通信情報保護學會誌
第2卷 第3號, 1992. 9

Bent함수와 bent 수열을 중심으로 본 상관성이 우수한 수열군

정 하 봉*

레이다 시스템, ranging 시스템, 확산 대역 통신(spread spectrum communication) 시스템, 그리고 요즈음 각광받고 있는 코드분할방식 다중통신(CDMA com- munication) 시스템에서는 주지하다시피 상관성(correlation property)이 좋은 수열(sequence)들의 사용이 필수 불가결하다. 수열의 상관성은 그 수열 자신의 상관성이냐 다른 수열 간의 상관성이냐에 따라 자기상관관계(autocorrelation)와 교차상관관계 (crosscorrelation)로 나누어 생각할 수 있고 수열의 주기성의 유무에 따라 주기적 상관관계(periodic correlation)와 비주기적 상관관계(aperiodic correla- tion)로 나누어 볼 수 있다. 여기서 수열의 상관성이 좋다는 말은 정규화된 수열의 자기상관 계수(autocorrelation coefficient)와 수열 간의 교차상관 계수 (crosscorrelation coefficient)의 최대 크기가 수열의 길이에 비해 상대적으로 작은 값을 갖는다는 것을 의미한다. 본 논문에서는 주기성을 갖는 이진 수열군의 하나인 bent 수열과 이 bent 수열을 구성하는데 기본이 되는 bent 함수를 중심으로 주기적 상관성이 우수한 여러 수열군에 대해 알아보고자 한다.

1. 수열의 상관관계

확산 대역 통신 시스템의 확산 수열(spreading sequence)이나 CDMA통신 시스템에서의 서명 수열(signature sequence)로 쓰이는 수열, 또는 수열군이 가져야 할 여러가지 성질 중에 가장 중요한 성질의 하나가 수열의 상관성이 우수해야 한다는 것이다. 여기서 수열의 상관성이 우수하다는 말은 정규화된 수열의 자기상관 계수(autocorrelation coefficient)와 수열 간의 교차상관 계수(crosscorrelation coefficient)의 최대 크기가 수열의 길이에 비해 상대적으로 작은 값을 갖는다는 것을 말하며 상관성이 우수한 수열은 동기화(synchronization)가 쉽고 또 그러한 수열간에는 간섭(interference) 현상이 극소화되게 된다. 한편 수열의 상관관계는 수열의 주기성의 유무에 따라 주기적 상관관계와 비주기적 상관관계로 나눌 수 있다. 각 경우에 해당하는 상관 계수들은 다음과 같이 정의할 수 있다.

정의 1 : 주기가 N인 수열 $x(t)$, $t=0,1,2,\cdots,N-1$, 의 주기적 자기상관 계수 $P_x(\tau)$는 임의의 정수 τ에 대해 다음과 같이 정의한다.

$$P_x(\tau) \triangleq \sum_{t=0}^{N-1} x(t)x^*(t\oplus\tau) \qquad (1)$$

정의 2 : 주기가 N인 수열 $x(t)$와 $y(t)$, $t=0,1,2,\cdots,N-1$, 의 주기적 교차상관 계수 $P_{x,y}(\tau)$는 임의의 정수 τ에 대해 다음과 같이 정의한다.

$$P_{x,y}(\tau) \triangleq \sum_{t=0}^{N-1} x(t)y^*(t\oplus\tau) \qquad (2)$$

* 홍익대학교 공과대학 전자공학과 조교수

정의 3 : 길이가 N인 비주기 수열 $x(t)$, $t=0, 1, 2, \cdots, N-1$, 의 비주기적 자기상관 계수 $C_x(\tau)$는 $-N+1 \le \tau \le N-1$인 정수 τ에 대해 다음과 같이 정의한다.

$$C_x(\tau) \triangleq \sum_{t=\max(0,-\tau)}^{\min(N-1,N-1-\tau)} x(t)x^*(t+\tau) \qquad (3)$$

