새로운 p진 Bent 수열의 생성

준회원 김 영 식, 장 지 웅, 종신회원 노 종 선*

New Constructions of p-ary Bent Sequences

Young-Sik Kim, Ji-Woong Jang *Associate Member*, **Jong-Seon No*** *Life Members*

요 약

본 논문에서는 소수 p에 대해 Kumar와 Moreno가 소개한 유한체 상에서 정의된 bent 함수를 이용하여 균형성과 최적의 상관성질을 갖는 p진 bent 수열군의 일반화된 생성방법을 소개한다[3]. 이렇게 생성된 수열군을 일반화된 p진 수열이라 부르기로 한다. Moriuchi와 Imamura가 [6]에서 소개한 균형성과 최적의 상관특성을 갖는 p진 수열군은 일반화된 bent 수열의 특별한 예임을 보인다.

ABSTRACT

In this paper, using bent functions defined on the finite field we generalized the construction method of the family of p-ary bent sequences with balanced and optimal correlation property introduced by Kumar and Moreno for an odd prime p[3], *called a generalized p-ary bent sequence.* It turns out that the family of balanced p-ary sequences with optimal correlation property introduced by Moriuchi and Imamura [6] is a special case of the generalized p-ary bent sequences.

Key Words : bent sequences, bent functions, generalized bent sequences

I. 서 론

Rothaus는 m-tuple 이진 벡터공간에서 $\{0,1\}$로의 사상(mapping)인 이진 bent 함수를 소개하였고 그 후 이진 bent 함수의 다양한 그룹들이 발견되어왔다[1][2][4]. Olsen, Scholtz, Welch는 이진 bent 함수를 이용하여 균형성을 갖고 Welch의 하한값에 근사하는 상관값을 갖는 이진 bent 수열을 생성하였다[9]. Kumar, Scholtz, Welch는 이진에서 q진으로 문자의 크기를 확장하여 q진 벡터공간으로부터 modulo q연산된 정수들의 집합으로의 사상인 일반화된 bent 함수를 소개하였다[4]. Kumar와 Moreno는 홀수 소수 p에 대해 이진 bent 수열의 생성법을 p진 bent 함수에 적용하여 p진 bent 수열군을 정의하였다[3]. 또한, 이들은 $c|m$, $b\in F_{p^m}^*$에 대하여 $\mathrm{tr}_1^m(bx^{p^n+1})$로 정의되는 p^m개의 원소를 갖는 유한체 F_{p^m}상의 bent 함수를 정의하였는데, 이 bent 함수는 Moriuchi와 Imamura가 제안한 균형성과 최적의 상관 특성을 갖는 p진 수열의 생성에 이용된다[6].

본 논문에서는 홀수 소수 p에 대해 유한체에서 정의된 bent 함수를 이용하여 Kumar와 Moreno가 제안한 균형성과 최적의 상관 특성을 갖는 p진 bent 수열군의 생성법을 일반화시키고 이를 일반화된 bent 수열군이라 부를 것이다. 특히 Moriuchi와 Imamura가 제안한 균형성과 최적의 상관 특성을 갖는 p진 수열은 일반화된 bent 수열의 특별한 예임을 보인다.

* 서울대학교 전기컴퓨터공학부 부호 및 암호 연구실(jsno@snu.ac.kr)
※본 연구는 ITRC연구과제, BK21의 지원으로 수행되었음.
논문번호: 030258 - 0618, 접수일자: 2003년 6월 18일

Ⅱ. 사전지식

홀수 소수 p에 대해 S가 다음과 같이 주어지는 주기가 $N=p^n-1$인 M개의 p진 수열군이라 하자.

$$S=\{s_i(t)\,|\,0\le i\le M-1,\ 0\le t\le N-1\}.$$

수열군 S의 원소인 수열 $s_i(t)$와 $s_j(t)$의 상관함수는 $\omega=e^{j\frac{2\pi}{p}}$일 때, 아래와 같이 쓸 수 있다.

$$R_{i,j}(\tau)=\sum_{t=0}^{N-1}\omega^{s_i(t+\tau)-s_j(t)} \qquad (1)$$

여기서 $0\le i,j\le M-1,\ 0\le\tau\le N-1$이다. 위 식에서 상관값의 최대값은 다음과 같이 정의된다.

$$R_{\max}=\max_{0\le i,j\le M-1,\ 0\le\tau\le N-1}|R_{i,j}(\tau)|.$$

여기서 $i=j$이고 $\tau=0$인 경우는 제외된다.

