通信情報保護學會論文誌
第 8 卷　第 2 號, 1998. 6

완비함수의 존재성에 관한 몇가지 성질

이 민 섭*, 최 춘 수*

Some Properties on Existence of a Complete Function

Min Surp Rhee*, Chun Soo Choi*

요 약

블럭암호의 비도는 S-box의 비도와 운영방식에 의존된다. S-box의 크기의 증가에 따라 비도가 증가하지만, 큰 S-box를 설계하는 일은 일반적으로 매우 어렵다. 한편, S-box 의 비도는 이 함수의 성분함수인 Boole 함수의 비선형성, 상관면역위수, SAC, 균형성 등에 의존되며, S-box 자체의 비선형성, 입력성분(또는 입력비트)에 대한 출력성분(또는 출력비트)의 독립성 등에 의존된다. 이와 같은 출력 성분의 독립성에 관한 개념의 하나가 완비성이다.

본 논문에서는 Galois 체 $GF(2)$위에 n차원 벡터공간 $GF(2)^n$에서 완비함수의 존재성에 관한 몇 가지 알고리즘과 완비함수가 만족하는 성질들을 조사하였다.

Abstract

While there is evidence that large substitution boxes(S-boxes) have better cryptographic properties than small S-boxes, they are much harder to design. The difficulty arises from the relative scarcity of suitable Boole functions as the size of the S-box increases. Completeness of an S-box is one of important concepts of encryption schemes. In this paper, we describe some methods on existence of a complete function on $GF(2)^n$ and study some properties on a complete function on $GF(2)^n$, where $GF(2)^n$ is an n dimensional vector space over a Galois field $GF(2)$.

Key Words : S-box, completeness, Boole function, permutation

1. 서 론

두 원소 0과 1을 가지는 Galois 체 $GF(2)$위에 두 연산 $\oplus$와 $\otimes$는

$$0 \oplus 0 = 1 \oplus 1 = 0, \quad 0 \oplus 1 = 1 \oplus 0 = 1$$
$$1 \otimes 1 = 1, \quad 1 \otimes 0 = 0 \otimes 1 = 0 \otimes 0 = 0$$

이다. 단, 문자의 곱셈에서는 보통 $\otimes$을 생략한다. 체 $GF(2)$위에 n차원 벡터공간 $GF(2)^n$

이 연구는 단국대학교 대학연구비의 지원으로 연구 되었음.

*단국대학교 수학과

에서 m차원 벡터공간 $GF(2)^m$으로 보내는 S-box 중, 특히 일대일대응 함수 $f : GF(2)^n \rightarrow GF(2)^n$가 다음과 같은 조건을 만족할 때 이 함수를 완비함수(complete function)라고 한다 :

임의의 $i,j \in \{1, 2, \cdots, n\}$에 대하여 $f_j(\overrightarrow{x}) \neq f_j(\overrightarrow{y})$인 i번째 성분만 다른 벡터 $\overrightarrow{x}$와 $\overrightarrow{y}$가 $GF(2)^n$에 존재한다. 단, $f_j(\overrightarrow{x})$는 벡터 $f(\overrightarrow{x})$의 j번째 성분이다.

즉, 완비함수는 임의의 j번째 성분이 다른 함수 값에 대하여 임의의 i번째 성분만 다른 벡터가 존재하는 함수를 의미한다. 즉, 임의의 i번째 성분만 다른 벡터에 대하여 함수값의 어떤 성분도 달라질 수 있는 함수이다.

Shannon의 고전적 논문[7]에 의하면 S-box는 혼돈이론(confusion property)을 가지는 블럭암호를 만든다고 설명했다. DES와 같은 대칭블럭암호의 비도가 강하게 되려면 S-box $f : GF(2)^n \rightarrow GF(2)^m$ 가 강해야 한다. 이와 같은 S-box가 강하게 되려면 여러 가지 성질을 만족해야 한다. 일반적으로, 큰 S-box는 작은 S-box보다 강함은 많은 연구에 의하여 잘 알려져 있다[2,3,4]. 같은 크기에서는 성분함수의 비선형성(nonlinearity), SAC, 균형성(balanceness), 상관면역위수(correlation immune order) 등에 관계된다[6]. 또한 S-box의 비선형성, 출력성분의 독립성, 완비성[5]등을 고려해야만 한다. 즉, 임의의 i와 j에 대하여, i번째 입력비트(또는 성분)가 바뀔 때마다 j번째의 출력비트(또는 성분)가 바뀔 확률이 $\frac{1}{2}$이고, 하나의 입력비트(또는 성분)가 바뀔 때, i번째 출력비트가 j번째의 출력비트와 같을 확률이 $\frac{1}{2}$이 되는 S-box가 바람직하다. 특히, 이와 같은 S-box중에 출력비트의 수와 입력비트의 수가 같은 전단사 함수로서 입력성분에 따른 출력성분의 독립성에 관한 개념들 중에 하나가 완비성이다.

이 논문에서는 [5]에서 설계한 완비함수의 존재성을 엄밀하게 증명하고, 완비함수의 몇 가지 성질을 밝히고 $GF(2)^n$위에 완비함수 E_k에 관하여 살펴본다. 자주 쓰이는 몇 가지 기호를 설명하면 다음과 같다:

(1) V_n : 체 $GF(2)$위에서의 n차원 벡터공간 $GF(2)^n$. $GF(2)^n$의 원소인 벡터 $\overrightarrow{x} = (x_1, \cdots, x_n)$는 $\overrightarrow{x} = x_1 \cdots x_n$ 으로 나타내기도 함

(2) $\overline{x_i}$: $x_i \in GF(2)$의 여성분, 즉 $\overline{0} = 1$ 이고 $\overline{1} = 0$