정의 4 : 길이가 N인 비주기 수열 $x(t)$와 $y(t)$, $t=0, 1, 2, \cdots, N-1$, 의 비주기적 교차상관 계수 $C_{x,y}(\tau)$는 $-N+1 \le \tau \le N-1$인 정수 τ에 대해 다음과 같이 정의한다.

$$C_{x,y}(\tau) \triangleq \sum_{t=\max(0,-\tau)}^{\min(N-1,N-1-\tau)} x(t)y^*(t+\tau) \qquad (4)$$

위의 정의들에서 $\oplus$는 addition modulo N을 의미하며 $*$는 공액 복소수를 의미한다.

수열 또는 수열군의 상관성의 우열을 주기적 상관계수로 가름하느냐 비주기적 상관계수로 가름하느냐는 그 수열이 응용되는 분야에 따라 달라질 수 있다. 확산 대역 통신 시스템이나 CDMA통신 시스템에서는 일반적으로 주기성을 갖는 수열들이 사용되므로 여기서도 수열의 주기적 상관관계 만을 다루도록 한다. 식(1)로 부터 정규화된 수열, 즉 $|x(t)|=1$인 수열의 $P_x(0)$는 항상 수열의 길이(N)와 같게 된다. 따라서 자기상관 계수의 크기를 말할 때는 자동적으로 $\tau \neq 0$ 일 때를 의미하고 $\tau \neq 0$ 인 자기상관 계수의 최대 크기가 N에 비해 상대적으로 작다는 것은 그 수열의 동기를 잡기가 그 만큼 용이하다는 것을 의미하게 되어 이 성질은 레이다 시스템이나 ranging 시스템, 그리고 확산 대역 통신 시스템 등에의 응용에 있어 중요한 성질이 된다. 또한 한 수열군 내의 수열 간의 교차상관 계수의 최대 크기가 작다는 것은 각 수열간의 간섭현상이 상대적으로 작다는 것을 의미하게 되며, 따라서 이 성질은 CDMA 통신 시스템등에서의 중요한 성질이 된다. 일반적으로 M개의 수열을 포함하는 수열군의 상관성의 우열은 $\tau \neq 0$ 인 경우의 자기상관 계수의 최대 크기인 P_a 와 수열군 내의 수열간의 교차상관 계수의 최대 크기인 P_c 의 값으로 나타내게 되고 이들 간의 관계식은 다음처럼 나타낼 수 있다[1].

$$\left(\frac{P_c^2}{N}\right) + \frac{N-1}{N(M-1)}\left(\frac{P_c^2}{N}\right) \ge 1 \qquad (5)$$

실제로 많은 경우에는 수열군이 갖는 상관성이 우열을 나타내는 지표로 P_a 와 P_c 의 최대값인 $P_{\max}$가 사용된다. 식(5)를 변형시키면 $P_{\max}$에 대해 다음 식을 얻을 수 있다.

$$P_{\max} = \max(P_a, P_c) \ge N\left[\frac{M-1}{NM-1}\right]^{\frac{1}{2}} \qquad (6)$$

식(6)을 좀더 자세히 알아보자. 임의의 수열군이 가질 수 있는 $P_{\max}$ 의 가능한 최소값에 대해서는 Welch[2]와 Sidelnikov[3]에 의해 다음과 같은 bound가 알려져 있다.

정리 1(Welch) : 길이가 N인 정규화된 임의의 복소수 수열(complex-valued sequence) M개의 집합이 있을 때 이 집합의 $P_{\max}$는 모든 양의 정수 k에 대해 다음 식을 만족한다.

$$P_{\max}^{2k} \ge \frac{1}{NM(NM-1)}\left\{\frac{N^{2k}(NM)^2}{\binom{k+N-1}{N-1}} - MN^{2k+1}\right\} \qquad (7)$$

정리 2(Sidelnikov) : p를 임의의 소수(素數)라고 하고 w를 1의 p 乘根이라 하자. 길이가 N이고 수열의 각 값이 w^i으로 주어지는 수열 M개로 이루어진 집합이 있을 때 이 집합의 $P_{\max}$는 양의 정수 k에 대해 다음 식을 만족한다.

