cdots & \alpha^{(q-2)^2} \\ 0 & 1 & 1 & 1 & \cdots & 1 \end{bmatrix}$$
$$=\begin{bmatrix} \vec{e^t} & \mathrm{M} \\ & \\ & \\ 0 & \vec{1} \end{bmatrix}$$

으로 나타내고,

$$B_1=\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & -1 \\ 0 & -1 & -1 & \cdots & -1 & -1 \\ 0 & -\alpha^{q-2} & -\alpha^{q-3} & \cdots & -\alpha & -1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & -\alpha^{(q-2)^2} & -\alpha^{(q-2)^2-1} & \cdots & -\alpha^{q-2} & -1 \end{bmatrix}$$
$$=\begin{bmatrix} 1 & -\overrightarrow{e_{q-2}} \\ & \\ & \\ \vec{0^t} & -M^r \end{bmatrix}$$

로 두자. M^r은 M을 오른쪽으로 회전하여 얻은 행렬이다. 그러면,

$$A_1B_1=\begin{bmatrix} \vec{e_0^t} & -MM^r-\begin{bmatrix} 0 & 0 & \cdots & 1 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & 0 \end{bmatrix} \\ & \\ 0 & \vec{m} \end{bmatrix}$$

보조정리 1.3. 위의 A_1B_1에서 $P=-MM^r=(p_{ij})$는

$$p_{ij}=\begin{cases}1\ ;\ j=i+1,\ 0\le i<q-2\\ 1\ ;\ i=0,\ j=q-2\\ 0\ ;\ \text{그밖의 경우}\end{cases}$$

로 주어진다.

증명. 임의의 $0\neq\beta\in GF(q)$에 대하여 $\beta^{q-1}=1$임을 유의하면,

$$-p_{ij}=\sum_{k=0}^{q-2}(\alpha^{q-2-j+1})^k=\sum_{k=0}^{q-2}\beta^k=\begin{cases}0, & \beta\neq 1\\ -1, & \beta-1\end{cases}$$

위의 보조정리로부터 $\vec{m}$을 쉽게 결정할 수 있다.

따름정리 1.4. $\vec{m}=-\vec{1}M^r=\overrightarrow{e_{q-2}}=(0,0,\cdots,0,1)$. 결국 $A_1B_1=I$가 된다.

정리 1.5. ANF의 계수행렬 A_n의 역행렬 A_n^{-1}은 다음의 점화관계를 갖는다.

$$A_0^{-1}=[1]$$
$$A_n^{-1}=B_1\otimes A_{n-1}^{-1},\ n=1,2,3,\cdots$$

단, B_1은 위에서 정의된 행렬이다.

증명. B_n을 A_n^{-1}라고 두면 $A_nB_n=I_n$ 임을 보이면 된다. 수학적 귀납법을 적용하면,

(1) $A_0B_0=[1]=I_0$

(2) $A_{n-1}B_{n-1}=I_{n-1}$ 이라고 가정하면,

$$\begin{aligned}A_nB_n&=(A_1\otimes A_{n-1})(B_1\otimes B_{n-1})\\&=A_1B_1\otimes A_{n-1}B_{n-1}\\&=A_1B_1\otimes I_{n-1}\\&=I_1\otimes I_{n-1}=I_n\end{aligned}$$

보기 2. $GF(3)$, $GF(4)$와 $GF(5)$에서 행렬 B_1은 다음과 같이 주어진다.

$$GF(4):\begin{bmatrix}1&0&0&1\\0&1&1&1\\0&\alpha^2&\alpha&1\\0&\alpha&\alpha^2&1\end{bmatrix}\quad \text{단 } \alpha^2+\alpha+1=0$$

$$GF(3):\begin{bmatrix}1&0&2\\0&2&2\\0&1&2\end{bmatrix}\qquad GF(5):\begin{bmatrix}1&0&0&0&4\\0&4&4&4&4\\0&2&1&3&4\\0&1&4&1&4\\0&3&1&2&4\end{bmatrix}$$

보기 3. $GF(2)$인 경우에는 ANF의 계수행렬이 보다 단순히 결정된다.

