일반화 벤트 함수의 새로운 생성 방법

정회원 김 성 환*, 길 강 미*, 김 경 희*, 노 종 선*

New Construction of Generalized Bent Functions

Sunghwan Kim*, Gang-Mi Gil*, Kyung-Hee Kim*, and Jong-Seon No* ***Regular Members***

요 약

본 논문에서는 $n=2m$과 홀수 소수 p에 대해서 유한체 F_{p^n}에서 소체 F_p로의 새로운 일반화 벤트 함수를 F_{p^n}에서 정의된 partial spread를 이용하여 생성한다. 또한 제안된 일반화 벤트 함수와 그것의 트레이스 변환된 함수를 트레이스 함수를 이용하여 표현한다.

ABSTRACT

In this paper, for $n=2m$ and odd prime p, new generalized bent functions from the finite field F_{p^n} to the prime field F_p are constructed from the partial spreads for F_{p^n}. Closed form expressions for the proposed generalized bent functions and their trace transform are derived in the form of the trace functions.

Ⅰ. 서 론

1976년 로타우스가 n항 이진 벡터 공간에서 F_2로의 벤트(bent) 함수를 소개하면서 벤트 함수에 대한 연구가 있었다[4]. 이 벤트 함수의 정의는 다음과 같다. 어떤 부울(Boolean) 함수의 푸리에 계수값이 단지 +1 혹은 -1만의 값을 가질 때 그 부울 함수를 벤트 함수라고 한다. 이 벤트 함수는 좋은 푸리에 변환 성질을 갖고 있기 때문에 최적 상관 특성을 갖는 이진 시퀀스 군의 생성, 오류 정정 부호, 암호학 등과 같은 다양한 분야에서 사용할 수 있다.

일반적으로 벤트 함수를 분류하는 것은 쉽지 않다. 분류 중 잘 알려진 것으로 class M으로 불리는 Maiorana-McFarland 벤트 함수가 있다. Dillon은 제곱 차수를 갖는 군(Group)에 대한 partial spread를 이용한 기초 하다마드 차집합(elementary Hadamard difference set)을 제안하였다[2]. 이를 PS-와 PS+로 불리는데 이것의 특성 함수가 벤트 함수가 됨을 보였다. 다른 몇 개의 벤트 함수의 분류는 Carlet에 의해서 정의되었는데 class D, class C 등이 있다. Carlet는 모든 벤트 함수가 일반화 partial spread의 특성을 갖는다는 것을 증명하였다[6]. Kumar, Scholtz, Welch는 q항 벡터장에서 정수 q 잉여의 집합으로의 일반화 벤트 함수를 정의하였다[3]. 이때 이 함수들의 푸리에 계수 값은 모두 크기(magnitude)를 1로 갖는다. 그들은 몇 가지 일반화 벤트 함수를 발표하였다.

이 논문에서는 $n=2m$과 홀수 소수 p에 대해서 유한체 F_{p^n}에서 소체 F_p로의 새로운 일반화 벤트 함수를 F_{p^n}에서 정의된 partial spread를 이용하여 생성한다. 또한 제안된 일반화 벤트 함수와 그것의 트레이스 변환된 함수를 트레이스 함수를 이용하여 표현한다.

Ⅱ. 사 전 지 식

q를 정수, J_q를 q잉여 집합, V_q^n은 정수 q잉여 집합상의 n차원 벡터 공간, $\omega=e^{j\frac{2\pi}{q}}$, $j=\sqrt{-1}$이라

* 서울대학교 전기컴퓨터공학부 부호및암호연구실 (jsno@snu.ac.kr),
논문번호 : 010384-1210, 접수일자 : 2001년 12월 10일
※ 본 연구는 BK21과 정보통신부 지정 ITRC 프로그램의 지원으로 수행되었습니다.

고 하자. $f(x)$는 V_q^n에서 J_q로의 함수라고 하자. 이 때 함수 $f(x)$의 푸리에 변환은 다음과 같이 정의된다.

$$F(\lambda)=\frac{1}{\sqrt{q^n}}\sum_{x\in V_q^n}\omega^{f(x)-\lambda\cdot x^T},\quad \text{all}\ \ \lambda\in V_q^n \tag{1}$$

여기서 x^T는 x의 전치를 나타낸다. 이때 일반화 벤트 함수는 다음과 같이 정의된다.

