일반화된 이진 Bent 시퀀스

정회원 길 강 미*, 노 종 선*, 신 동 준**

Generalized Binary Bent Sequences

Gang-Mi Gil*, Jong-Seon No*, Dong-Joon Shin** *Regular Members*

요 약

본 논문에서 Olsen, Scholtz, Welch가 소개한 이진 bent 시퀀스군을 일반화시켜 최적의 상관 특성과 균형 특성을 갖는 일반화된 이진 bent 시퀀스를 생성하였다. 변형된 trace 변환이 정의되고 이로부터 F_{2^n}에서 중간체 F_{2^e}로의 선형함수를 사용하였다. 여기서 $e|n$이다. 만일 $e=1$이면 새로운 방법은 기존의 이진 bent 시퀀스의 경우와 같아진다. 또한 새로운 방법이 최적의 상관 특성과 균형 특성을 갖는 간단한 이진 시퀀스군을 생성시킨다는 것을 보여주는 몇 가지 예가 주어진다.

ABSTRACT

In this paper, we generalize the family of binary bent sequences introduced by Olsen, Scholtz and Welch [2] to obtain the generalized binary bent sequences with optimal correlation and balance properties. The modified trace transform is introduced and it enables us to use linear function from F_{2^n} to the intermediate field F_{2^e}, where $e|n$. If we choose $e=1$, our method becomes the conventional binary bent sequence case. Also, some examples are given which show that our construction gives the family of simple binary sequences with optimal correlation and balance properties.

Ⅰ. 서 론

우수한 자기상관, 상호상관 특성과 균형(balance) 특성을 갖는 이진 bent 시퀀스를 생성하기 위하여 bent 함수가 사용된 많은 연구결과들이 있다[1],[2],[3],[8]. 코드분할 다중접속 시스템, 레이더 시스템, 동기 시스템 등이 위상이 안 맞는 경우의 자기상관값과 상호상관값이 낮은 시퀀스를 요구하는데 이진 bent 시퀀스들이 이들 시스템에 사용될 수 있을 것이다.

Rothaus는 bent 함수를 F_2상의 n차원 벡터공간에서 F_2로의 함수로 정의하고 bent 함수를 몇 가지 중요한 클래스로 분류하였다[1]. Olsen, Scholtz, Welch는 bent 함수를 이용하여 이진 bent 시퀀스를 생성하였다. 이렇게 생성된 이진 bent 시퀀스는 위상이 안 맞는 경우의 상관값의 절대값이 시퀀스 길이의 제곱근보다 크지 않아서 Welch에 의해 제안된 하한 조건[9]을 근사적으로 만족시키며 좋은 상관 특성을 나타낸다[2]. 또한 bent 시퀀스를 생성시키는데 trace 변환을 사용했는데 이는 Rothaus에 의해 사용된 퓨리에 변환과 동일하다는 것을 보였다. Lempel과 Cohn은 Olsen, Scholtz, Welch의 결과를 확장시켜 Welch의 하한 조건을 만족시키는 상관값을 갖는 bent 시퀀스를 생성시키는 bent 함수의 필요충분조건을 얻었다[3].

본 논문에서는 Olsen, Scholtz, Welch이 생성한 이진 bent 시퀀스를 일반화시켜 최적의 상관 특성과 균형 특성을 갖는 일반화된 이진 bent 시퀀스를 얻는다. 변형된 trace 변환(modified trace transform)이 도입되고 이는 F_{2^n}에서 중간체 F_{2^e}로의 선형함

* 서울대학교 전기·컴퓨터공학부(jsno@snu.ac.kr), ** 한양대학교 전자전기컴퓨터공학부 (djshin@hanyang.ac.kr)
논문번호 : 010252-0917, 접수일자 : 2001년 9월 17일
※ 본 연구는 BK21과 ITRC 지원 및 관리로 수행되었습니다.

수를 가능케 한다. 여기서 d는 n이다. 만일 $e=1$이면 새로운 방법은 기존의 이진 bent 시퀀스의 경우와 같아진다. 또한 새로운 방법이 최적의 상관 특성과 균형 특성을 갖는 간단한 이진 시퀀스 군(class)를 생성시킨다는 것을 보여주는 몇 가지 예가 주어진다.

Ⅱ. 이진 Bent 시퀀스

주기가 N인 두 이진 시퀀스 $s_y(t)$와 $s_z(t)$의 상관함수 $R_{yz}(\tau)$는 다음과 같이 정의된다.

$$R_{yz}(\tau)=\sum_{t=0}^{N-1}(-1)^{s_y(t)+s_z(t+\tau)} \tag{1}$$

여기서 $t+\tau$는 mod N으로 계산된다. V_2^k를 유한체 F_2상의 k차원 벡터공간이라고 하면 bent 함수는 다음과 같이 정의된다.