(3) $\overrightarrow{\overline{x_i}}$: 벡터 $\overrightarrow{x} = V_n$의 각 성분의 여성분으로 이루어진 벡터

(4) $\overrightarrow{e_i}$: 오직 i번째 성분만 1이고 나머지 성분은 모두 0인 기본벡터

(5) E_k : 다음과 같이 정의된 함수

$$E_k \;:\; V_n \rightarrow V_n$$

$$E_k(\overrightarrow{x}) = \begin{cases} \overrightarrow{\overline{x}} & : \overrightarrow{x} \in \{\overrightarrow{e_k}, \overrightarrow{\overline{e_k}}\} \\ \overrightarrow{x} & : \overrightarrow{x} \notin \{\overrightarrow{e_k}, \overrightarrow{\overline{e_k}}\} \end{cases}$$

(6) $(\overrightarrow{x}, \overrightarrow{y}) = (x_1, \cdots, x_m, y_1 \cdots, y_n) : \overrightarrow{x} = (x_1, \cdots, x_m)$와 $\overrightarrow{y} = (y_1 \cdots, y_n)$에 의하여 만들어진 $m+n$차원 벡터

(7) S_n : 집합 $\{1, 2, \cdots, n\}$

2. 완비함수의 존재성과 설계

이 절에서는 완비함수의 존재성과 설계에 관하여 살펴본다. 이를 위하여 서론에서 정의한 완비함수를 엄밀하게 정의하면 다음과 같다.

정 의 2.1임의의 벡터$\overrightarrow{x} \in V_n$에 대하여

$f(\overrightarrow{x}) = (f_1(\overrightarrow{x}), f_2(\overrightarrow{x}), \cdots, f_n(\overrightarrow{x})),$

$f_i : V_n \rightarrow GF(2)$

으로 정의되는 함수 $f : V_n \rightarrow V_n$가 임의의 $i,$

$j \in S_n$에 대하여 i번째 성분만 다른 벡터 $\vec{x}$ 와 $\vec{y}$가 V_n에 존재하여 $f_i(\vec{x}) \neq f_i(\vec{y})$일 때, f를 완비함수라고 한다.

예를 들면, 일대일대응 함수 $f : V_3 \rightarrow V_3$가 임의의 $\vec{x} \in V_3$에 대하여

$$f(\vec{x}) = (f_1(\vec{x}),\ f_2(\vec{x}),\ f_3(\vec{x})),$$

$$f_i(\vec{x}) = x_i \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_3$$

로 정의되면 f는 완비함수이다.

이제 주어진 완비함수로 부터 새로운 완비함수를 만들기 위하여 함수연산을 정의하여 보자. 집합 S_n에서 S_n으로 보내는 전단사함수(bijective function)를 특히, S_n위에서의 치환(permutation)이라 하고 치환들의 집합을 n차 대칭군(symmetric group)이라 한다.

정 의 2.2 임의의 $\vec{x} \in V_n$에 대하여 $f(\vec{x}) = (f_1(\vec{x}),\ f_2(\vec{x}),\ \cdots,\ f_n(\vec{x}))$ 으로 정의되는 함수 $f : V_n \rightarrow V_n$과 S_n 위에서의 치환 σ가 주어져 있을 때, 새로운 함수 $\sigma\ f : V_n \rightarrow V_n$을 다음과 같이 정의한다 :

$$(\sigma\ f)(\vec{x}) = (f_{\sigma(1)}(\vec{x}),\ f_{\sigma(2)}(\vec{x}),\ \cdots,\ f_{\sigma(n)}(\vec{x}))$$

$$(f\ \sigma)(\vec{x}) = f(x_{\sigma(1)},\ x_{\sigma(2)},\ \cdots,\ x_{\sigma(n)})$$

즉 $\sigma\ f$는 함수f의 함수값의 성분의 치환이고, $f\ \sigma$는 $\vec{x}$의 성분 x_i들의 치환에 의하여 만들어진 함수이다.

위의 정의들로부터 다음 성질을 쉽게 얻을 수 있다.

성 질 2.3 함수 $f : V_n \rightarrow V_n$가 완비함수일 때, S_n위에서의 임의의 치환σ에 대하여 함수 $\sigma\ f$와 $f\ \sigma$ 또한 완비함수이다.

증 명 함수 f는 완비함수이므로 임의의 i, $j \in S_n$에 대하여 $f_i(\vec{x}) \neq f_i(\vec{y})$인 i번째 성분만 다른 벡터 $\vec{x}$와 $\vec{y}$가 V_n에 존재한다. 따라서 치환σ에 대하여 $f_{\sigma(j)}(\vec{x}) \neq f_{\sigma(j)}(\vec{y})$이고 치환$\sigma$는 전단사함수이므로 $\sigma\ f$는 완비함수이다. 한편, 치환σ에 대하여 $\sigma(\vec{x}) = (x_{\sigma(1)},\ x_{\sigma(2)},\ \cdots,\ x_{\sigma(n)})$이고 서로 다른 i와 j에 대하여 $\sigma(i) \neq \sigma(j)$이다. 함수 f가 완비함수이므로 임의의 $\sigma(i)$, $j \in S_n$에 대하여 $f_j(\vec{x}) \neq f_j(\vec{y})$인 $\sigma(i)$번째 성분만 다른 벡터 $\vec{x}$와 $\vec{y}$가 V_n에 존재한다. 따라서 $\sigma(i)$가 S_n의 임의의 값이므로 $f\ \sigma$ 또한 완비함수이다.

위 정리에 의하면, n차 대칭군의 원소인 치환들의 개수가 $n!$개이므로 V_n에서 하나의 완비함수f를 찾을 때마다 완비함수f를 이용하여 $n!$개의 서로 다른 완비함수를 V_n에서 찾을 수 있다.