정의 1[Olsen, Scholtz, Kumar[3]]: V_q^n으로부터, J_q로의 함수 $f(x)$는 그것의 푸리에 계수 $F(\lambda)$값이 모든 $\lambda\in V_q^n$에 대해서 크기 1의 값만 갖게 될 때 일반화 벤트 함수라고 한다.

□

일반화 벤트 함수는 그것의 푸리에 계수 값이 다음 식과 같이 ω의 정수 지수 형태가 되면 정규 벤트 함수라고 부른다.

$$F(\lambda)=\omega^{f(\lambda)},\quad \text{all}\ \ \lambda\in V_q^n \tag{2}$$

여기서 $f(\lambda)\in J_q$이다. 정규 벤트 함수 $f(x)$에 대해서 그것의 푸리에 변환 $f(\lambda)$는 또한 V_q^n에서 J_q로의 일반화 벤트 함수이다.

이 논문에서는 정수 q는 홀수 소수 p만을 고려하고 있다. 따라서 V_q^n은 p개의 원소를 갖는 유한체 F_p상에서의 n차원 벡터장이고 $f(x)$는 V_p^n에서 F_p로의 함수이다.

F_{p^m}을 p^m개 원소를 갖는 유한체라고 하자. 어떤 양의 정수 e와 m에 대해서 $n=em>1$라고 하자. 그러면 F_{p^n}에서 F_{p^m}으로의 트레이스 함수는 다음과 같이 정의된다.

$$tr_m^n(x)=\sum_{i=0}^{e-1}x^{p^{mi}}$$

여기서 x는 F_{p^n}상의 원소이다.

정의된 트레이스 함수는 다음의 성질을 만족시킨다.

(i) $tr_m^n(ax+by)=atr_m^n(x)+btr_m^n(y)$

(ii) $tr_m^n(x^{p^m})=tr_m^n(x)$

(iii) $tr_1^n(x^{p^m})=tr_1^m(tr_m^n(x))$

단, $a,b\in F_{p^m}$, $x,y\in F_{p^n}$이다.

Olsen, Scholtz, Welch[3]는 F_{p^n}에서 F_{p^m}로의 함수에 대한 트레이스 변환을 정의하였다. F_{p^n}에서 F_{p^m}로의 함수에 대한 트레이스 함수는 다음과 같이 일반화될 수 있다.

정의 2: $f(x)$를 F_{p^n}에서 F_{p^m}로의 함수라고 하자. 그러면 $f(x)$의 트레이스 변환과 그것의 역변환은 다음 식과 같이 정의된다.

$$F(\lambda)=\frac{1}{\sqrt{p^n}}\sum_{x\in F_{p^n}}\omega^{f(x)-tr_1^n(x\cdot\lambda)} \tag{3}$$
$$\omega^{f(x)}=\frac{1}{\sqrt{p^n}}\sum_{\lambda\in F_{p^n}}F(\lambda)\cdot\omega^{tr_1^n(x\cdot\lambda)}$$

여기서 $x,\ \lambda\in F_{p^n}$.

□

F_{p^n}의 원소 x와 λ는 V_p^n상에의 원소 $\underline{x}$와 $\underline{\lambda}$와 다음과 같은 관계식을 만족할 수 있다.

$$x=\sum_{i=1}^{n}x_i\cdot\alpha_i\ \Rightarrow\ \underline{x}=(x_1,x_2,\cdots,x_n)$$
$$\lambda=\sum_{i=1}^{n}\lambda_i\cdot\alpha_i\ \Rightarrow\ \underline{\lambda}=(\lambda_1,\lambda_2,\cdots,\lambda_n)$$

여기서 x_i와 λ_i는 F_p상의 원소이고 $\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$는 F_p상에서 F_{p^n}의 기저라고 하자.

F_{p^n}상에서 x를 V_p^n상의 $\underline{x}$로 대체함으로써 F_{p^n}에서 F_p로의 함수 $f(x)$는 V_p^n에서 F_p로의 함수 $f(\underline{x})$와 대응관계가 있다.