정의 1[1][2]: V_2^k에서 F_2로의 함수 $f(\underline{x})$에 대해서 다음과 같이 정의되는 $(-1)^{f(\underline{x})}$의 모든 하다마드 변환 $\hat{f}(\underline{\lambda})$가 ±1의 값을 가지면 $f(\underline{x})$를 bent라고 한다.

$$\hat{f}(\underline{\lambda})=\frac{1}{\sqrt{2^k}}\sum_{\underline{x}\in V_2^k}(-1)^{f(\underline{x})}(-1)^{\underline{x}\cdot\underline{\lambda}^T} \quad \square$$

유한체 F_{2^n}에서 F_2상의 k차원 벡터 공간 V_2^k로의 선형 전사함수를 $L(x)$라면 L의 인접함수(adjoint) L^*는 다음과 같이 정의된다.
모든 $\underline{u}\in V_2^k$에 대해서 $L(x)\cdot\underline{u}^T$는 F_{2^n}에서 F_2로의 유일한 선형함수를 정의하고 $tr_1^n(\zeta\cdot x)\equiv L(x)\cdot\underline{u}^T$인 유일한 $\zeta\in F_{2^n}$가 존재한다. 이 때 함수 L^*는 $L^*(\underline{u})=\zeta$로 정의된다.
적절한 인접함수 L^*를 갖는 선형 전사함수 L과 bent 함수를 사용하여 Olsen, Scholtz, Welch는 다음의 이진 bent 시퀀스를 생성하였다.

정리 2[2]: $n=0 \bmod 4$, $n=2m$이고, α를 F_{2^n}의 원시원, $\sigma\in F_{2^n}\setminus F_{2^m}$, $\delta\in F_{2^m}^*$이라 하자. F_{2^n}에서 F_2로의 선형 전사함수 L의 인접함수 L^*의 치역은 $\mathrm{range}(L^*)=\{\alpha x \mid x\in F_{2^m}\}$이고 $f(\underline{x})$는 V_2^m에서 F_2로의 bent 함수라고 가정한다. 그러면 이진 시퀀스들의 집합 S는 다음과 같이 정의된다.

$$\begin{aligned}&S=\{s_{\underline{z}} \mid \underline{z}\in V_2^m\}\\&s_{\underline{z}}(t)=f(L(\alpha^t))+L(\alpha^t)\cdot\underline{z}^T+tr^{n_1}(\delta\alpha^t)\end{aligned} \tag{2}$$

S에 속하는 시퀀스들의 상호상관함수와 위상이 안 맞는 경우의 자기상관함수는 3가지 값

$\{-2^m-1,-1,2^m-1\}$을 갖는다. $\square$

(2)의 이진 bent 시퀀스의 상관 특성이 Welch의 하한 견지에서 최적이라는 것이 알려져 있다.
$n=2m=4k$이고 α를 F_{2^n}의 원시원이라 하고 $\{\beta_1,\beta_2,\cdots,\beta_{2k}\}$를 F_2상의 F_{2^m}의 기저라 한다. $\sigma\in F_{2^n}\setminus F_{2^m}$, $\delta\in F_{2^m}^*$, L은 아래와 같이 정의되는 선형 전사함수라 한다.

$$\begin{aligned}&L(\alpha^t)\\&=(tr_1^n(\sigma\beta_1\alpha^t),tr_1^n(\sigma\beta_2\alpha^t),\cdots,tr_1^n(\sigma\beta_{2k}\alpha^t))\end{aligned} \tag{3}$$

V_2^{2k}에 속하는 원소 $\underline{z}$에 대하여 다음의 관계식이 성립한다.

$$\begin{aligned}L(\alpha^t)\cdot\underline{z}^T&=\sum_{i=1}^{2k}z_i\cdot tr_1^n(\sigma\beta_i\alpha^t)\\&=tr_1^n((\sum_{i=1}^{2k}z_i\cdot\beta_i)\sigma\alpha^t)\\&=tr_1^n(\eta\sigma\alpha^t)\end{aligned}$$

여기서 $\eta=\sum_{i=1}^{2k}z_i\cdot\beta_i\in F_{2^m}$이다. 따라서 (2)의 이진 bent 시퀀스는 다음과 같이 다시 쓸 수 있다.

$$s_\eta(t)=f(L(\alpha^t))+tr_1^n((\eta\sigma+\delta)\alpha^t) \tag{4}$$

Ⅲ. 이진 Bent 시퀀스의 일반화

유한체 F_{2^n}상의 k차원 벡터공간을 $V_{2^n}^k$라 하고 그 원소를 $\underline{x}=(x_1,x_2,\cdots,x_k)$, $x_i\in F_{2^n}$로 표현한다. $f(\underline{x})$를 $V_{2^n}^k$에서 F_{2^n}로의 함수로 놓으면 $f(\underline{x})$에 대한 trace 변환을 다음과 같이 변환할 수 있다.