다음과 같이 정의된 E_k가 완비함수임을 밝히므로 $n \geq 3$일 때, V_n위에서 완비함수의 존재성이 증명된다 :

$$E_k(\vec{x}) = \begin{cases} \overline{\vec{x}} & : \vec{x} \in \{\vec{e_k},\ \overline{\vec{e_k}}\} \\ \vec{x} & : \vec{x} \notin \{\vec{e_k},\ \overline{\vec{e_k}}\} \end{cases}$$

단, $\vec{e_k}$는 k번째 성분을 제외한 모든 성분이 0이고 $\overline{\vec{e_k}}$는 $\vec{e_k}$의 여성분으로 이루어진 벡터이다. 그러면 임의의 k에 대하여 함수E_k는 가장 간단한 형의 완비함수가 된다.

정 리 2.4 임의의 $n \geq 3$에 대하여, 함수E_k는 완비함수이다.

증 명 정리 2.4를 증명하기 위하여 먼저 E_1이 완비함수임을 증명한다.
먼저 $i = 1$이면, 실제로

$$E_1(\vec{e_1}) = \overline{\vec{e_1}} \neq \vec{0} = E_1(\vec{0})\text{이고}$$

$$E_1(\overrightarrow{e_1} \oplus \overrightarrow{e_2}) = \overrightarrow{e_1} \oplus \overrightarrow{e_2} \neq \overrightarrow{e_2} = E_1(\overrightarrow{e_2})$$

이다. 따라서 임의의 j에 대하여 $E_1(\overrightarrow{x})$와 $E_1(\overrightarrow{y})$가 적어도 j번째 성분이 달라지는 첫번째 성분만 다른 벡터 $\overrightarrow{x}$와 $\overrightarrow{y}$가 V_n에 존재한다.

이제, $i\neq 1$인 경우에는 두 가지 방법으로 증명한다.

(ⅰ) $n=3$: $E_1(\overrightarrow{e_i}) = \overrightarrow{e_i} \neq \overrightarrow{e_1} = E_1(\overline{\overrightarrow{e_1}})$,

$E_1(\overrightarrow{e_i}) = \overrightarrow{e_i} \neq \overrightarrow{0} = E_1(\overrightarrow{0})$

(ⅱ) $n\geq 4$: $E_1(\overrightarrow{e_1} \oplus \overrightarrow{e_i}) = \overrightarrow{e_1} \oplus \overrightarrow{e_i} \neq \overrightarrow{e_1}$

$= E_1(\overline{\overrightarrow{e_1}})$,

$E_1(\overrightarrow{e_2} \oplus \overrightarrow{e_i}) = \overrightarrow{e_2} \oplus \overrightarrow{e_i} \neq \overrightarrow{e_2}$

$= E_1(\overline{\overrightarrow{e_2}})$

이다. 따라서 임의의 j에 대하여 $E_1(\overrightarrow{x})$와 $E_1(\overrightarrow{y})$이 적어도 j번째 성분이 달라지는 i번째 성분만 다른 벡터 $\overrightarrow{x}$와 $\overrightarrow{x}$가 V_n에 존재한다. 그러므로 함수E_1은 완비함수이다.

S_n위에서의 치환 $\sigma=(1k)$를 생각하면

$$E_k(\overrightarrow{x}) = (\sigma \cdot E_1 \cdot \sigma)(\overrightarrow{x})$$

가 된다. 따라서 함수 E_k는 완비함수이다.

$n\geq 3$일 때 V_n위에서 완비함수의 존재성을 다른 방법을 통하여 생각해 보자.

벡터공간은 덧셈군이므로 집합 {0,…,0 1…1 }은 n차원 벡터공간 V_n의 정규부분군이고, 따라서 2^n개의 벡터는 2^{n-1}개의 잉여류(또는 벡터의 쌍)들

$$Y=\{\{\overrightarrow{y_i}, \overline{\overrightarrow{y_i}}\}\ i=1,\ 2,\ \cdots,\ 2^{n-1}\}$$

의 형태로 분할할 수 있다. 또한, V_n은 다음과 같은 부분집합 X_n을 가진다.

보조정리 2.5 $n\geq 3$일 때, 벡터공간 V_n으로부터 부분집합 $X_n = \bigcup_{j=1}^{n}\{\overrightarrow{v_j}, \overrightarrow{v_j}'\}$을 선택할 수 있다. 여기서 $\overrightarrow{v_j}$와 $\overrightarrow{v_j}'$는 V_n에서 j번째 성분만 다른 벡터이고 $j\neq l$인 임의의 j, l에 대하여$\{\overrightarrow{v_j}, \overrightarrow{v_j}'\}\cap\{\overrightarrow{v_l}, \overrightarrow{v_l}'\}=\varnothing$이다.

증명 $n=3$이면, $X_3=\{\{000,100\},\ \{101,111\},\ \{011,010\}\}$이 존재한다.

$n=r\ \geq\ 3$인 경우에 V_r의 부분집합X_r이 존재한다고 가정하자. 즉,

$X_r = \bigcup_{j=1}^{r}\{\overrightarrow{v_j}, \overrightarrow{v_j}'\}$, 단 $\overrightarrow{v_j}$와$\overrightarrow{v_j}'$는 V_r에서 j번째 성분만 다른 벡터이다

이제, $n=r+1$일 때 성립함을 보이자. 벡터공간 V_r의 임의의 벡터 $\overrightarrow{v}=(v_1,\ \cdots,\ v_r)$에 대하여 V_{r+1}의 원소 $\overrightarrow{v_*}=(v_1,\cdots\ ,v_r,0)$와 $\overrightarrow{v^*}=(v_1,\cdots,v_r,1)$을 약속하면,

$$X_{r+1} = \bigcup_{j=1}^{r}\{\overrightarrow{v_j^*},\ \overrightarrow{v_j^{*}}'\}\cup\{\overrightarrow{x^*}\ \overrightarrow{x_*}'\},\ \overrightarrow{v_j}, \overrightarrow{v_j}'\ \in X_r$$

$$\overrightarrow{x}\in V_r \backslash X_r$$

은 j 번째 성분만 다른 $2r+2$개의 벡터들이다 $(j=1,2,\cdots,r+1)$. 그러므로 X_{r+1}는 $n=r+1$인 경우에 요구되는 집합이다.