다음의 관계를 갖는 F_{p^n}상의 트레이스 직교기저(trace-orthogonal basis)인 $\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$를 정의한다.

$$tr_1^n(\alpha_i\cdot\alpha_j)=\begin{cases}a_i, & \text{if } i=j\\ 0, & \text{otherwise}\end{cases} \tag{4}$$

여기서 $a_i\in F_p^*$이다. 모든 양의 정수 n과 홀수 소수 p에 대해서 F_p상에 F_{p^n}의 트레이스 직교기저가 존재함은 널리 알려져 있다[5].

직교기저를 기저로 선택하면 다음과 같은 관계식을 가질 수 있다.

$$tr_1^n(\lambda\cdot x)=\sum_{i=1}^{n}a_i\cdot\lambda_i\cdot x_i \tag{5}$$

$1\le i\le n$인 i와 $\underline{\lambda}'=(\lambda_1',\lambda_2',\cdots\lambda_n')$에 대해서 $\lambda_i'=a_i\cdot\lambda_i$라고 하자. 그러면 위에서 정의된 관계식은 다음과 같이 쓸 수 있다.

$$tr_1^n(\lambda\cdot x)=\sum_{i=1}^{n}\lambda_i'\cdot x_i=\underline{\lambda}'\cdot\underline{x}^T \tag{6}$$

V_p^n에서 F_p로의 함수 $f(x)$의 푸리에 변환은 F_{p^n}에서 F_p로의 상응하는 함수 $f(x)$의 트레이스 변환과의 관계는 다음과 같이 주어진다.

$$F(\lambda)=F(\lambda')$$

즉 함수 $f(x)$의 트레이스 변환 값의 집합은 상응하는 함수 $f(x)$의 푸리에 계수의 집합과 같다는 것을 말한다. 따라서 함수 $f(x)$의 트레이스 변환값이 단지 크기 1인 값을 갖는다고 하면, 상응하는 함수 $f(x)$는 일반화 벤트 함수가 된다. 이제 F_{p^n}상에 정의된 함수 $f(x)$는 그것의 트레이스 변환이 단지 크기 1을 갖는다고 한다면 벤트 함수로 정의된다.

G는 지곱 차수 M^2을 갖는 군이라고 하자. 그리고 H_i 차수 M인 군 G의 부분집합이라고 하자. Dillon은 부분군 $H_1, H_2, \cdots, H_N$의 집합이 서로 pairwise disjoint 즉 $i\neq j$에 대해 다음 식을 만족하면 partial spread라고 정의하였다.

$$H_i \cap H_j = \{0\}$$

만약 $N=M+1$이라면 이를 spread라고 한다. 군 G에 대한 partial spread를 이용하여, Dillon은 PS-와 PS+로 불리는 기초 하다마드 차집합을 생성하였다. $M=2N$이라고 하면 PS-는 변수 $(v,k,\lambda)=(4N^2, 2N^2-N, N^2-N)$을 갖는 기초 하다마드 차집합이 되고 다음과 같이 정의된다.

$$D_- = \bigcup_{i=1}^{N} H_i^*$$

여기서 $H_i^* = H_i \setminus \{0\}$이다. PS+는 변수 $(v,k,\lambda)=(4N^2, 2N^2+N, N^2+N)$를 갖는 기초 하다마드 차집합이고 다음과 같이 정의된다.

$$D_+ = \bigcup_{i=1}^{N+1} H_i$$

그는 또한 partial spread가 짝수차 이진 벡터장 V_2^{2m}에 대해서 정의된다면, 그 기초 하다마드 차집합 D_-와 D_+의 특성 함수는 짝수차 이진 벡터장 V_2^{2m}에 대해서 벤트 함수가 된다.