정의 3: $tr_1^e(f(\underline{x}))$는 $V_{2^n}^k$에서 F_2로의 함수라 한다. $tr_1^e(f(\underline{x}))$의 변형된 trace 변환은 다음과 같이 정의된다.

$$\hat{f}(\underline{\lambda})=\frac{1}{\sqrt{2^{ek}}}\sum_{\underline{x}\in V_{2^n}^k}(-1)^{tr_1^e(f(\underline{x}))+tr_1^e(\underline{\lambda}\cdot\underline{x}^T)}$$

여기서 $\underline{x}=(x_1,x_2,\cdots,x_k)$, $\underline{\lambda}=(\lambda_1,\lambda_2,\cdots,\lambda_k)\in V_{2^n}^k$이고 변형된 trace 역변환(inverse modified trace transform)은 다음과 같이 주어진다.

$$(-1)^{tr_1^e(f(\underline{x}))} = \frac{1}{\sqrt{2^{ek}}} \sum_{\underline{\lambda}\in V_{2^r}^k} \hat{f}(\underline{\lambda}) \cdot (-1)^{tr_1^r(\underline{\lambda}\cdot \underline{x}^T)} \quad \square$$

만일 λ_i, x_i를 F_2상의 F_{2^r}의 trace 정규직교의 기저(trace orthonomal basis) $\{\delta_1, \delta_2, \cdots, \delta_e\}$를 사용하여 $\lambda_i = \sum_{j=1}^{e} \lambda_{ij}\delta_j$, $x_i = \sum_{j=1}^{e} x_{ij}\delta_j$ 로 표현하면 trace 함수는 다음과 같이 쓸 수 있다.

$$\begin{aligned} &tr_1^e(\underline{\lambda}\cdot \underline{x}^T) \\ &= tr_1^e(\lambda_1\cdot x_1 + \lambda_2\cdot x_2 + \cdots + \lambda_e\cdot x_e) \\ &= \lambda_{11}\cdot x_{11} + \lambda_{12}\cdot x_{12} + \cdots + \lambda_{1e}\cdot x_{1e} \\ &+ \lambda_{21}\cdot x_{21} + \cdots + \lambda_{2e}\cdot x_{2e} + \cdots \\ &+ \lambda_{k1}\cdot x_{k1} + \lambda_{k2}\cdot x_{k2} + \cdots + \lambda_{ke}\cdot x_{ke} \end{aligned}$$

이것은 두 ek차원 이진 벡터들의 내적에 대응된다. 그리고 $tr_1^e(f(\underline{x}))$도 $V_{2^r}^k$상에서 정의된 부울 함수로 표현될 수 있다. 그래서 F_2상의 F_{2^r}의 trace 정규직교의 기저가 사용된다면 변형된 trace 변환은 하다마드 변환에 대응된다. 만일 $V_{2^r}^k$에 속하는 모든 $\underline{\lambda}$에 대해서 변형된 trace 변환 $\hat{f}(\underline{\lambda})$가 오직 $+1$ 또는 -1 값을 갖는다면 F_2상의 F_{2^r}의 trace 정규직교의 기저를 사용한 $tr_1^e(f(\underline{x}))$의 부울 함수 표현은 bent 함수에 대응된다.

유한체 F_{2^n}에서 F_2상의 $2k$차원 벡터 공간 $V_{2^r}^{2k}$로의 선형 전사함수를 $L(x)$라면 L의 인접함수 L^*는 다음과 같이 정의된다.

모든 $\underline{u}\in V_{2^r}^{2k}$에 대해서 $L(x)\cdot \underline{u}^T$는 F_{2^n}에서 F_{2^r}로의 유일한 선형함수를 정의하고 $tr_e^n(\zeta\cdot x)\equiv L(x)\cdot \underline{u}^T$인 유일한 $\zeta\in F_{2^n}$가 존재한다. 이 때 함수 L^*는 $L^*(\underline{u})=\zeta$로 정의된다.

선형함수 $L(x)$의 정의를 사용하여 부울 함수의 trace 변환은 다음 정리와 같이 유도될 수 있다.

정리 4: $n=2m=4k$라 하고 $L(x)$를 F_{2^n}에서 $V_{2^r}^{2k}$로의 선형 전사함수, $f(\underline{x})$는 $V_{2^r}^{2k}$에서 F_{2^r}로의 함수라 한다. 그러면 함수 $tr_1^e(f(\underline{x}))$의 trace 변환은 다음과 같이 주어진다.

$$\hat{F}(\lambda) = \begin{cases} 0, & \lambda\notin \text{range}(L^*) \\ 2^{\frac{m}{2}}\cdot \hat{f}(\underline{u}), & \lambda\in \text{range}(L^*),\ L^*(\underline{u})=\lambda \end{cases}$$

(증명)

trace 변환의 정의를 사용하면 $tr_1^e(f(L(x)))$의 trace 변환은 다음과 같이 표현된다.

$$\begin{aligned} \hat{F}(\lambda) &= \frac{1}{\sqrt{2^n}} \sum_{x\in F_{2^r}} (-1)^{tr_1^r(f(L(x)))+tr_1^n(\lambda\cdot x)} \\ &= \frac{1}{\sqrt{2^n}} \sum_{x\in F_{2^r}} \frac{1}{\sqrt{2^m}} \cdot \sum_{\underline{u}\in V_{2^r}^{2k}} \hat{f}(\underline{u}) \\ &\quad \cdot (-1)^{tr_1^r(L(x)\cdot \underline{u}^T)} \cdot (-1)^{tr_1^n(x\cdot\lambda)} \\ &= \frac{1}{\sqrt{2^{n+m}}} \sum_{\underline{u}\in V_{2^r}^{2k}} \hat{f}(\underline{u}) \\ &\quad \cdot \sum_{x\in F_{2^r}} (-1)^{tr_1^r(L(x)\cdot \underline{u}^T)+tr_1^n(x\cdot\lambda)} \end{aligned}$$