정리 2.6 n차원 벡터공간 V_n위에서 완비함수가 존재한다.

증명 함수 f : $V_n \rightarrow V_n$ 를 X_n에 속하는 $2n$개의 벡터에 대하여 위에서 정의한 집합 Y의 적당한 n개의 쌍을 선택하여 $f(\overrightarrow{v_j})=\overrightarrow{y_i}$ 이고 $f(\overrightarrow{v_j}')=\overline{\overrightarrow{y_i}}$으로 정의된 일대일대응 함수는 완비함수이다.

정리 2.6에 의하여 만들 수 있는 완비함수의 개수는 적어도 $\binom{2^{n-1}}{n}\times n!\times 2^n\times(2^n\text{-}2n)!$ 이다.

이제, V_n에서의 완비함수 f로 부터 $V_{n'}$ 에서의 완비함수 F*를 유도하는 방법을 알아 본다.

보조정리 2.7 함수 f : $V_n \to V_n$ 가 완비함수라면, 함수 f로 부터 완비함수 F: $V_{n^2} \to V_{n^2}$ 를 유도할 수 있다.

증명 S_{n^2} 위에서의 치환 σ을

$\sigma(s) = (q-1)n+p$ (단, $s=(p-1)n+q$ 이고 $1 \le p,\ q \le n$ 이다)

로 정의하고, 임의의 $\overrightarrow{x_p} \in V_n$에 대하여 함수 f를 $f(\overrightarrow{x_p})=(f_1(\overrightarrow{x_p}),)\cdots f_n(\overrightarrow{x_p}))$ 이라고 하자. 단, $\overrightarrow{x_p}=(x_{(p-1)n+1},\ x_{(p-1)n+2},\ \cdots,\ x_{pn})$이다.

임의의 $\overrightarrow{x_p} \in V_{n^2}$ 에 대하여 함수 G :$V_{n^2} \to V_{n^2}$과 함수 F:$V_{n^2} \to V_{n^2}$를

$$G(\vec{x})=(G_1(\vec{x}),\ G_2(\vec{x}),\ \cdots,\ G_{n^2}(\vec{x})),$$
$$\vec{x}=(\overrightarrow{x_1},\ \cdots,\overrightarrow{x_n})$$

(단, $G_{(p-1)n+q}(\vec{x}) = f_q(\overrightarrow{x_p}),\ 1 \le p,q \le n$)

$$F(\vec{x})=(G \circ \sigma \circ G)(\vec{x})$$

으로 정의하고 함수 F가 완비함수임을 보이자.

함수 f 와 치환 σ가 일대일대응 함수이므로 함수 G, F 또한 일대일대응 함수이다. S_{n^2}의 임의의 값 $j=(p-1)n+q(1 \le p,\ q \le n)$ 에 대하여, 함수 f가 완버함수이므로 $\{(p-1)n+1,\ \cdots,\ pn\}$ 에서 임의의 i_p에 대하여 $\overrightarrow{u_p}$와 $\overrightarrow{v_p}$가 i_p번째 성분만 다르면서

$$G_j(\vec{u})=f_q(\overrightarrow{u_p}) \neq f_q(\overrightarrow{v_p})= G_j(\vec{v})$$

인 두 개의 벡터 $\vec{u}=(\overrightarrow{u_1},\ \cdots,\overrightarrow{u_n})$와 $\vec{v}=(\overrightarrow{v_1},\ \cdots,\overrightarrow{v_n})$ 가 존재한다.

한편, $i_p = (p-1)n+k$이라고 하자. 단, $1 \le k \le n$ 이다. 그러면 $\sigma^{-1}(i_p)=(k-1)n+p$ 이다. 이제, $(k-1)n+p=t$ 이라고 놓자. 그러면 치환 σ의 정의에 의하여, $\sigma^{-1}(\vec{u})$ $\sigma^{-1}(\vec{v})$는 적어도 t번째 성분이 다르다. 함수 f가 완비함수이므로 $\{(k-1)n+1,\cdots,\ kn\}$ 에서 임의의 i_k에 대하여

$$G_t(\vec{x}) = f_p(\overrightarrow{x_k}) \neq f_p(\overrightarrow{y_k}) = G_t(\vec{y})$$

인 i_k번째 성분만 다른 벡터 $\vec{x}=(\overrightarrow{x_1},\cdots,\ \overrightarrow{x_n})$와 $\vec{y}=(\overrightarrow{y_1},\cdots,\ \overrightarrow{y_n})$가 존재한다. 따라서 $\vec{u}=(\sigma \circ G)(\vec{x})$이고 $\vec{v}=(\sigma \circ G)(\vec{y})$이므로 임의의 $i,\ j \in S_{n^2}$ 에 대하여

$$F_j(\vec{x})=(G \circ \sigma \circ G)_j(\vec{x})=G_j(\vec{u})$$
$$\neq G_j(\vec{v})=(G \circ \sigma \circ G)_j(\vec{y})=F_j(\vec{y})$$

인 i번째 성분만 다른 벡터 $\vec{x}$와 $\vec{y}$가 존재한다. 따라서, 함수 F는 완비함수이다.

보조정리 2.8 함수 f: $V_n \to V_n$와 F:$V_{n^k} \to V_{n^k}$가 완비함수이라면 함수 f와 F로 부터 완비함수 F*: $V_{n^{k+1}} \to V_{n^{k+1}}$ 를 유도할 수 있다.