주기가 p^n-1인 p진 수열군의 $R_{\max}$값이 $p^{n/2}+1$인 경우, 수열군이 최적의 상관 특성을 갖는다고 말한다.

이제 z가 정수이고 V_z^m이 modulo z연산을 한 정수들의 집합 J_z상의 m차원 벡터공간이라 하자. 또한, $\omega_z=e^{j\frac{2\pi}{z}}$, $j=\sqrt{-1}$이고 $f(\underline{x})$가 V_z^m으로부터 J_z로의 함수라 하면 함수 $f(\underline{x})$의 푸리에 변환은 다음과 같이 정의된다.

$$F(\underline{\lambda})=\frac{1}{\sqrt{z^m}}\sum_{x\in V_z^m}\omega_z^{f(x)-\underline{\lambda}\cdot\underline{x}^T},\ \text{all}\ \underline{\lambda}\in V_z^m.$$

단, 위 식에서 $\underline{x}^T$는 $\underline{x}$의 전치이다. 이 때, 일반화된 bent 함수는 아래와 같이 정의된다.

정의 1 [Kumar, Scholtz, Welch[4]] : 임의의 $\underline{\lambda}\in V_z^m$에 대해 V_z^m으로부터 J_z로의 함수 $f(\underline{x})$의 푸리에 계수가 항상 크기가 1일 때, $f(\underline{x})$를 일반화된 bent 함수라 한다. □

본 논문에서는 z가 소수 p인 경우만 고려한다. 그러므로 V_p^m은 p개의 원소를 갖는 유한체 F_p상의 m차 벡터공간이 되고 $f(\underline{x})$는 V_p^m으로부터 F_p로의 함수가 된다.

이제 F_{p^m}이 p^m개의 원소를 갖는 유한체라 하고 정수 e와 k에 대해 $m=ek>1$이라 하면 F_{p^m}에서 그 부분체 F_{p^k}로의 trace 함수 $\mathrm{tr}_k^m(\cdot)$은 $\mathrm{tr}_k^m(x)=\sum_{i=0}^{e-1}x^{p^{ik}}$로 정의된다[5]. 단, x는 F_{p^m}의 원소이다.

Olsen과 Scholtz 그리고 Welch는 F_{2^m}에서 F_2로의 trace 변환을 소개하였다[7]. 이 때, 유한체 p^m개의 원소를 갖는 F_{p^m}으로부터 F_p로의 함수에 대한 trace 변환은 다음과 같이 일반화 될 수 있다.

정의 2 [Olsen, Scholtz, Welch[7]] : $f(x)$가 F_{p^m}에서 F_p로의 함수라 하면, 임의의 $\lambda\in F_{p^m}$에 대해 $f(x)$의 trace 변환과 그 역변환은 다음과 같이 정의된다.

$$F(\lambda)=\frac{1}{\sqrt{p^m}}\sum_{x\in F_{p^m}}\omega^{f(x)-\mathrm{tr}_1^m(\lambda x)},$$

$$\omega^{f(x)}=\frac{1}{\sqrt{p^m}}\sum_{\lambda\in F_{p^m}}F(\lambda)\omega^{\mathrm{tr}_1^m(\lambda x)}.$$

□

이제 F_{p^m}상에서 정의된 함수 $f(x)$가 trace 변환 계수의 크기로 1만을 가질 경우 이를 일반화된 bent 함수라 정의한다.

또한 $V_{p^k}^e$에서 F_p로의 함수 $f(\underline{x})$의 trace 변환 쌍은 다음과 같이 중간체에서 정의된 trace 변환으로 변형시킬 수 있다.