선형함수 $L(x)$의 인접함수로부터

$$tr_1^e(L(x)\cdot \underline{u}^T) = tr_1^e(tr_e^n(x\cdot L^*(\underline{u})))$$

따라서 $tr_1^e(f(L(x)))$의 trace 변환은 다음과 같이 표현된다.

$$\hat{F}(\lambda) = \frac{1}{\sqrt{2^{n+m}}} \sum_{\underline{u}\in V_{2^r}^{2k}} \hat{f}(\underline{u}) \cdot \sum_{x\in F_{2^r}} (-1)^{tr_1^n((\lambda+L^*(\underline{u}))\cdot x)}$$

명백히 위 식에서 내부 합은 $\lambda=L^*(\underline{u})$이면 2^n이고 그렇지 않으면 0이다. 그러므로 $\lambda\in \text{range}(L^*)$라면

$$\begin{aligned} &\hat{F}(\lambda) \\ &= \frac{1}{\sqrt{2^{n+m}}} \cdot 2^n \cdot \hat{f}(\underline{u}), \quad \text{when } \lambda = L^*(\underline{u}) \\ &= 2^{\frac{m}{2}} \cdot \hat{f}(\underline{u}) \end{aligned}$$

$\lambda\notin \text{range}(L^*)$이면 $\lambda=L^*(\underline{u})$를 만족시키는 $V_{2^r}^{2k}$의 원소 $\underline{u}$가 존재하지 않는다. 따라서 $\hat{F}(\lambda)=0$이다. $\square$

선형 함수 $L(x)$가 다음과 같이 주어졌다고 가정한다.

$$L(x) = (tr_e^n(\sigma\beta_1 x), tr_e^n(\sigma\beta_2 x), \cdots, tr_e^n(\sigma\beta_{2k} x)) \tag{5}$$

여기에서 $\sigma\in F_{2^n}\setminus F_{2^m}$, $n=2m=4k$이고 $\{\delta_1, \delta_2, \cdots, \delta_{2k}\}$를 F_{2^r}상의 F_{2^m}의 기저라 한다. 그러면 임의의 $\underline{u}\in V_{2^r}^{2k}$에 대해서 다음의 관계식이 성립한다.

$$L(x)\cdot \underline{u}^T = tr_e^n(\eta\cdot\sigma\cdot x) \tag{6}$$

여기서 $\underline{u}=(u_1, u_2, \cdots, u_{2k})$이고

$$\eta = \sum_{i=1}^{2k} \beta_i u_i \tag{7}$$

명백히 $\underline{u}$가 $V_{2^r}^{2k}$ 상에서 변할 때 η는 F_{2^m}의 모든 원소를 커버한다. 즉,

$$\{\eta \mid \underline{u} \in V_{2^e}^{2k}\} = F_{2^m}$$

따라서

$$\text{range}(L^*) = \{\eta \cdot \sigma \mid \eta \in F_{2^m}\} \tag{8}$$

이로부터 다음과 같은 정리에서처럼 균형 특성과 최적의 상관특성을 갖는 새로운 이진 시퀀스군를 생성할 수 있다.

정리 5: $n=2m=4ek$, L를 F_{2^n}에서 $V_{2^e}^{2k}$로의 선형 전사함수, $\delta \in F_{2^m}^*$라 한다. $V_{2^e}^{2k}$에서 정의된 $tr_1^e(f(\underline{x}))$의 변형된 trace 변환은 $+1$ 또는 -1 값만을 갖는다고 가정한다. 그러면 일반화된 이진 bent 시퀀스군

$$\begin{aligned} &S = \{s_{\underline{z}}(t) \mid \underline{z} \in V_{2^e}^{2k},\ 0 \le t \le 2^n - 2\} \\ &s_{\underline{z}}(t) = \\ &tr_1^e(f(L(\alpha^t))) + tr_1^e(L(\alpha^t) \cdot \underline{z}^T) + tr_1^n(\delta \cdot \alpha^t) \end{aligned} \tag{9}$$

는 균형 특성과 $\{2^n-1, 2^m-1, -1, 2^m-1\}$의 상관함수값을 갖는다.