증명 $S_{n^{k+1}}$ 위에서의 치환 τ 를

$\tau(s)=(q-1)n+p$(단, $s=(p-1)n^k+q$, $1 \le p \le n$ 이고 $1 \le q \le n^k$)

로 정의하고 함수 f와 F의 함수 값을

$f(\overrightarrow{u_p})=(f_1(\overrightarrow{u_p}),\cdots,\ f_n(\overrightarrow{u_p}))$이고

$F(\overrightarrow{x_p})=(F_1(\overrightarrow{x_p}),\ \cdots,\ F_{n^k}(\overrightarrow{x_p}))$

(단, 임의의 $1 \le p \le n$ 와 $1 \le q \le n^k$에 대하여 $\overrightarrow{u_q}=(u_{(q-1)n+1},\cdots,u_{qn})$이고 $\overrightarrow{x_p}=(x_{(p-1)n^k+1},\cdots,\ x_{pn^k})$)

으로 놓자. 함수 G:$V_{n^{k+1}} \to V_{n^{k+1}}$는 임의의 $\vec{x}=(\overrightarrow{x_1},\overrightarrow{x_2},\cdots,\overrightarrow{x_n})$에 대하여

$$G(\vec{x})=(G_1(\vec{x}),\ G_2(\vec{x}),\ \cdots,\ G_{n^{k+1}}(\vec{x}))$$

(임의의 $1 \le p \le n$ 와 $1 \le q \le n^k$ 에 대하여 $G_{(p-1)n^k+q}(\vec{x})=F_q(\overrightarrow{x_p})$)

으로 정의하고, 함수 G^*:$V_{n^{k+1}} \to V_{n^{k+1}}$는 임의의 $\vec{u}=(\overrightarrow{u_1},\overrightarrow{u_2},\cdots,\overrightarrow{u_{n^k}})$에 대하여

$$G^*(\vec{u})=(G^*_1(\vec{u}),\ G^*_2(\vec{u}),\cdots,G^*_{n^{k+1}}(\vec{u}))$$

(임의의 $1 \le p \le n$와 $1 \le q \le n^k$에 대하여 $G^*_{(q-1)n^k+p}(\vec{u})=f_p(\overrightarrow{u_q})$)으로 정의한다. 이제, 함수 F^*:$V_{n^{k+1}} \to V_{n^k}$ 을 임의의 $\vec{u} \in V_{n^{k+1}}$에 대하여

$$F^*(\vec{x})=(G^* \circ \tau \circ G)(\vec{x})$$

정의하고 함수 F^*가 완비함수임을 보이자. 함수 f와 F 그리고 치환 τ가 일대일대응 함수이므로 함수 F^* 또한 일대일대응 함수이다. $S_{n^{k+1}}$의 임의의 값 $j=(q-1)n+p$ (임의의 $1 \le p \le n$와 $1 \le q \le n^k$)에 대하여, 함수 f가 완비함수이므로 $\{(q-1)n+1, (q-1)n+2, \cdots, qn\}$ 에서 임의의 i_q에 대하여 $\overrightarrow{u_q}$와 $\overrightarrow{v_q}$가 i_q 번째 성분만 다르면서

$$G^*_j(\overrightarrow{u})=f_p(\overrightarrow{u_q}) \neq f_p(\overrightarrow{v_q})=G^*_j(\overrightarrow{v})$$

인 두 개의 벡터 $\overrightarrow{u}=(\overrightarrow{u_1}, \cdots, \overrightarrow{u_{n^k}})$와 $\overrightarrow{v}=(\overrightarrow{v_1}, \cdots, \overrightarrow{v_{n^k}})$가 존재한다.
$i_q=(q-1)n+r$ 이라 하면$(1 \le r \le n)$, $\tau^{-1}(i_q)=(r-1)n^k+q$ 이다. $(r-1)n^k+q=t$이라 놓으면 치환 τ의 정의에 의하여, $\tau^{-1}(\overrightarrow{u})$ 와 $\tau^{-1}(\overrightarrow{v})$ 는 V_{n^k}에서 적어도 t번째 성분만 다른 벡터이다. 함수 F가 완비함수이므로 $\{(r-1)n^k+1, (r-1)n^k+2, \cdots, rn^k\}$에서 임의의 i_r에 대하여 $\overrightarrow{x_r}$와 $\overrightarrow{y_r}$는 i_r번째 성분만 다르면서

$$G_t(\overrightarrow{x})=F_q(\overrightarrow{x_r}) \neq F_q(\overrightarrow{y_r})=G_t(\overrightarrow{y})$$

인 $\overrightarrow{x}=(\overrightarrow{x_1}, \cdots, \overrightarrow{x_n}$와 $\overrightarrow{y}=(\overrightarrow{y_1}, \cdots, \overrightarrow{y_n})$가 존재한다. 따라서 $\overrightarrow{u}=(\tau \circ G)(\overrightarrow{x})$이고 $\overrightarrow{v}=(\tau \circ G)(\overrightarrow{y})$이므로 임의의 $i, j \in S_{n^{k+1}}$에 대하여

$$\begin{aligned} F^*_j(\overrightarrow{x}) &= (G^* \circ \tau \circ G)_j(\overrightarrow{x}) = G^*_j(\overrightarrow{u}) \\ &\neq G^*_j(\overrightarrow{v}) = (G^* \circ \tau \circ G)_j(\overrightarrow{y}) \\ &= F^*_j(\overrightarrow{y}) \end{aligned}$$

인 i번째 성분만 다른 벡터 $\overrightarrow{x}$와 $\overrightarrow{y}$가 존재한다. 따라서, 함수 F는 완비함수이다.

정리 2.9 함수 $f:V_n \to V_n$ 가 완비함수이라면, 함수 f 는 완비함수 $F:V_{n^k} \to V_{n^k}$를 유도할 수 있다.