정의 3 : $m=ek$라 하고 $f(\underline{x})$가 $V_{p^k}^e$에서 F_p로의 함수라 하면, $f(\underline{x})$의 변형된 trace 변환과 그 역변환은 아래와 같이 정의된다.

$$F_M(\underline{\lambda})=\frac{1}{\sqrt{p^m}}\sum_{x\in V_{p^k}^e}\omega^{f(x)-\mathrm{tr}_1^k(\underline{\lambda}\cdot\underline{x}^T)},$$

$$\text{all}\ \underline{\lambda}\in V_{p^k}^e,$$

$$\omega^{f(x)}=\frac{1}{\sqrt{p^m}}\sum_{\underline{\lambda}\in V_{p^k}^e}F_M(\underline{\lambda})\omega^{\mathrm{tr}_1^k(\underline{\lambda}\cdot\underline{x}^T)},$$

$$\text{all}\ \underline{\lambda}\in V_{p^k}^e.$$

□

이제 다음 정리와 같이 F_{p^m}상에서 p진 bent 함수를 생성할 수 있다[10].

정리 1 [Kim, Jang, No, Helleseth[10]] : $m=2k$ 또는 $2k+1$이라 하고 $a_i \in F_p$, $b \in F_{p^m}^*$라 하자. 또한, F_{p^m}에서 F_p로의 p진 quadratic 함수 $f(x)$가 아래와 같이 정의된다 하자.

$$f(x) = \mathrm{tr}_1^m\left(\sum_{i=0}^{k} a_i x^{1+p^i}\right). \qquad (2)$$

이 때, $f(x)$가 다음을 만족하면 $f(x)$는 bent 함수이다.

$$\sum_{i=0}^{k} a_i(\varepsilon^{il}+\varepsilon^{-il}) \neq 0,$$

$$\text{for all } l,\ 0 \le l \le m-1.$$

여기서 위 식에서 $\varepsilon = e^{j\frac{2\pi}{m}}$이다. □

III. 새로운 p진 Bent 수열의 생성

Kumar와 Moreno는 m차 p진 벡터공간 V_p^m상에서 정의된 p진 bent 함수를 이용하여 Olsen과 Scholtz, Welch가 제안한 이진 bent 수열을 다음과 같이 p진 bent 수열로 확장시켰다.

정리 2 [Kumar, Moreno[3]] : p가 홀수 소수이고 m은 정수, $n=2m$, α는 F_{p^n}의 원시원이라 하자. 또한 $f(\cdot)$가 V_p^m상의 bent 함수이고, $\sigma \in F_{p^n} \setminus F_{p^m}$과 F_p상의 F_{p^m}의 기저 $\{\beta_1, \beta_2, \cdots, \beta_m\}$에 대해, $L(x) = (\mathrm{tr}_1^n(\beta_1 \sigma x), \cdots, \mathrm{tr}_1^n(\beta_m \sigma x))$라 하자. 이 때 $\delta \in F_{p^m}^*$라 하면 p진 bent 수열군은 다음과 같이 정의된다.

$$S = \{s_\eta(t) \mid \eta \in F_{p^m},\ 0 \le t \le p^n-2\}$$
$$s_\eta(t) = f(L(\alpha^t)) + \mathrm{tr}_1^n((\eta\sigma+\delta)\alpha^t).$$

여기서 수열군 내의 수열간의 상관값의 상한값은 p^m+1이고 $|S| = p^m$이다. □

p-진 bent 수열군의 생성을 다음과 같이 일반화 할 수 있다.

정리 3 : p가 홀수 소수이고 m, e, k가 정수라 하자. $n=2m=2ek$이고 α가 F_{p^n}의 원시원이라고 하자. 그리고 $f(\cdot)$가 $V_{p^k}^e$에서 정의된 p진 bent 함수라 하자. $L(x) = (\mathrm{tr}_k^n(\beta_1 \sigma x), \mathrm{tr}_k^n(\beta_2 \sigma x), \cdots, \mathrm{tr}_k^n(\beta_e \sigma x))$이고 여기서 $\sigma \in F_{p^n} \setminus F_{p^m}$이고 $\{\beta_1, \beta_2, \cdots, \beta_e\}$가 F_{p^k}상에서 F_{p^m}의 기저이다. $\delta \in F_{p^m}^*$라 하자. 그러면 일반화된 p진 bent 수열군은 다음과 같이 정의된다.

$$S = \{s_\eta(t) \mid \eta \in F_{p^m},\ 0 \le t \le p^n-2\}$$
$$s_\eta(t) = f(L(\alpha^t)) + \mathrm{tr}_1^n((\eta\sigma+\delta)\alpha^t).$$

여기서 이들 수열들의 상관값의 상한값은 p^m+1이고, $|S| = p^m$이다. □

[9]의 이진 bent 수열의 증명과 유사한 방식으로, 정의 3에서 정의된 변형 trace 변환을 이용하여 위의 정리를 증명 할 수 있다. 이는 다음의 보조정리로부터 출발한다.