곧, $A_1=\begin{bmatrix}1&1\\0&1\end{bmatrix}$, $B_1=\begin{bmatrix}1&1\\0&1\end{bmatrix}$

$A_n=A_1\otimes A_{n-1}$, $B_n=B_1\otimes B_{n-1}$

그런데, $A_1=B_1$이므로 B_n과 A_n의 역할이 같다.

$\therefore A_n^{-1}=B_n=A_n$

2. 변환의 실행

대수적 표준형식 변환 ANFT는 이 변환행렬의 구조로부터 아주 효과적으로 계산할 수가 있다. $\Phi_n=(\phi_1,\phi_1,\cdots,\phi_{2^n-1})$을 $GF(2)$에서 값을 취하는 함수값의 벡터라고 하자. 곧, 벡터기호를 갖는 진리표로 나타난다고 하자. 또 함수값벡터 $\vec{v}$를 $\vec{v}=\vec{v}^1\mid\vec{v}^2$와 같이 $\vec{v}$의 전반, 후반을 나누어 나타내자. 그러면 위수 n인 ANFT는 2개의 2를 법으로 하는 덧셈과 위수 $n-1$인 ANFT로 바뀌어진다.

$$\Phi_nA_n=\Phi^1A_{n-1}\mid(\Phi_n^1+\Phi_n^2)A_{n-1}$$

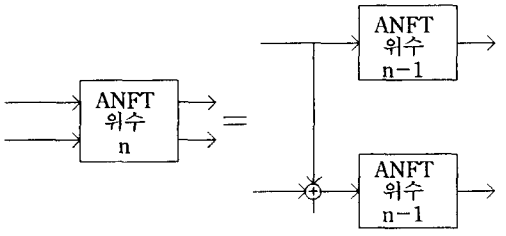


그림 1.

이러한 과정을 n번 반복하면 위수 n인 ANFT는 위수 0인 ANFT로 곧, 2를 법으로 하는 덧셈만으로 바꾸어 써지게 된다. 여기서 2를 법으로 하는 덧셈의

총수는

$$\frac{m}{2}\log_2 m,\quad m=2^n=\text{벡터 } \Phi_n\text{의 길이}$$

가 된다.

아래 그림 2는 $n=3$인 ANFT를 점화식으로 나타낸 것이고, 그림 3은 Fast Fourier Transform과 비슷하게 교차형태로 나타낸 것이다.

이러한 알고리즘은 hardware나 응용프로그램에서 쉽게 만들어 계산할 수가 있다.

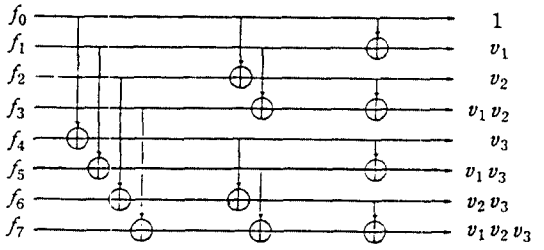


그림 2.

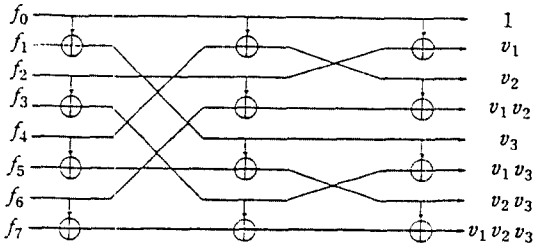


그림 3.

3. 난수이진함수

난수이진함수에 1절의 내용을 적용하여 보자. 이진함수란 독립변수의 각 성분의 함수값이 0과 1을 확률 1/2로 취하는 함수 곧, 진리표에서 각 비트-항-은 독립적인 난수인 함수이다. 이제 ANF계수에 관한 통계적 분석을 행하여 보자.

보조정리 3.1. 난수이진함수에 대하여 ANF의 계수들은 독립이고, 확률을 P[0]=P[1]=1/2로 갖는 분포를 이루는 이진확률변수(binary random variable)이다.

증명. 변환행렬 A_n이 역행렬을 갖기 때문에 $P_r(0)=P_r(1)=1/2$이 된다.

이제 함수의 복잡도의 의미를 통하여 난수이진함수의 복잡도에 관하여 알아보자. 함수의 복잡도는 ANF의 각 곱셈항의 수만이 아니라 (앞의 보조정리로부터 이항분포에 따르게 된다) 곱셈항의 위수와도 관련이 있다. 함수의 복잡도를 정의하기 전에 함수의 비선형 위수에 관한 통계적 분석을 하여 보자. 여기서 함수의 위수는 ANF에서 곱셈항의 최대위수가 된다.