(증명)

$s_{\underline{z}}(t)$에서 α^t를 F_{2^n}의 원소 x로 대신하여 시퀀스 $s_{\underline{z}}(x)$를 다시 표현한다.

$$\begin{aligned} &s_{\underline{z}}(x) = \\ &tr_1^e(f(L(x))) + tr_1^e(L(x) \cdot \underline{z}^T) + tr_1^n(\delta \cdot x) \end{aligned}$$

(5)의 $L(x)$의 정의로부터 (9)의 시퀀스는 다음과 같다.

$$\begin{aligned} &s_{\underline{z}}(x) \\ &= tr_1^e(f(L(x))) + tr_1^e(tr_e^n(\eta' \sigma \cdot x)) \\ &\quad + tr_1^n(\delta \cdot x) \\ &= tr_1^e(f(L(x))) + tr_1^n((\eta' \sigma + \delta) \cdot x) \end{aligned} \tag{10}$$

여기서 $\eta' \in F_{2^m}$은 (7)에서처럼 정의된다. 그러면 $s_{\underline{z}}(x)$의 trace 변환은 다음과 같다.

$$\begin{aligned} &\hat{S}_{\underline{z}}(\lambda) \\ &= \frac{1}{\sqrt{2^n}} \sum_{x \in F_{2^n}} (-1)^{tr_1^e(f(L(x))) + tr_1^n((\eta' \sigma + \delta + \lambda) \cdot x)} \end{aligned}$$

정리 4로부터 trace 변환을 다음과 같이 계산할 수 있다.

$$\hat{S}_{\underline{z}}(\lambda) = \begin{cases} 0, & \text{for } \eta' \sigma + \delta + \lambda \notin \text{range}(L^*) \\ 2^{-\frac{m}{2}} \cdot \hat{f}(\underline{u}), & \text{for } \eta' \sigma + \delta + \lambda \in \text{range}(L^*), \\ & L^*(\underline{u}) = \eta' \sigma + \delta + \lambda \end{cases}$$

(8)로부터 L^*의 치역은 다음과 같은 특성을 갖는다.

$$\begin{aligned} &\text{range}(L^*) + \eta' \sigma + \delta \\ &= \{\eta \sigma \mid \eta \in F_{2^m}\} + \eta' \sigma + \delta \\ &= \{\eta \sigma \mid \eta \in F_{2^m}\} + \delta \\ &= \text{range}(L^*) + \delta \\ &= \{\eta \sigma + \delta \mid \eta \in F_{2^m}\} \end{aligned}$$

H를 다음과 같이 정의한다.

$$H = \text{range}(L^*) + \eta' \sigma + \delta = \{\eta \sigma + \delta \mid \eta \in F_{2^m}\} \tag{11}$$

그러면 집합 H는 시퀀스군 S 내의 모든 시퀀스에 대해 동일하다. 또한 $1 \le \tau \le 2^n - 2$와 원시원 $\alpha \in F_{2^n}$에 대해서

$$|H \cap H\alpha^\tau| \le 1 \tag{12}$$

가 성립한다는 것은 쉽게 증명된다. $\hat{h}(\underline{u})$가 $+1$ 또는 -1 값만을 갖는다는 가정으로부터 $s_{\underline{z}}(x)$의 trace 변환은 다음과 같이 주어진다.

$$\hat{S}_{\underline{z}}(\lambda) = \begin{cases} 0, & \text{for } \lambda \notin H \\ \pm 2^{\frac{m}{2}}, & \text{for } \lambda \in H \end{cases} \tag{13}$$

(1)에서 시퀀스 $s_y(t)$와 $s_z(t)$의 상호상관함수는 다음과 같이 쓸 수 있다.

$$R_{yz}(\tau) = \sum_{x \in F_{2^n}} (-1)^{s_x(x) + s_z(x\alpha^\tau)}$$

다음의 세 가지 경우에 대해서 정리를 증명할 수 있다.

i) $\tau = 0$:

Parseval의 정리를 이용하여 상호상관함수를 다음과 같이 나타내면

$$\begin{aligned} R_{yz}(\tau) &= -1 + \sum_{x \in F_{2^n}} (-1)^{s_x(x) + s_z(x\alpha^\tau)} \\ &= -1 + \sum_{\lambda \in F_{2^n}} \hat{S}_{\underline{y}}(\lambda) \cdot \hat{S}_{\underline{z}}(\lambda \alpha^{-\tau}) \end{aligned}$$

(12),(13)로부터 상관함수는 다음과 같이 유도된다.

$$\begin{aligned} R_{yz}(\tau) &= -1 \pm 2^{\frac{m}{2}} \cdot 2^{\frac{m}{2}} \cdot |H \cap H\alpha^\tau| \\ &= \begin{cases} -1, & \text{for } |H \cap H\alpha^\tau| = 0 \\ -1 \pm 2^m, & \text{for } |H \cap H\alpha^\tau| = 1 \end{cases} \end{aligned}$$

ii) $\tau = 0$이고 $\underline{y} \ne \underline{z}$:

$$\begin{aligned} R_{yz}(0) &= \sum_{t=0}^{2^n-2} (-1)^{tr_1^e(L(\alpha^t) \cdot (\underline{y}+\underline{z})^T)} \\ &= \sum_{t=0}^{2^n-2} (-1)^{tr_1^n(\eta' \sigma \cdot \alpha^t)} \\ &= -1 \end{aligned}$$

여기서 $\eta' = \sum_{i=1}^{2k} \beta_i(y_i + z_i) \neq 0$이다.

iii) $\tau = 0$이고 $\underline{y} = \underline{z}$:

이 경우는 상관함수가 $2^n - 1$ 값을 갖는다. S의 시퀀스들의 상관 특성을 증명했다.