Ⅲ. 일반화 벤트 함수의 생성방법

$n=2m$이고 F_{p^n}은 원소가 p^n개의 원소를 갖는 유한체라고 하자. $T=p^m+1$이고 α는 F_{p^n}의 원시원이라고 하자. 그러면 α^T는 F_{p^m}상의 원시원이 된다. H_i는 F_{p^n}의 차수 p^m인 가법군(additive group)이라고 하고 다음과 같이 정의된다고 하자.

$$H_i = \{\eta\alpha^i \mid \eta \in F_{p^m}\}, \quad 0 \le i \le T-1 \tag{7}$$

또한 다음을 정의할 수 있다.

$$H_i^* = H_i \setminus \{0\}, \quad 0 \le i \le T-1$$

모든 $i\neq j$와 $0\le i,j\le T-1$에 대해서 다음 식이 성립한다.

$$H_i \cap H_j = \{0\}$$

그리고

$$F_{p^n} = \bigcup_{i=0}^{T-1} H_i$$

그러면 다음과 같이 주어지는 부분군의 집합은 F_{p^n}의 spread를 만든다.

$$H_0, H_1, H_2, \cdots, H_{T-1}$$

T_s를 정수 T 잉여 집합 즉 $\{0,1,2\cdots T-1\}$이고 I_k는 어떤 서로소인 부분집합이면서 다음을 만족한다.

$$I_k \subset T_s, \quad 0 \le k \le p-1 \tag{8}$$

그리고 I_k의 크기는 $1\le k\le p-1$인 k에 대해서 $|I_0| = p^{m-1}+1$이고 $|I_k| = p^{m-1}$을 만족한다.

그러면 모든 $0\le k,l\le p-1$인 $k\neq l$에 대해서

$$I_k \cup I_l = \phi$$

$$\bigcup_{k=0}^{p-1} I_k = T_s$$

또한 정수 집합 T_s의 부분집합 $\overline{I_k}$를 다음과 같이 정의한다.

$$\overline{I_k} = \left\{ \frac{T}{2} - i_k \bmod T \mid i_k \in I_k \right\}, \quad 0 \le k \le p-1 \tag{9}$$

그러면 모든 $0\le k,l\le p-1$인 $k\neq l$에 대해서

$$\overline{I_k} \cup \overline{I_l} = \phi$$

$$\bigcup_{k=0}^{p-1} \overline{I_k} = T_s$$

F_{p^n}에 대한 partial spread를 사용하여, F_{p^n}의 부분집합 D_k는 다음과 같이 만들 수 있다.

$$D_0 = \bigcup_{i \in I_0} H_i$$

$$D_k = \bigcup_{i_k \in I_k} H_{i_k}^*, \quad 1 \le k \le p-1 \tag{10}$$

모든 $k\neq l$, $0\le k,l\le p-1$에 대해서 다음이 성립함은

자명하다.

$$D_k \cap D_l = \phi$$

$$F_{p^n} = \bigcup_{k=0}^{p-1} D_k$$

위에서 정의된 부분집합 D_k로부터 다음 정리와 같이 일반화 벤트 함수를 생성할 수 있다.

정의 3: $n=2m$이고, D_k는 F_{p^n}상에서 위의 식과 같이 정의된다고 하자. 홀수 소수 p에 대해서 F_{p^n}에서 F_p로의 다음 식과 같이 정의되는 함수 $f(x)$는 정규 벤트 함수이다.

$$f(x) = \begin{cases} 0, & \text{if } x \in D_0 \\ k, & \text{if } x \in D_k, \quad 1 \le k \le p-1 \end{cases} \tag{11}$$

증명: $f(x)$의 트레이스 변환이 크기 1을 갖는다는 것을 보이는 것으로 이 증명은 충분하게 된다. $f(x)$의 트레이스 변환은 다음과 같이 주어진다.

$$\begin{aligned} F(\lambda) &= \frac{1}{\sqrt{p^n}} \sum \omega^{f(x) - tr_1^n(\lambda \cdot x)} \\ &= \frac{1}{\sqrt{p^n}} \Big[\sum_{x \in D_0} \omega^{-tr_1^n(\lambda \cdot x)} + \omega \sum_{x \in D_1} \omega^{-tr_1^n(\lambda \cdot x)} \\ &\qquad + \cdots + \omega^{p-1} \sum_{x \in D_{p-1}} \omega^{-tr_1^n(\lambda \cdot x)} \Big] \end{aligned}$$

$\lambda = 0$에 대해서, $F(\lambda) = 1$은 자명하다. 이제 $\lambda \neq 0$에 대해서 증명을 한다. α는 F_{p^n}상의 원시원이라고 하자. $x = \delta \cdot \alpha^i$, $\delta \in F_{p^m}^*$, $i \in T_s$라고 하자. 그러면 트레이스 변환은 다음과 같이 쓸 수 있다.