(1) $p=2$인 경우, 모든 양의 정수 k에 대해

$$C_{\max}^2 > \frac{k+1}{2}(2N-k) - \frac{2^k N^{2k+1}}{M(k!)^2\binom{2N}{k}} \qquad (8)$$

(2) $p>2$인 경우, $0 \le k \le (2N/5)$인 정수 k에 대해

$$C_{\max}^2 > (2k+1)(N-k) + \frac{k(k+1)}{2} - \frac{2^k N^{2k+1}}{M(2k!)^2\binom{N}{k}} \qquad (9)$$

특히 수열이 ± 1의 값을 갖는 이진 수열인 경우, 수열 $x(t)$의 한 주기가 α개의 $+1$과 $(N-\alpha)$개의 -1로 구

성되어 있다면 자기상관 계수 $P_x(\tau)$는 다음 식을 만족하게 되며

$$\sum_{\tau=0}^{N-1} P_x(\tau) = \sum_{\tau=0}^{N-1} P_x(\tau) \sum_{t=0}^{N-1} x(t\oplus\tau)x(t) = (2\alpha - N)^2 \quad (10)$$

따라서 $\tau \neq 0$인 경우의 자기상관 계수의 최대 크기인 P_a는 다음 식을 만족하게 된다.

$$P_a \geq \frac{|N^2-(2\alpha-1)N+4\alpha^2|}{N-1} \quad (11)$$

수열의 자기 상관성이 우수한 대표적인 이진 수열로는 m-sequence를 예로 들 수가 있다. 이 m-sequence는 다음 절에서 언급할 상관성이 좋은 여러 수열군의 기본이 되므로 좀더 자세히 알아 보기로 하자. 원소의 갯수가 2^n개인 Galois field를 GF(2^n)로 표시할 때 GF(2^n) 상에서 정의되는 Trace함수 $\mathrm{tr}_1^n(x)$: GF(2^n)→GF(2)는 다음과 같이 정의된다.

$$\mathrm{tr}_1^n(x) \triangleq \sum_{i=0}^{n-1} x^{2^i} \quad (12)$$

α를 GF(2^n)의 임의의 원시 원소(primitive element)라고 하자. 길이가 2^n-1인 m-sequence $m(t)$, $t=0,1,2,\cdots,2^n-2$는 다음과 같이 나타낼 수 있다.

$$m(t) = \mathrm{tr}_1^n(\alpha^{t+i}) \quad (13)$$

이때 m-sequence 의 자기상관 계수들은 다음과 같은 값을 가지며

$$P_m(\tau) = \begin{cases} N & \text{if } \tau = 0 \\ -1 & \text{if } \tau \neq 0 \end{cases} \quad (14)$$

이는 식(11)로 부터 볼때, 길이가 $N=2^n-1$인 수열이 가질 수 있는 가장 우수한 상관성에 해당한다.

2. 상관성이 우수한 수열들

식(5)~(9)는 주어진 $P_{\max}$하에서의 길이가 N인 수열군의 크기 M의 상한 한계를 나타내는 식으로도 볼 수 있다. 주어진 길이(N)와 $P_{\max}$값에 대해 가능한 최대갯수(M)의 수열을 포함하는 수열군을 최적 수열군(optimal set of sequences)라고 할때 다음 표 1[6]에서는 대표적인 이진(+1, -1) 최적 수열군들을 볼 수 있다.