시퀀스 $s_{\underline{z}}(t)$의 균형 특성을 증명하기 위해서 다음과 같이 정의된 B에 대해 $B=0$을 증명하면 된다.

$$B = \sum_{\underline{x} \in F_{2^r}} (-1)^{s_{\underline{z}}(\underline{x})} \tag{14}$$

(10)을 (14)에 대입해주면

$$B = \sum_{\underline{x} \in F_{2^r}} (-1)^{tr_1^r(f(L(\underline{x}))) + tr_1^n((\eta' \sigma + \delta) \cdot \underline{x})}$$

$\delta \neq 0$이어서 (8)에 의해 $\eta' \sigma + \delta$는 L^*의 치역에 속하지 않는다. 따라서 정리 4에 의해 명백히 $B=0$이다. □

예제 6: $V_{2^r}^{2k}$에서 정의된 함수 $f(\underline{x})$를

$$f(\underline{x}) = x_1 x_{k+1} + x_2 x_{k+2} + \cdots + x_k x_{2k} + g(x_1, x_2, \cdots, x_k),$$

라 한다. 여기서 $g(x_1, x_2, \cdots, x_k)$는 유한체 F_{2^r}상의 k차원 벡터공간에서 정의된 임의의 함수이다. 함수 $f(\underline{x})$의 변형된 trace 변환은 다음과 같이 주어진다.

$$\begin{aligned}
&\hat{f}(\underline{\lambda}) \\
&= \frac{1}{\sqrt{2^{2ek}}} \sum_{\underline{x} \in V_{2^r}^{2k}} (-1)^{tr_1^r(f(\underline{x})) + tr_1^r(\underline{x} \cdot \underline{\lambda}^T)} \\
&= \frac{1}{\sqrt{2^{2ek}}} \sum_{(x_1, \cdots, x_k) \in V_{2^r}^k} (-1)^{tr_1^r(g(x_1, \cdots, x_k)) + tr_1^r(x_1\lambda_1 + \cdots + x_k\lambda_k)} \\
&\quad \cdot \sum_{(x_{k+1}, \cdots, x_{2k}) \in V_{2^r}^k} (-1)^{tr_1^r(x_1 x_{k+1} + \cdots + x_k x_{2k}) + tr_1^r(x_{k+1}\lambda_{k+1} + \cdots + x_{2k}\lambda_{2k})} \\
&= \frac{1}{\sqrt{2^{2ek}}} \sum_{(x_1, \cdots, x_k) \in V_{2^r}^k} (-1)^{tr_1^r(g(x_1, \cdots, x_k)) + tr_1^r(x_1\lambda_1 + \cdots + x_k\lambda_k)} \\
&\quad \cdot \sum_{(x_{k+1}, \cdots, x_{2k}) \in V_{2^r}^k} (-1)^{tr_1^r((x_1 + \lambda_{k+1}) \cdot x_{k+1} + \cdots + (x_k + \lambda_{2k}) \cdot x_{2k})}
\end{aligned}$$

위 식의 내부 합은 다음과 같이 주어진다.

$$\begin{cases} 2^{ek}, & \text{for } (x_1, x_2, \cdots, x_k) = (\lambda_{k+1}, \lambda_{k+2}, \cdots, \lambda_{2k}) \\ 0, & \text{otherwise} \end{cases}$$

따라서 함수 $f(\underline{x})$의 변형된 trace 변환은 다음과 같이 주어진다.

$$\begin{aligned}
&\hat{f}(\underline{\lambda}) \\
&= 1 \cdot (-1)^{tr_1^r(g(\lambda_{k+1}, \cdots, \lambda_{2k})) + tr_1^r(\lambda_{k+1} \cdot \lambda_1 + \cdots + \lambda_{2k} \cdot \lambda_k)} \\
&= \pm 1
\end{aligned}$$

만일 F_2상의 F_{2^r}의 trace 정규직교의 기저를 사용하여 함수 $f(\underline{x})$를 V_2^{2ek}에서 정의된 부울 함수로서 표현한다면 변형된 trace 변환이 하다마드 변환에 대응되기 때문에 그 부울 함수는 bent 함수가 된다.

(15)에서 정의된 함수 $f(\underline{x})$를 이용하여 균형 특성과 최적의 상관특성을 갖는 새로운 이진 시퀀스군을 생성할 수 있다. $n = 2m = 4ek$라 하고 $L(\alpha^t)$이 (5)에서 정의된 F_{2^n}에서 $V_{2^e}^{2e}$로의 선형 전사함수이고 $\delta \in F_{2^m}^*$라 한다. 그러면 아래와 같이 정의된 이진 시퀀스군

$$\begin{aligned}
&S = \{ s_{\underline{z}}(t) \mid \underline{z} \in V_{2^r}^{2k},\ 0 \le t \le 2^n - 2 \} \\
&s_{\underline{z}}(t) \\
&= tr_1^e\Big(\sum_{i=1}^{k} tr_e^n(\sigma\beta_i \cdot \alpha^t) \cdot tr_e^n(\sigma\beta_{k+i} \cdot \alpha^t) \\
&\quad + g(tr_e^n(\sigma\beta_1 \cdot \alpha^t), \cdots, tr_e^n(\sigma\beta_k \cdot \alpha^t)) \\
&\quad + tr_1^e\Big(\sum_{i=1}^{2k} z_i \cdot tr_e^n(\sigma\beta_i \cdot \alpha^t) \Big) + tr_1^n(\delta \cdot \alpha^t)
\end{aligned} \tag{15}$$

는 균형 특성과 $\{2^n - 1, 2^m - 1, -1, 2^m - 1\}$의 최적의 상관함수 값을 갖는다. □

예제 6에 따라 $k=1$이고 $n = 2m = 4e$이라면 다음 예제와 같은 이진 시퀀스군을 얻을 수 있다.