$$\begin{aligned} F(\lambda) = \frac{1}{\sqrt{p^n}} \Big[& 1 + \sum_{i \in I_0} \sum_{\delta \in F_{p^m}} \omega^{-tr_1^m(\delta \cdot tr_m^n(\alpha^i \cdot \lambda))} \\ & + \omega \sum_{i \in I_1} \sum_{\delta \in F_{p^m}} \omega^{-tr_1^m(\delta \cdot tr_m^n(\alpha^i \cdot \lambda))} \\ & + \cdots \\ & + \omega^{p-1} \sum_{i \in I_1} \sum_{\delta \in F_{p^m}} \omega^{-tr_1^m(\delta \cdot tr_m^n(\alpha^i \cdot \lambda))} \Big] \end{aligned} \tag{12}$$

$(k+1)$번째 합의 내부 합은 다음과 같이 주어진다.

$$\begin{aligned} & \sum_{\delta \in F_{p^m}} \omega^{-tr_1^m(\delta \cdot tr_m^n(\alpha^i \cdot \lambda))} \\ & = \begin{cases} p^m - 1, & \text{if } tr_m^n(\alpha^i \cdot \lambda) = 0 \\ -1, & \text{otherwise} \end{cases} \end{aligned} \tag{13}$$

따라서 $tr_m^n(\alpha^i \cdot \lambda) = 0$인 경우를 살펴보면, 홀수 소수 p에 대해서 다음과 같은 관계식을 살펴 볼 수 있다.

$$\begin{aligned} tr_m^n\left(\alpha^{\frac{T}{2}}\right) &= \alpha^{\frac{p^m+1}{2}} + \alpha^{p^m \cdot \frac{p^m+1}{2}} \\ &= \alpha^{\frac{p^m+1}{2}} + \alpha^{\frac{p^{2m}+p^m}{2}} \\ &= \alpha^{\frac{p^m+1}{2}} + \alpha^{\frac{p^{2m}-1}{2}} \cdot \alpha^{\frac{p^m+1}{2}} \\ &= 0 \end{aligned}$$

그리고 모든 정수 i에 대해서

$$tr_m^n\left(\alpha^{\frac{T}{2}+iT}\right) = \alpha^{iT} \cdot tr_m^n\left(\alpha^{\frac{T}{2}}\right)$$

$tr_m^n(\alpha^t)$의 균형성질로부터 t가 $0 \le t \le p^n - 2$ 상에서 변함에 따라 $tr_m^n(\alpha^t) = 0$은 $p^m - 1$번 발생하게 된다. 따라서 t가 $0 \le t \le T-1$상에서 변함에 따라 $t = \frac{T}{2}$일 때 $tr_m^n(\alpha^t) = 0$은 한번 발생한다.

$\lambda = \varepsilon \cdot \alpha^j$, $\varepsilon \in F_{p^m}^*$, $j \in T_s$라고 하자. 그러면,

$$tr_m^n(\alpha^i \cdot \lambda) = \delta\varepsilon \cdot tr_m^n(\alpha^{i+j}) = \begin{cases} 0, & j \in \overline{I_k} \\ \neq 0, & \text{otherwise} \end{cases} \tag{14}$$

식 (13)과 (14)을 사용하여 식 (12)의 이중합은 다음과 같이 쓸 수 있다.

$$\begin{aligned} & \sum_{i \in I_k} \sum_{\delta \in F_{p^m}} \omega^{-tr_1^m(\delta \cdot tr_m^n(\alpha^i \cdot \lambda))} \\ & = \begin{cases} -|I_k|, & \text{if } j \notin \overline{I_k} \\ p^m - |I_k|, & \text{if } j \in \overline{I_k} \end{cases} \end{aligned} \tag{15}$$

주어진 0이 아닌 λ에 대해서 j는 단지 하나의 부분집합 $\overline{I_k}$에 속한다. 만약 $j \in \overline{I_0}$라면, $f(x)$의 트레이스 변환은 다음과 같이 계산된다.

$$\begin{aligned} F(\lambda) = \frac{1}{\sqrt{p^n}} (1 + p^m - p^{m-1} - 1 - p^{m-1}\omega \\ - p^{m-1}\omega^2 - \cdots - p^{m-1}\omega^{p-1}) \end{aligned} = 1 \tag{16}$$