증명 보조정리 2.7로 부터 함수 $f:V_n \to V_n$는 V_{n^2}에서의 완비함수를 유도할 수 있다. 함수 $f:V_n \to V_n$가 V_{n^k}에서 완비함수를 유도할 수 있다고 가정하자. 그러면 보조정리 2.8에 의하여 함수 f는 $V_{n^{k+1}}$에서의 완비함수를 유도할 수 있다. 따라서 수학적 귀납법에 의하여 정리 2.9가 성립한다.

3. 완비함수의 성질

이 절에서는 완비함수의 성질에 관하여 살펴 본다.

성질 3.1 완비함수는 아핀이 아니다. 즉, 아핀함수는 완비함수가 될 수 없다.

증명 함수 f가 아핀함수라 하면

$$f(\overrightarrow{x}) = \overrightarrow{x}M \oplus \overrightarrow{h}$$

을 만족하는 벡터 $\overrightarrow{h} \in V_n$와 $n \times n$ 행렬 M이 존재한다. 한편, 함수 f가 완비함수이므로, 임의의 $i, j \in S_n$ 에 대하여 $f_j(\overrightarrow{x}) \neq f_j(\overrightarrow{y})$인 i 번째 성분만 다른 벡터 $\overrightarrow{x}$ 와 $\overrightarrow{y}$가 V_n에 존재한다. 실제로 $\overrightarrow{x}=\overrightarrow{y} \oplus \overrightarrow{e_i}$ 이므로 $f(\overrightarrow{x})=\overrightarrow{y}M \oplus \overrightarrow{e_i}M \oplus \overrightarrow{h}$이고 $f(\overrightarrow{y})=\overrightarrow{y}M \oplus \overrightarrow{h}$ 이다. $f_j(\overrightarrow{x}) \neq f_j(\overrightarrow{y})$이므로 $\overrightarrow{e_i}M$의 j번째 성분은 $f_j(\overrightarrow{x})-f_j(\overrightarrow{y})=1$이다. j는 임의로 선택되었으므로 $\overrightarrow{e_i}M=(1, \cdots, 1)$이다. 이와 같은 방법으로, i도 임의의 값이므로 $i \neq j$에 대하여 $\overrightarrow{e_j}M=(1, \cdots, 1)$이다. 따라서 $f(\overrightarrow{e_i})=f(\overrightarrow{e_j})$이므로 함수 f가 일대일대응 함수가 아니다. 따라서 함수 f는 아핀이 아니다.

V_n의 성분들의 치환은 선형이다. 따라서 성질 3.1에 의하여 V_n의 성분들의 임의의 치환은 완비함수가 아니다. 그러나, 함수 $f:V_n \to V_n$ 가 완비함수이고 $\overrightarrow{h}$는 V_n의 임의의 벡터일 때 새로운 함수 $f(\overrightarrow{x}) \oplus \overrightarrow{h}$는 완비함수이다.

성질 3.1로부터 완비함수는 선형일 수 없지

만 다음 정리에 의하면, 선형구조를 가질 수 있다.

정리 3.2 임의의 $n \geq 3$에 대하여, E_k는 비선형함수로 $\vec{1} = (1, \cdots, 1)$에서 선형구조를 가진다. 즉, 임의의 벡터 $\vec{x} \in V_n$에 대하여 $E_k(\vec{x} \oplus \vec{1}) \oplus E_k(\vec{x})$은 상수이다.

증명 정리 2.4에 의하여 E_k는 완비함수이고 성질 3.1로부터 E_k는 선형이 아니다.

한편, 임의의 벡터 $\vec{x} \in V_n$에 대하여 $E_k(\vec{x} \oplus \vec{1}) \oplus E_k(\vec{x})$이 상수임을 보이면 된다.

(i) $\vec{x} = \vec{e_k}$ 또는 $\vec{x} = \overline{\vec{e_k}}$:

$$E_k(\vec{x} \oplus \vec{1}) \oplus E_k(\vec{x}) = E_k(\vec{e_k} \oplus \vec{1}) \oplus E_k(\vec{e_k})$$
$$= E_k(\overline{\vec{e_k}}) \oplus E_k(\vec{e_k})$$
$$= \vec{e_k} \oplus \overline{\vec{e_k}}$$
$$= \vec{1}$$

(ii) $\vec{x} \neq \vec{e_k}$이고 $\vec{x} \neq \overline{\vec{e_k}}$: $\vec{x} \oplus \vec{1} \neq \vec{e_k}$이고 $\vec{x} \oplus \vec{1} \neq \overline{\vec{e_k}}$이므로

$$E_k(\vec{x} \oplus \vec{1}) \oplus E_k(\vec{x}) = \vec{x_k} \oplus \vec{1} \oplus \vec{x_k} = \vec{1}$$

따라서 E_k는 $\vec{1} = (1, 1, \cdots, 1)$에서 선형구조를 가진다.

한편, 다음과 같이 정의된 함수

$f: V_3 \to V_3$, $f(\vec{x}) = (f_1(\vec{x}), f_2(\vec{x}), f_3(\vec{x}))$

$f_1(\vec{x}) = x_2 \oplus x_1x_3$, $f_2(\vec{x}) = x_2 \oplus x_3 \oplus x_1x_3$,

$f_3(\vec{x}) = x_1 \oplus x_2 \oplus x_2x_3$

는 완비함수이다. 그러나 f의 역함수 f^{-1}는

$f^{-1}(\vec{x}) = (f^{-1}_1(\vec{x}), f^{-1}_2(\vec{x}), f^{-1}_3(\vec{x}))$

$f^{-1}_1(\vec{x}) = x_3 \oplus x_1x_2$, $f^{-1}_2(\vec{x}) = x_1 \oplus x_1x_3 \oplus x_2x_3$,

$f^{-1}_1(\vec{x}) = x_1 \oplus x_2$

는 표-1 로 부터 완비함수가 아니다. 따라서 일반적으로 완비함수의 역함수는 완비함수가 아니다.