보조정리 1 : 양의 정수 e와 m, k에 대해 $n=2m=2ek$라 하고 $L(x)$가 F_{p^n}에서 $V_{p^k}^e$로의 선형 사상이라 하자. 또한 $f(\underline{x})$가 $V_{p^k}^e$에서 F_p로의 함수라 하면 $f(L(x))$의 trace 변환은 다음과 같이 주어진다.

$$\hat{F}(\lambda) = \begin{cases} 0, & \lambda \notin \mathrm{range}(L^*) \\ p^{\frac{m}{2}} F_M(\underline{u}), & \lambda \in \mathrm{range}(L^*) \\ & L^*(\underline{u}) = \lambda. \end{cases}$$

여기서 $F_M(\underline{u})$는 정의 3에서 정의된 $f(\underline{x})$의 변형 trace 변환이다.

증명) Trace 변환의 정의를 이용하면 $f(L(x))$의 trace 변환을 다음과 같이 나타낼 수 있음은 자명하다.

$$F(\lambda) = \frac{1}{\sqrt{p^n}} \sum_{x \in F_{p^n}} \omega^{f(L(x)) - \mathrm{tr}_1^n(\lambda x)}$$
$$= \frac{1}{\sqrt{p^n}} \sum_{x \in F_{p^n}} \frac{1}{\sqrt{p^m}} \sum_{\underline{u} \in V_{p^k}^e} F_M(\underline{u}) \times \omega^{\mathrm{tr}_k^n(L(x)\cdot \underline{u}^T)} \omega^{-\mathrm{tr}_1^n(\lambda x)}$$
$$= \frac{1}{\sqrt{p^{n+m}}} \sum_{\underline{u} \in V_{p^k}^e} F_M(\underline{u}) \sum_{x \in F_{p^n}} \omega^{\mathrm{tr}_k^n(L(x)\cdot \underline{u}^T)} \times \omega^{-\mathrm{tr}_1^n(\lambda x)}.$$

선형 사상 $L(x)$의 수반식(adjoint)으로부터 다음

을 얻을 수 있다.

$$\mathrm{tr}_1^k(L(x)\cdot \underline{u}^T)=\mathrm{tr}_1^k(\mathrm{tr}_k^n(xL^*(\underline{u}))).$$

그러므로 함수 $f(L(x))$의 trace 변환은 아래와 같이 다시 쓸 수 있다.

$$F_M(\lambda) = \frac{1}{\sqrt{p^{n+m}}} \sum_{\underline{u}\in V_{p^k}^e} F_M(\underline{u}) \times \sum_{x\in F_{p^n}} \omega^{\mathrm{tr}_1^n((L^*(x)-\lambda)x)}.$$

$\lambda=L^*(x)$인 경우 위 식의 두 번째 합이 p^n이고, 그 이외의 경우 0이 되는 것은 자명하다. 그러므로 $\lambda\in \mathrm{range}(L^*)$인 경우 다음을 유도할 수 있다.

$$F(\lambda) = \frac{1}{\sqrt{p^{n+m}}} p^n F_M(\underline{u}),\ \text{when}\ \lambda=L^*(\underline{u})$$
$$= p^{\frac{m}{2}} F_M(\underline{u}).$$

또한, $\lambda\neq \mathrm{range}(L^*)$인 경우 $\lambda=L^*(\underline{u})$를 만족시키는 $\underline{u}$가 $V_{p^k}^e$상에 존재하지 않으므로 $F(\lambda)=0$가 된다. □

이제 선형 사상 $L(x)$의 정의로부터 임의의 $\underline{u}\in V_{p^k}^e$에 대해 다음의 관계식을 얻을 수 있다.