만약 $j \in \overline{I_k}$, $1 \le k \le p-1$이라면, $f(x)$의 트레이스 함수는 다음과 같다.

$$\begin{aligned} F(\lambda) = \frac{1}{\sqrt{p^n}} (& 1 - p^{m-1} - 1 - p^{m-1}\omega - p^{m-1}\omega^2 \\ & - \cdots p^{m-1}\omega^{k-1} + p^m\omega^k - p^{m-1}\omega^k - p^{m-1} \\ & \omega^{k+1} - \cdots p^{m-1}\omega^{p-1}) \\ = \omega^k \end{aligned} \tag{17}$$

따라서 모든 $\lambda \in F_{p^n}$에 대해서 $F(\lambda)$는 omega의 정수 지수 형태이다. 따라서 $f(x)$는 정규 벤트 함수이다.

□

식 (10)에서 정의된 부분집합 D_k로부터 $0 \le k \le p-1$에서 F_{p^n}의 부분집합인 $\overline{D_k}$를 다음과 같이 정의 할 수 있다.

$$\overline{D_0} = \bigcup_{k_0 \in \overline{I_0}} H_{i_0}$$

$$\overline{D_k} = \bigcup_{i_k \in I_k} H^*_{i_k}, \quad 1 \le k \le p-1$$

식 (16)과 (17)으로부터 식 (11)에서 정의된 일반화 벤트 함수의 푸리에 변환 $\hat{f}(\lambda)$은 다음과 같은 정리로 유도될 수 있다.

정리 4: $n=2m$과 홀수 소수 p에 대해서 식 (11)에서 정의된 일반화 벤트 함수의 푸리에 변환 $\hat{f}(\lambda)$는 다음과 같은 값으로 주어진다..

$$\hat{f}(\lambda) = \begin{cases} 0, & \text{if } \lambda \in \overline{D_0} \\ k, & \text{if } \lambda \in \overline{D_k}, \quad 1 \le k \le p-1 \end{cases} \tag{18}$$

□

F_{p^n}에서 F_{p^m}으로의 트레이스 함수가 다음과 같은 관계식을 갖는 것은 쉽게 유도할 수 있다.

$$[tr_m^n(x)]^{p^m-1} = \begin{cases} 0, & x \in H_{\frac{T}{2}} \\ 1, & \text{otherwise} \end{cases}$$

위 식을 이용하여 (7)에서 정의된 부분 군 H_i에 대한 특성함수를 다음과 같이 정의할 수 있다.

$$\phi_{H_i}(x) = \begin{cases} 1, & x \in H_i \\ 0, & \text{otherwise} \end{cases}$$

그러면 이 함수 $\phi_{H_i}(x)$는 다음과 같이 쓸 수 있다.

$$\phi_{H_i}(x) = 1 - \left[tr_m^n(x \cdot \alpha^{-i+\frac{T}{2}}) \right]^{p^m-1}, \quad 0 \le i \le T-1 \tag{19}$$

특성함수인 식 (19)을 이용하여서 식 (11)에서 정의된 일반화 벤트 함수와 그것의 푸리에 변환은 다음과 같이 주어진다.

$$f(x) = \sum_{k=0}^{p-1} \sum_{i_k \in I_k} k \cdot \left(1 - \left[tr_m^n\left(x \cdot \alpha^{-i_k+\frac{T}{2}}\right) \right]^{p^m-1} \right)$$

$$\hat{f}(\lambda) = \sum_{k=0}^{p-1} \sum_{i_k \in I_k} k \cdot \left(1 - \left[tr_m^n\left(\lambda \cdot \alpha^{-i_k+\frac{T}{2}}\right) \right]^{p^m-1} \right)$$

$k=0$일 때 합은 제거 될 수 있고 p임여에서 계산된다. 따라서 어떤 k, $1 \le k \le p-1$에 대해서 $|I_k| = |\overline{I_k}| = p^{m-1}$이므로 다음이 성립한다.

$$\sum_{i_k \in I_k} k = 0 \mod p,$$

$$\sum_{i_k \in \overline{I_k}} k = 0 \mod p$$

따라서 식 (11)에서 정의된 일반화 벤트 함수와 그것의 푸리에 변환은 다음 따름 정리와 같이 쓸 수 있다.