〈표 1〉 완비함수의 역함수가 완비함수가 아닌 예

$\vec{x}$	$f(\vec{x})$	$f^{-1}(\vec{x})$	$(f \circ f^{-1})(\vec{x})$
0 0 0	0 0 0	0 0 0	0 0 0
0 0 1	0 1 0	1 0 0	0 0 1
0 1 0	1 1 1	0 0 1	0 1 0
0 1 1	1 0 0	1 1 1	0 1 1
1 0 0	0 0 1	0 1 1	1 0 0
1 0 1	1 0 1	1 0 1	1 0 1
1 1 0	1 1 0	1 1 0	1 1 0
1 1 1	0 1 1	0 1 0	1 1 1

한편, 항등함수가 완비함수가 아니므로 완비함수들의 합성함수가 완비함수가 아님은 쉽게 알 수 있다. 즉, $E_k \circ E_k = 1_{V_n}$ 은 완비함수가 아니다. 그러나, 정리3.3과 정리3.4가 성립한다.

정리 3.3 임의의 $n \geq 4$에 대하여, $E_j \circ E_k$가 완비함수일 필요충분조건은 $j \neq k$ 이다.

증명 ($\Rightarrow$) $j=k$이라고 가정하자. 그러면 $E_j \circ E_k = 1_{V_n}$으로 완비함수가 아니다. 따라서 $E_j \circ E_k$가 완비함수라는 가정에 위배되므로 이것은 모순이다. 그러므로 $j \neq k$ 이다.

($\Leftarrow$) $j \neq k$ 이라고 가정하자. 그러면 함수 $E_j \circ E_k : V_n \rightarrow V_n$는 다음과 같다.

$$(E_j \circ E_k)(\vec{x}) = \begin{cases} \overline{\vec{x}} : \vec{x} \in \{\vec{e_j}, \vec{e_k}, \overline{\vec{e_j}}, \overline{\vec{e_k}}\} \\ \vec{x} : \vec{x} \notin \{\vec{e_j}, \vec{e_k}, \overline{\vec{e_j}}, \overline{\vec{e_k}}\} \end{cases}$$

이제, $E_j \circ E_k$가 완비함수임을 세 가지 경우로 나누어 증명한다.

(i) $i=j$: $(E_j \circ E_k)(\vec{e_i} \oplus \vec{e_k}) = \vec{e_i} \oplus \vec{e_k} \neq \overline{\vec{e_k}} = (E_j \circ E_k)(\vec{e_k})$이다. 따라서 모든 $h \neq j$에 대하여 $(E_j \circ E_k)_h(\vec{x}) \neq (E_j \circ E_k)_h(\vec{y})$인 i번째 성분만 다른 벡터 $\vec{x} = \vec{e_i} \oplus \vec{e_k}$ 와 $\vec{y} = \vec{e_k}$가 존재한다.

또한, $t \neq j$이고 $t \neq k$일 때 $(E_j \circ E_k)(\vec{e_i} \oplus \vec{e_t})\, \vec{e_i} \oplus \vec{e_t} \neq \vec{e_t} = (E_j \circ E_k)(\vec{e_t})$이다. 따라서 $(E_j \circ E_k)_j(\vec{x}) \neq (E_j \circ E_k)_j(\vec{y})$인 i번째 성분만 다른 벡터 $\vec{x} = \vec{e_i} \oplus \vec{e_t}$ 와 $\vec{y} = \vec{e_t}$가 존재한다.

(ii) $i=k$: (i)의 경우와 같이 증명된다.

(iii) $i \neq j$ 이고 $i \neq k$: $(E_j \circ E_k)(\vec{e_i} \oplus \vec{e_j}) = \vec{e_i} \oplus \vec{e_i} \neq \overline{\vec{e_j}} = (E_j \circ E_k)(\vec{e_j})$이다. 따라서 모든 $h \neq i$에 대하여 $(E_j \circ E_k)_h(\vec{x}) \neq (E_j \circ E_k)_h(\vec{y})$인 i번째 성분만 다른 벡터 $\vec{x} = \vec{e_i} \oplus \vec{e_j}$와 $\vec{y} = \vec{e_j}$가 존재한다. 또한, $(E_j \circ E_k)(\vec{e_i}) = \vec{e_i} \neq \vec{0} = (E_j \circ E_k)(\vec{0})$이다.

따라서 $(E_j \circ E_k)_i(\vec{x}) \neq (E_j \circ E_k)_i(\vec{y})$인 i번째 성분만 다른 벡터 $\vec{x} = \vec{e_i}$와 $\vec{y} = \vec{0}$가 존재한다. 그러므로 함수 $E_j \circ E_k$ 는 완비함수이다.

정리 3.3은 $n=3$일 때는 만족하지 않는다. 그것은 표-2 로 부터 알 수 있다

정리 3.4 n보다 작은 임의의 m에 대하여 함수 $E_1 \circ E_2 \circ \cdots \circ E_m$는 완비함수이다. 단, $n \geq 5$이다.