$$L(x)\cdot \underline{u}^T=\mathrm{tr}_k^n(\zeta\sigma x).$$

여기서 $\underline{u}=(u_1, u_2, \cdots, u_e)$이고 $\zeta=\sum_{i=1}^{e}\beta_i u_i$이다. 이 때, $\underline{u}$가 $V_{p^k}^e$상의 모든 원소를 거쳐가는 동안 ζ가 F_{p^m}의 모든 원소를 거친다는 것은 자명하다. 즉, 다음이 성립한다.

$$\{\zeta\,|\,\underline{u}\in V_{p^k}^e\}=F_{p^m}.$$

그러므로 L^*의 치역(range)은 다음과 같다.

$$\mathrm{range}(L^*)=\{\zeta\sigma\,|\,\zeta\in F_{p^m}\}. \qquad (3)$$

정리 3의 증명) $s_\eta(x)$의 trace 변환은 다음과 같이 나타낼 수 있다.

$$\widehat{S_\eta}(\lambda)=\frac{1}{\sqrt{p^n}} \sum_{x\in F_{p^n}} \omega^{f(L(x))-\mathrm{tr}_1^n((\lambda-\eta\sigma-\delta)x)}.$$

보조정리 1를 이용하여 위의 trace 변환을 아래와 같이 계산할 수 있다.

$$\widehat{S_\eta}(\lambda)=\begin{cases} p^{\frac{m}{2}} F_M(\underline{u}), & \text{for } \lambda-\eta\sigma-\delta\in \mathrm{range}(L^*) \\ & :L^*(\underline{u})=\lambda-\eta\sigma-\delta, \\ 0, & \text{for } \lambda-\eta\sigma-\delta\notin \mathrm{range}(L^*). \end{cases}$$

단, 위 식에서 $F_M(\underline{u})$는 $f(x)$의 변형된 trace 변환이다. (3)식으로부터 L^*의 치역은 아래와 같은 특성을 갖는다.

$$\mathrm{range}(L^*) = \{\zeta\sigma\,|\,\zeta\in F_{p^m}\}+\eta\sigma+\delta$$
$$= \{\zeta\sigma\,|\,\zeta\in F_{p^m}\}+\delta$$
$$= \mathrm{range}(L^*)+\delta$$
$$= \{\zeta\sigma+\delta\,|\,\zeta\in F_{p^m}\}.$$

이제 집합 H가 아래와 같이 정의된다고 하자.

$$H=\mathrm{range}(L^*)+\eta\sigma+\delta=\{\zeta\sigma+\delta\,|\,\zeta\in F_{p^m}\}.$$

그러면 집합 H는 수열군 S에 속한 모든 수열에 대해 같아진다.

$w\in F_{p^m}$에 대해서 방정식 $x^2+x+w=0$가 $\sigma_0\in F_{p^n}\backslash F_{p^m}$인 σ_0를 근으로 갖고, σ_0는 F_{p^m}상에서 F_{p^n}을 생성시킨다는 것은 잘 알려진 사실이다. 즉 다음이 성립한다.

$$F_{p^n}=\{\phi\sigma_0+\psi\,|\,\phi,\psi\in F_{p^n}\}.$$

그러므로 α^τ는 $\alpha^\tau=\phi\sigma_0+\psi$로 대신 할 수 있다. 이제 $H\bigcap H\alpha^\tau$의 원소인 z를 다음과 같이 나타낼 수 있다.

$$z=\zeta_1\sigma_0+\delta.$$

이를 이용하여 다음을 얻을 수 있다.

$$z = \alpha^\tau(\zeta_2\sigma_0+\delta)$$
$$= (\phi\sigma_0+\psi)(\zeta_2\sigma_0+\delta)$$
$$= \phi\zeta_2\sigma_0^2+(\phi\delta+\psi\zeta_2)\sigma_0+\psi\delta$$
$$= (-\phi\zeta_2+\phi\delta+\psi\zeta_2)\sigma_0$$
$$+\psi\delta-\phi\zeta_2 w.$$

이러한 식의 표현의 유일성으로부터 아래와 같은 결론을 얻을 수 있다.