따름정리 5: 식 (11)에서 정의된 일반화 벤트 함수와 그것의 푸리에 변환 $\hat{f}(\lambda)$는 다음 식과 같이 주어진다.

$$f(x) = \sum_{k=0}^{p-1} \sum_{i_k \in I_k} (p-k) \cdot \left[tr_m^n(x \cdot \alpha^{-i_k+\frac{T}{2}}) \right]^{p^m-1} \tag{20}$$

$$\hat{f}(\lambda) = \sum_{k=0}^{p-1} \sum_{i_k \in I_k} (p-k) \cdot \left[tr_m^n\left(\lambda \cdot \alpha^{-i_k+\frac{T}{2}}\right) \right]^{p^m-1} \tag{21}$$

□

(4)에서 정의된 트레이스 직교기저를 이용하여 따름정리 5에서 정의된 일반화 벤트 함수 $f(x)$와 그것의 푸리에 변환인 식 (21)은 벡터장 V_p^n에서 정의되는 일반화 벤트 함수 $f(x)$로 변환될 수 있다.

참 고 문 헌

[1] C. Carlet, "Two new classes of bent functions," in *Proc. EURO-CRYPT'93 (Lecture Notes in Computer Science 765)*, pp. 77-101, 1994.

[2] J. F. Dillon, "Elementary Hadamard difference sets," Ph.D. dissertation, University of Maryland, 1974.

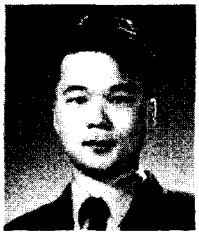
[3] P.V. Kumar, R.A. Scholts and L.R. Welch, "Generalized bent functions and their properties," *Journal of Combinatorial Theory*, Series A. vol. 40, pp. 90-107, 1985.

[4] O.S. Rothaus, "On bent functions," *Journal of Combinatorial Theory*, Series A. vol. 20, pp. 300-305, 1976.

[5] G. Seroussi and A. Lempel, "Factorization of symmetric matrics and trace-orthogonal bases in finite field," *SIAM J. Comput.*, vol. 9, no. 4, pp. 758-767, Nov. 1980.

[6] C. Carlet and P. Guillot, "A characterization of binary bent functions," *Journal of Combinatorial Theory*, Serial A. vol. 76, pp. 328-335, 1996.

김 성 환(Sunghwan Kim) 정회원



1999년 2월 : 서울대학교 전기공학부 공학석사
2001년 2월 : 서울대학교 대학원 전기공학부 공학석사
2001년 3월~현재 : 서울대학교 대학원 전기·컴퓨터 공학부 박사과정
<주관심 분야> 디지털통신, 오류정정부호, 시퀀스

길 강 미(Gang-Mi Gil) 정회원

2000년 2월 : 서울대학교 전기공학부 공학석사
2002년 2월 : 서울대학교 대학원 전기·컴퓨터 공학부 공학석사
2002년 3월~현재 : 삼성전자
<주관심 분야> 디지털통신, 오류정정부호, 시퀀스

김 경 희(Jong-Seon No) 정회원

1988년 2월 : 서울대학교 수리과학부 수학과 이학사
1990년 8월 : 서울대학교 대학원 수리과학부 수학과 이학석사
1998년 8월 : 서울대학교 대학원 수리과학부 수학과 이학박사
1998년 2월~2001년 2월 : 고등과학원 연구원
2001년 4월~2002년 3월 : 서울대학교 대학원 전기·컴퓨터공학부 박사 후 연구원

노 종 선(Jong-Seon No) 종신회원

1981년 2월 : 서울대학교 전자공학과 공학사
1984년 2월 : 서울대학교 대학원 전자공학과 공학석사
1988년 5월 : University of Southern California, 전기공학과 공학박사
1988년 2월~1990년 7월 : Hughes Network Systems, Senior MTS
1990년 9월~1999년 7월 : 건국대학교 전자공학과 부교수
1999년 8월~현재 : 서울대학교 전기·컴퓨터공학부 부교수
<주관심 분야> 시퀀스, 오류정정부호, 암호학, 이동통신