정리 3.2. n변수 난수 이진함수에 대하여 비선형 위수 Θ의 평균과 분산은 다음과 같다.

$$E[\Theta]=n-\sum_{k=0}^{n-1}2^{-S_n(k)}$$

$$Var[\Theta]=\sum_{k=0}^{n-1}(2k+1)2^{-S_n(k)}-\left(\sum_{k=0}^{n-1}2^{-S_n(k)}\right)^2$$

여기서 $S_n(k)=\sum_{i=0}^{k}\binom{n}{i}$이다.

증명. ANF에는 2^n개의 계수가 있고 각 계수는 확률 1/2로 나타난다. i차 곱셈항의 계수는 $\binom{n}{i}$개 만큼 있다. 함수의 위수는 곱셈항의 최대위수이므로

$$\Pr[\Theta=n-j]=\left(\prod_{k=0}^{j-1}2^{-\binom{n}{k}}\right)\left(1-2^{-\binom{n}{k}}\right)$$

$$=2^{-S_n(j-1)}-2^{-(2^n-1)},\quad 0\le j\le n$$

$$\Pr[\Theta=0]=2^{-(2^n-1)}$$

위의 계산을 정리하여 위수 Θ에 관한 정리를 얻는다.

평균과 분산은 각각 근사값으로 다음과 같이 된다.

$$E[\Theta]\approx n-1/2-2^{-(n+1)}$$
$$Var[\Theta]\approx 1/4+2^{-n}$$

결국 난수이진함수는 거의 최대값에 가까운 위수를 갖는다고 할 수 있다. 이미 언급되었지만 ANF의 곱셈항의 수나 비선형 함수의 위수만으로는 함수의 복잡도를 서술하는데 충분하지 못하다. 그러므로 복잡도의 측도로서 각 계수에 가중치를 준 합을 생각하게 된다.

정의 3.3. n개의 변수를 갖는 이진함수 f의 복잡도를 f의 ANF에 있는 2^n개의 계수에 실수 가중치를 준 합으로 정의한다.

복잡도 c는 $c : GF(2)^{2^n} \rightarrow N$으로 2^n의 길이를 갖는 이진벡터에 실수를 대응시킨다.

실수 $\bar{\gamma}=c(\vec{a})=\vec{a}\vec{w}^t$, $\vec{a}$는 ANF 계수벡터, $\vec{w}$는 가중치벡터라고 하자. 이제 $\vec{w}$를 (1,2,2,3,2,3,3,4, 2,3,3,4,…)라고 하면 이것은 합이 곱보다 다소 어려운 경우를 표현하는데 디지탈 전자회로에서 나타나는 가중치벡터이다. 이 때의 난수이진함수의 복잡도는 $\bar{\gamma}$는

$$\bar{\gamma}=(\frac{n}{2}+1)2^{n-1}$$

이 된다.

위의 복잡도 정의에서 각 가중치는 hardware나 software에서 함수를 계산할 때 어려운 정도를 나타내는 값을 갖도록 한다. 특별히 $q=2$인 경우에 행렬 B_1은 음부호가 없어지므로 $B_1=A_1$이 되어 $GF(2)$인 경우가 된다.

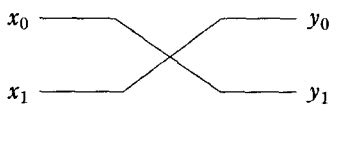
보기 4. $GF(2)^2$와 $GF(4)$를 비교하여 보자.

변수 x_0, x_1이 $GF(2)$에서 값을 취하는 길이 2인 벡터 $\vec{x}=(x_0,x_1)$가 $\vec{y}=(y_0,y_1)$로 아래의 그림에서처럼 교차하여 변환되었다고 하자. 이 경우에 가중치벡터 $\vec{w}$가 (1,2,2,4)로 주어진다면 이 변환의 복잡도 $2\gamma_2$는

$$2\gamma_2 = 2\times 4 = 8$$

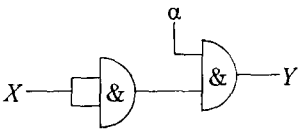
이 된다.

x_0	x_1	y_0	y_1
0	0	0	0
0	1	1	0
1	0	0	1
1	1	1	1



이제, $GF(4)$에서 값을 취하는 X,Y를 변수로 하는 벡터 변수 (X,Y)를 생각해보자. 여기서 $Y=\alpha x^2$, $\alpha^2+\alpha+1=0$이 된다. 유한체 $GF(4)$에서 이 변환을 계산하는 회로는 2개의 $GF(4)$ 곱인자(multiplier)로 이루어진다.