예제 7: $V_{2^r}^2$가 F_{2^r}상에서 정의된 2차원 벡터공간이라고 하고 $f(\underline{x})$가 $V_{2^r}^2$상에 다음과 같이 정의된 함수라고 한다.

$$f(\underline{x}) = x_1 x_2 \tag{16}$$

명백히 $f(\underline{x})$의 변형된 trace 변환은 ± 1 값만을 갖는다. 따라서 (16)의 함수 $f(\underline{x})$를 이용해 최적의 상관 특성과 균형 특성을 갖는 새로운 이진 시퀀스군을 생성할 수 있다. $\{\beta_1, \beta_2\}$를 F_{2^r}상에서 정의된 F_{2^n}의 기저라고 하고 $\sigma \in F_{2^n} \backslash F_{2^m}$, $\delta \in F_{2^m}^*$라고 하면 주기가 $2^n - 1$의 이진 시퀀스군

$$\begin{aligned}
&S = \{ s_{\underline{z}}(t) \mid \underline{z} \in V_{2^r}^2,\ 0 \le t \le 2^n - 2 \} \\
&s_{\underline{z}}(t) = tr_1^e(tr_e^n(\sigma\beta_1 \cdot \alpha^t) \cdot tr_e^n(\sigma\beta_2 \cdot \alpha^t)) \\
&\quad + tr_1^n(\sigma(z_1 \cdot \beta_1 + z_2 \cdot \beta_2) \cdot \alpha^t) \\
&\quad + tr_1^n(\sigma \cdot \alpha^t)
\end{aligned} \tag{17}$$

는 균형 특성과 최적의 상관 특성을 갖고 상관값은 $\{2^n - 1, -2^m - 1, -1, 2^m - 1\}$가 된다. □

따름정리 8: $n = 2m = 4e$이고 $\sigma \in F_{2^n} \backslash F_{2^m}$, $\delta \in F_{2^m}^*$

라 한다. 그러면 다음과 같이 정의되는 이진 시퀀스군

$$S=\{s_\eta(t) \mid \eta\in F_{2^m},\ 0\le t\le 2^n-2\}$$
$$s_\eta(t) = tr_1^n(\alpha^{(2^r+1)t}) + tr_1^n((\delta\cdot\sigma^{-1}+\eta)\cdot\alpha^t) \quad (18)$$

는 균형 특성과 최적의 상관 특성을 갖고 상관값은 $\{2^n-1,-2^m-1,-1,2^m-1\}$가 된다.

(증명)

예제 7에서 $\{1,\beta\}=\{1,\alpha^{2^m+1}\}$를 F_{2^r}상의 F_{2^m}의 기저라고 하고 $\eta=z_1\cdot 1+z_2\cdot\beta\in F_{2^m}$이라면 시퀀스 (17)은 다음과 같이 쓸 수 있다.

$$s_\eta(t) = tr_1^e(tr_e^n(\sigma\cdot\alpha^t)\cdot tr_e^n(\sigma\beta\cdot\alpha^t)) + tr_1^n(\sigma\eta\cdot\alpha^t) + tr_1^n(\delta\cdot\alpha^t)$$

여기에서 내부 trace를 풀어주면

$$\begin{aligned} &s_\eta(t)\\ &= tr_1^e(tr_e^n(\sigma\cdot\alpha^t)\cdot(\sigma\beta\cdot\alpha^t)))\\ &\quad + tr_1^n((\sigma\eta+\delta)\cdot\alpha^t)\\ &= tr_1^n(\sum_{i=0}^{2^r}\sigma^{1+2^{2r}}\beta\cdot\alpha^{(1+2^{2r})t}))\\ &\quad + tr_1^n((\sigma\eta+\delta)\cdot\alpha^t)\\ &= tr_1^n(\beta\sigma^2\alpha^{2t}) + tr_1^n(\beta\sigma^{1+2^r}\alpha^{(1+2^r)t})\\ &\quad + tr_1^n(\beta\sigma^{1+2^{2r}}\alpha^{(1+2^{2r})t} + tr_1^n(\beta\sigma^{1+2^{3r}}\alpha^{(1+2^{3r})t})\\ &\quad + tr_1^n((\sigma\eta+\delta)\cdot\alpha^t) \end{aligned} \quad (19)$$