증명 $m=1$인 경우에는 명백하다. $m=k$일 때 함수 $E_1 \circ E_2 \circ \cdots \circ E_m$는 완비함수라고 가정하자. $m=k+1$일 때 즉, 함수 $E = E_1 \circ E_2 \circ \cdots \circ E_m = (E_1 \circ E_2 \circ \cdots \circ E_k) \circ E_{k+1}$이 완

〈표 2〉 :$n=3$인 경우 $E_i \circ E_j$의 함수값

$\vec{x}$	$(E_1 \circ E_2)(\vec{x})$	$(E_1 \circ E_3)(\vec{x})$	$(E_2 \circ E_3)(\vec{x})$
0 0 0	0 0 0	0 0 0	0 0 0
0 0 1	0 0 1	1 1 0	1 1 0
0 1 0	1 0 1	0 1 0	1 0 1
0 1 1	1 0 0	1 0 0	0 1 1
1 0 0	0 1 1	0 1 1	1 0 0
1 0 1	0 1 0	1 0 1	0 1 0
1 1 0	1 1 0	0 0 1	0 0 1
1 1 1	1 1 1	1 1 1	1 1 1

비함수인지를 살펴보자.

먼저 임의의 $j \in S_{k+1}$ 와 서로 다른 $i, j, k \in S_{k+1}$에 대하여

$$E(\vec{0}) = \vec{0} \neq \overline{\vec{e_j}} = \mathrm{E}(\vec{e_j}),$$

$$E(\vec{e_i} \oplus \vec{e_j} \oplus \vec{e_k}) = \vec{e_i} \oplus \vec{e_j} \oplus \vec{e_k} \neq \vec{e_i} \oplus \vec{e_k}$$

$$= \mathrm{E}(\vec{e_i} \oplus \vec{e_k})$$

이다. 임의의 $j \in S_{k+1}$와 $i \in S_n \backslash S_{k+1}$에 대하여

$$E(\vec{0}) = \vec{0} \neq \vec{e_i} = E(\vec{e_i}),$$

$$E(\vec{e_j}) = \overline{\vec{e_j}} \neq \vec{e_i} \oplus \vec{e_j} = E(\vec{e_i} \oplus \vec{e_j})$$

이다. 한편, 임의의 $i \in S_n \backslash S_{k+1}$에 대하여 $E(\vec{e_j}) = \vec{e_j} \neq \vec{e_i} \oplus \vec{e_j} = E(\vec{e_i} \oplus \vec{e_j})$이다. 따라서 함수 $E = (E_1 \circ E_2 \circ \cdots \circ E_k) \circ E_{k+1}$는 완비함수이다.

$m = n$인 경우에는 함수$\mathrm{E} = E_1 \circ E_2 \circ \cdots \circ E_n$는 임의의 $j \in S_n$에 대하여

$E(\vec{0}) = \vec{0} \neq \overline{\vec{e_j}} = \mathrm{E}(\vec{e_j})$이고 $E(\vec{e_i}) = \overline{\vec{e_i}} \neq \vec{e_i} \oplus \vec{e_j} = E(\vec{e_i} \oplus \vec{e_j})$이므로 완비함수이다.

4. 결 론

본 연구에서는[5]에서 보인 정리 2.6을 보다 엄밀하게 증명하였으며, 정리 2.4를 증명함으로서 완비함수의 존재성을 또다른 관점에서 보였으며 정리 3.4를 증명함으로서 이를 이용하여 보다 많은 완비함수를 찾을 수 있었다. 한편, 정리 2.6에 의하여 얻은 완비함수가 정리 2.4에서 얻은 E_k보다는 다소 복잡하지만, 이들은 단순한 완비함수들로 실제로 상관공격에 매우 약한 함수이다. 보다 복잡한 완비함수를 설계하기 위하여 작은 값의 n에 대하여 정리 2.4 와 정리 2.6 에 의하여 설계된 함수를 보조정리 2.7 과 정리 3.4를 적절히 이용함으로서 높은 차원에서 다소 복잡하게 만들 수 있었다. 그러나 이들에 관해서는 앞으로 더 많은 연구가 이루어져야 할 것이다. 또한 성질 3.1 과 정리 3.2를 증명함으로서 완비함수는 아핀함수가 될 수는 없지만 선형구조(linear structure)를 가짐을 보였다.

참고 문헌

[1] 김응태, 박승안, "선형대수학(제3판)경문사, 1991.

[2] C. Adams and S. Tavares, "The structured design of cryptogrphically good S-boxes", Journal of Cryptology, Vol. 3, No. 1, pp. 27-41, 1990

[3] J. Dtombe and S. Tavares, "Constructing Large Cryptographically Strong S-boxes" Advances in Cryptology:Proc. of CRYPTO' 92, pp. 165-181, Springer Verlag, 1993

[4] J. Gordon and H. Retkin, "Are big S-box best?", in Lecture Notes in Computer Science:Proc. of the Workshop on Cryptography, pp. 257-262, Springer-Verlag, 1982.

[5] John B. Kam and George I. Davida, "Structured design of substitution-permutation encryption networks", IEEE Tran. on Computers, Vol. C-28, pp. 747-753, 1979.

[6] W. Meier and O. Staffelbach, "Nonlinearity criteria for cryptographic functions", in Advances in Cryptology : Proc. of EUROCRYPT' 89, pp. 549-562, Springer-Verlag, 1990.

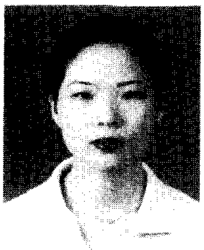
[7] C. Shannon, "Communication theory of secrecy systems", Bell Systems Technical Journal, Vol. 28, pp. 656-715, 1949.

□ 箸者紹介

이 민 섭(종신회원)

1976년 2월 서울대학교 사범대학 수학과 학사
1979년 2월 서강대학교 수학과 석사
1987년 5월 - University of Alabama 수학과 박사
1993년 Queensland University of Technology 방문교수(1년)
현재 : 단국대학교 수학과 교수 및 본학회 사업이사

※ 주관심분야 : 순서론, 암호이론



최 춘 수(학생회원)

1994년 2월 단국대학교 수학과 학사
1996년 2월 단국대학교 수학과 석사
1997년 9월 - 현재 : 단국대학교 수학과 박사과정

※ 주관심분야 : 암호이론