X	Y
0	0
1	α
α	0
α^2	α^2



이 경우의 복잡도는 분명히 교차된 경우보다 복잡하다. 복잡도를 $q=2$인 경우와 마찬가지 방법으로 구할 수 있다. 어쨌든 $GF(q)$에서의 복잡도는 상수에 의한 곱셈도 고려하여야 한다. 가중치벡터를 (2,4, 6,8)로 택하고, a에 의한 곱을 고려한다면, 복잡도는 $\gamma_4=12$가 된다.

4. 결 론

본 글에서는 유한체에서 정의된 함수를 대수적 표준형식으로 표현하는 변환 방법을 소개하였다. 이 때의 변환은 행렬형태에 기본을 두었고, Hadamard, Walsh나 Fourier 변환의 fast변환과 유사한 점이 있음을 보였다. ANFT를 난수이진함수에 적용하여 그 복잡도를 살펴보았다. 이러한 접근방법은 유한체 위의 변환이론에 기여하게 될 것이고 여기서 얻어진 대수적 표준형식은 정보보호분야에도 성공적으로 적용될 수 있을 것이다.

참 고 문 헌

1. B. Benjauthrit and I.S. Reed. "Galois Switching Functions and Their Applications", IEEE Trans. on Comp., Vol. C-25, pp.78-86, January 1976.

2. T.K. Gaylord and M.M. Mirsalehi, "Truth-table look-up processing: number representation, multilevel coding and logical minimization", Optical Engineering, Vol.25, No.1, January 1986.

3. S.W. Golomb, "On the classification of Balanced Binary Sequences of Period 2^n-1", IEEE Trans. On Info. Theory, Vol. IT-26, No.6, pp.

730-732, November 1980.

4. C.J.A. Jansen, and D.E. Boekee, "The Algebraic Normal Form of Arbitary Functions of Finite Fields", Proceedings of the Eighth Symposium on Information Theory in the Bendux, Deventer, The Netherlands, pp.66-76, May 1987.

5. E. Kranakis, Primality and Cayptography, John Wiely, New York, 1986.

6. R.A. Rueppel, New Approaches to stream Ciphers, PHD. Thesis, Swiss Fedral Institute of Technology, Zurich, 1984.

7. T. Siegenthaler, "Decrypting a Class of Stream Ciphers Using Ciphertext Only", IEEE Trans. on Comp., Vol.C-34, No.1, pp.81-85, January 1985.

8. T. Siegenthaler, "Correlation-Immune Polynomials over Finite Fields", Eurocrypt 86, Linkoping, Sweden, 1986.

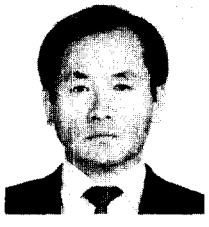
9. 박승안, GF(2)위의 고차다항식 및 이진수열에 관한 수학적연구, 한국전자통신연구소, 1986.

10. 박승안, 이민섭, 이재학, 신현용, 대수적 부호이론, 체신부, 1991.

□ 著者紹介

李 敏 燮(終身會員)

서울大學校 師範大學 數學科(理學士)
西江大學校 大學院(理學碩士)
University of Alabama (理學博士)
현재 檀國大學校 自然科學大學 數學科 教授, 情報通信保護學會誌 編輯委員



申 鉉 容(終身會員)

서울大學校 師範大學 數學科(理學士)
서울大學校 大學院(理學碩士)
University of Alabama (理學博士)
현재 韓國教員大學校 第3大學 數學科 副教授

李 俊 烈(終身會員)

서울大學校 師範大學 數學科(理學士)
서울大學校 大學院(理學碩士)
University of Alabama (理學博士)
현재 江原大學校 師範大學 數學科 副教授