$$\zeta_1 = -\phi\zeta_2+\phi\delta+\psi\zeta_2,$$
$$\delta = \psi\delta-\phi\zeta_2 w.$$

이 때, $\phi\neq 0$이면 두 번째 식은 ζ_2에 대하여 풀리게 되어서 첫 번째 식에서의 ζ_1의 값을 구할 수 있다. 그러므로 $\phi\neq 0$인 경우 $|H\bigcap H\alpha^\tau|=1$이 성립한다. 또한, $\phi=0$인 경우 $\delta\neq 0$이므로 근

이 존재하려면 ϕ는 1이어야만 한다. 즉, $\alpha^{\tau}=1$이 되어야 하는데 이는 α가 원시원이고 $0<\tau<p^n-2$라는 가정에 모순이 된다. 따라서 $\phi=0$이면 $|H\bigcap H\alpha^{\tau}|=0$이 된다. 그러므로 $1\le\tau\le p^n-2$와 F_{p^n}의 원시원 α에 대해 다음이 성립함을 증명하였다.

$$|H\bigcap H\alpha^{\tau}|\le 1. \tag{4}$$

또한 본 논문에서는 $F_M(\underline{u})$가 그 값으로 $+1$과 -1만을 취한다고 가정하였으므로 수열 $s_\eta(x)$의 trace 변환은 아래와 같이 주어진다.

$$\widehat{S}_\eta(\lambda)=\begin{cases}0, & \text{for } \lambda\notin H\\ \pm p^{\frac{m}{2}}, & \text{for } \lambda\in H.\end{cases} \tag{5}$$

또한 (1)에 속하는 수열 $s_{\underline{y}}(x)$와 $s_{\underline{z}}(x)$간의 상관값은 다음과 같이 쓸 수 있다.

$$R_{yz}(\tau)=-1+\sum_{x\in F_{p^n}}\omega^{s_{\underline{y}}(x)-s_{\underline{z}}(x\alpha^{\tau})}.$$

이제 정리 3을 다음의 두 가지 경우로 나누어 증명 할 것이다.

i) $\tau\neq 0$

Parseval의 정리와 F_{p^n}상의 원소 x로 나타낸 수열의 표현을 이용하면 상관함수는 다음과 같이 다시 쓸 수 있다.

$$R_{yz}(\tau)=-1+\sum_{\lambda\in F_{p^n}}\widehat{S}_{\underline{y}}(\lambda)\ \ \widehat{S}^{*}_{\underline{z}}(\lambda\alpha^{\tau}).$$

(4)와 (5)로부터 상관 함수는 다음과 같이 유도할 수 있다.

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

ii) $\tau=0$ and $\underline{y}\neq\underline{z}$

이 경우 $\eta=\sum_{i=1}^{e}\beta_i(y_i-z_i)\neq 0$이므로, 상관함수는 다음과 같이 나타낼 수 있다.

$$\begin{aligned}R_{yz}(0) &= \sum_{t=0}^{p^n-2}\omega^{\mathrm{tr}_1^k(L(\alpha^t)\cdot(\underline{y}-\underline{z})^T)}\\ &= \sum_{t=0}^{p^n-2}\omega^{\mathrm{tr}_1^n(\eta\sigma\alpha^t)}\\ &= -1.\end{aligned}$$

그러므로 수열군 S의 상관특성에 대한 증명이 되었다. □

이제 정리 1에서 정의된 F_{p^m}상의 p진 bent함수를 이용하면 p진 bent 수열 역시 다음과 같이 생성할 수 있다.

정리 4 : $n=2m$이고 $m=2k$ 또는 $2k+1$, $a_i\in F_p$이라 하자. 또한 $\sigma\in F_{p^n}\backslash F_{p^m}$이고 $\eta\in F_{p^m}$, $\delta\in F^{*}_{p^m}$라 하자. 이 경우 (2)에서 정의된 F_{p^m}에서 F_p로의 quadratic p진 bent 함수 $f(\cdot)$는 다음과 같이 주어진다.

$$f(\underline{x})=\mathrm{tr}_1^m\left(\sum_{i=0}^{k}a_i x^{1+p^i}\right).$$

이 때, p진 bent 수열군은 아래와 같이 정의된다.