그런데 $\beta\sigma^{1+2^{2r}}\alpha^{(1+2^{2r})t}\in F_{2^m}$이므로

$$tr_1^n(\beta\sigma^{1+2^{2r}}\alpha^{(1+2^{2r})t})=0$$

이다. 또한

$$\begin{aligned} &tr_1^n(\beta\sigma^{1+2^{3r}}\alpha^{(1+2^{3r})t})\\ &=[tr_1^n(\beta\sigma^{1+2^{3r}}\alpha^{(1+2^{3r})t})]^{2^r}\\ &= tr_1^n(\beta^{2^r}\sigma^{2^r(1+2^{3r})}\alpha^{2^r(1+2^{3r})t})\\ &= tr_1^n(\beta^{2^r}\sigma^{1+2^r}\alpha^{(1+2^r)t}) \end{aligned}$$

이므로 시퀀스 (19)는 다음과 같이 쓸 수 있다.

$$\begin{aligned} &s_\eta(t)\\ &= tr_1^n(\beta^{2^{2r-1}}\sigma\alpha^t) + tr_1^n((\beta+\beta^{2^r})\sigma^{1+2^r}\alpha^{(1+2^r)t})\\ &\quad + tr_1^n((\sigma\eta+\delta)\cdot\alpha^t)\\ &= tr_1^n((\beta+\beta^{2^r})\sigma^{1+2^r}\alpha^{(1+2^r)t})\\ &\quad + tr_1^n((\sigma(\eta+\beta^{2^{2r-1}})+\delta)\cdot\alpha^t)\\ &= tr_1^n((\beta+\beta^{2^r})\alpha^{(1+2^r)t'})\\ &\quad + tr_1^n((\sigma^{-1}\cdot\delta+\eta+\beta^{2^{2r-1}})\cdot\alpha^{t'})\\ &= tr_1^n(\beta^{(1+2^r)a}\alpha^{(1+2^r)t'})\\ &\quad + tr_1^n((\sigma^{-1}\cdot\delta+\eta+\beta^{2^{2r-1}})\cdot\alpha^{t'})\\ &= tr_1^n(\alpha^{(t'+(1+2^{2r}+1)a)(1+2^r)})\\ &\quad + tr_1^n((\sigma^{-1}\cdot\delta+\eta+\beta^{2^{2r-1}})\cdot\alpha^{t'})\\ &= tr_1^n(\alpha^{(1+2^r)t''}) + tr_1^n((\sigma^{-1}\cdot\delta'+\eta')\cdot\alpha^{t''}) \end{aligned}$$

여기에서 $\alpha^{t'}=\sigma\alpha^t$, $t''=t'+(2^{2e}+1)a$ 이고 δ'와 η'는 F_{2^m}의 원소이다. □

일반화된 이진 bent 시퀀스의 선형 스팬은 $2n$이고 일반화된 이진 bent 시퀀스의 가장 간단한 형태이며 기존의 이진 bent 시퀀스로는 주어질 수 없다.

참 고 문 헌

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

[2] J.D. Olsen, R.A. Scholtz and L.R. Welch, "Bent-function sequences," *IEEE Trans. Inform. Theory*, vol. 28, pp. 858-864, Nov. 1982.

[3] A. Lempel and M. Cohn, "Maximal families of bent sequences," *IEEE Trans. Inform. Theory*, vol. 28, pp. 865-868, Nov. 1982.

[4] S.W. Golomb, *Shift-Register Sequences*, Revised Ed., Aegean Park Press, San Francisco, 1982.

[5] R. Lidl and H. Niederreiter, *Finite Fields*, vol. 20 of Encyclopedia of Mathematics and Its Applications, Addison-Wesley, Reading, MA, 1983.

[6] J.S. No and P.V. Kumar, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span," *IEEE Trans. Inform. Theory*, vol. 35, no. 2, pp.371-379, Mar. 1989.

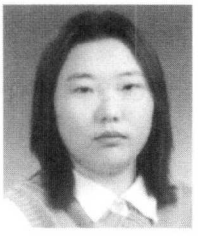
[7] J.S. No, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span," Ph.D. dissertation, University of Southern California, May, 1988.

[8] F.J. McWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, New York: North-Holland, 1977.

[9] L. R. Welch, "Lower bounds on the maximal cross correlation of signals," *IEEE Trans.*

Inform. Theory, vol. 20, pp. 396-399, May 1976.

길 강 미(Gang-Mi Gil)

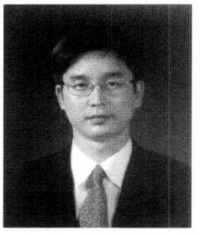


2000년 2월 : 서울대학교 전기공학부 공학석사
2000년 3월~현재 : 서울대학교 대학원 전기 · 컴퓨터공학부 석사과정
<주관심 분야> 디지털통신, 오류정정부호, 시퀀스

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

신 동 준(Dong-Joon Shin) 정회원



1990년 2월 : 서울대학교 전자공학과 공학사
1991년 12월 : Northwestern University, 전기공학과 공학석사
1998년 12월 : University of Southern California, 전기공학과 공학박사
1999년 1월~1999년 4월 : Research Associate(USC)
1999년 4월~2000년 8월 : Hughes Network Systems, MTS
2000년 9월~현재 : 한양대학교 전자전기컴퓨터공학부 전임강사
<주관심 분야> 디지털통신, 이산수학, 시퀀스, 오류정정부호, 암호학