$$S=\{s_\eta(t)\,|\,\eta\in F_{p^m},\ 0\le t\le p^n-2\}$$

$$\begin{aligned}s_\eta(t) &= \mathrm{tr}_1^m\left(\sum_{i=0}^{k}a_i[\,tr_m^n(\sigma\alpha^t)]^{1+p^i}\right)\\ &\quad+\mathrm{tr}_1^n((\eta\sigma+\delta)\alpha^t).\end{aligned}$$

□

Kumar와 Moreno에 의해 정의된 p진 bent 수열 [3]을 이용하여 Moriuchi와 Imamura는 다음과 같이 주어지는 균형성과 최적의 상관특성을 갖는 p진 수열군을 제시하였다.

$$\begin{aligned}s_\eta(t) &= \mathrm{tr}_1^k(b[\,\mathrm{tr}_k^n(\sigma\alpha^t)]^{p^{kr}+1})\\ &\quad+\mathrm{tr}_1^n((\eta\sigma+\delta)\alpha^t).\end{aligned}$$

그러나 위의 수열은 정리 3에서 정의된 일반화된 p진 bent 수열의 특별한 경우로 $f(\cdot)$가 Kumar와 Moreno가 제시한 p진 bent 수열인 경우이다.

수열의 주기가 커짐에 따라서 정리 2에서 정의한 p진 bent 수열의 항의 수가 늘어나는 것은 자명한 일이지만, 정리 3에서 정의한 수열의 경우에는 그렇지 않다. 또한 이진 bent 수열의 경우 n이 4의 배수인 경우에만 존재하는 것으로 알려져 있으나 p진 bent 수열의 경우 모든 짝수 n에 대해 존재한다.

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. Dillion, "Elementary Hadamard difference sets," Ph.D. dissertation, University of Maryland, 1974.

[3] P.V. Kumar and O. Moreno, "Prime-phase sequences with periodic correlation properties better than binary sequences," *IEEE Trans. Inform. Theory*, vol. 37, pp. 603-616, May 1991.

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

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

[6] T. Moriuchi and K. Imamura, "Balanced nonbinary sequences with good periodic correlation properties obtained from modified Kumar-Moreno sequences," *IEEE Trans. Inform. Theory*, vol. 41, pp. 572-576, Mar. 1995.

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

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

[9] L.R. Welch, "Lower bounds on the maximal cross correlation of signals," *IEEE Trans. Inform. Theory*, vol 20, pp. 396-399, May 1976.

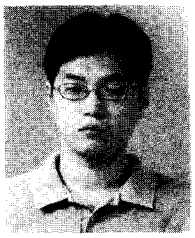
[10] Young-Sik Kim, Ji-Woong Jang, Jong-Seon No, and Tor Helleseth, "On p-ary Bent Functions Defined on Finite Fields," *Mathematical Properties of Sequences and Other Combinatorial Structures, The Kluwer International Series in Engineering and Computer Science*, Kluwer Academic Publishers, pp. 65-76, 2003.

김 영 식(Young-Sik Kim) 준회원

2001년 2월 : 서울대학교 전기공학부 공학사
2003년 2월 : 서울대학교 전기컴퓨터공학부 석사
2003년 3월~현재 : 서울대학교 전기컴퓨터공학부 박사과정

<주관심분야> 시퀀스, 오류정정부호, 디지털통신

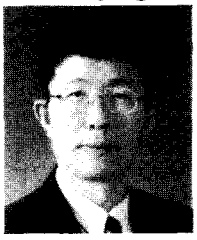
장 지 웅(Ji-Woong Jang) 준회원



2000년 2월 : 서울대학교 전기공학부 공학사
2002년 2월 : 서울대학교 전기컴퓨터공학부 석사
2002년 3월~현재 : 서울대학교 전기컴퓨터공학부 박사과정

<주관심분야> 시퀀스, 오류정정부호, 디지털 통신

노 종 선(Jong-Seon No) 종신회원



1981년 2월 : 서울대학교 전자공학과 공학사
1984년 2월 : 서울대학교 대학원 전자공학과 석사
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 전기컴퓨터공학부 부교수

<주관심분야> 시퀀스, 오류정정부호, 시공간부호, 암호학, 이동통신