앞서 언급했듯이 표 1의 Kasami 수열군과 Gold 수열군을 구성하는데 기본이 되는 수열은 m-sequence 이다. 길이가 $N=2^n-1$인 Gold 수열군 $G(u,v)$는 최대상관 계수 $P_{\max}$가

$$P_{\max} = P_a = P_c = 1+2^{\lfloor (n+2)/2 \rfloor} \triangleq t(n) \quad (15)$$

을 만족하는 $(N+2)$개의 수열로 구성되어 있다. 이 $(N+2)$개의 수열중 두개는 교차상관 계수가 -1, $-t(n)$, $t(n)-2$의 3개의 값만을 갖는 선호쌍(preferred pair) m-sequence 인 u와 v이고 나머지 N개는 위의 두 수열중 한 m-sequence인 u에 두번째 m-sequence v의 선형이동(linear shift)을 매이동치($i=0, \cdots, N-1$)마다 더해준 수열이다. 즉 Gold 수열군 $G(u,v)$는

$$G(u,v) = \{u, v, u\oplus v, u\oplus Tv, u\oplus T^2v, \cdots, u\oplus T^{N-1}v\} \quad (16)$$

표 1. 최적 수열군의 비교표

수열군	주기	n	수열군의 크기	$P_{\max}$	최대 Linear span
Gold	2^n-1	2m + 1	2^n+1	$1+2^{m+1}$	$2n$
Gold	2^n-1	4m + 2	2^n+1	$1+2^{2m+2}$	$2n$
작은 Kasami	2^n-1	2m	$2^{n/2}$	$1+2^m$	$3m$
큰 Kasami	2^n-1	4m + 2	$2^{n/2}\cdot(2^n+1)$	$1+2^{2m}$	$5(m+1)$
Bent	2^n-1	4m	$2^{n/2}$	$1+2^{2m}$	$2m\cdot {}_mC_{2m}$
No	2^n-1	2m	$2^{n/2}$	$1+2^m$	$m\cdot 2^{m-1}$

로 구성되어 있다. 윗식에서 $T^i v$는 수열 v를 *i-bit* 만큼 선형 이동한 수열을 의미한다.

작은 Kasami 수열군 $K_s(u)$에는 $2^{n/2}$개의 수열이 있고 길이가 2^n-1(n은 짝수)인 그들은 길이가 2^n-1인 *m-sequence* u와 길이가 $2^{n/2}-1$인 m-sequence w로부터 다음과 같이 구성된다.

$$K_s(u)=\{u,\ u\oplus w,\ u\oplus Tw,\ u\oplus T^2w,\ \cdots,\ u\oplus T^{2^{n/2}-2}w\} \quad (17)$$

큰 Kasami 수열군은 Gold 수열군과 작은 Kasami 수열군을 모두 포함하는 수열군으로 자세한 내용은 [4]를 참조할 수 있다.

이상의 수열군들은 기본적으로 m-sequence를 바탕으로 구성되었기 때문에 비교적 간단하게 수열들을 만들 수 있으나 반면 그런 이유로 해서 linear span [5]이 비교적 작은 값이 된다는 단점이 있다. 주기적 이진 수열의 linear span이란 그 수열을 shift register의 선형귀환(linear feedback) 회로로 발생시킬 경우, 필요한 최소의 shift register의 갯수를 의미한다. 따라서 도청자가 그 수열을 완벽히 재구성하기 위해서는 linear span의 두배 정도의 연속된 수열 bit만을 알면 되므로 linear span이 작다는 것은 정보보호의 측면에서 그만큼 단점이 되는 것이다. 일반적으로 finite field에 근거한 $x(\alpha^t), t=0,1,\cdots,$라는 형태를 갖는 수열의 linear span은 $x(\alpha^t)$를 α^t의 다항식으로 전개했을 때의 그 다항식의 항수와 같게 된다[5]. 표 1에서 보는 바와 같이 이러한 linear span의 관점에서 우수한 수열군에는 bent수열군과 No 수열군[6]이 있다. No 수열군[6]은 그 구성의 기본이 되는 수열로 GMW 수열[7]을 이용한다. No 수열군과 GMW 수열의 관계는 작은 Kasami 수열군과 m-sequence와의 관계와 동일하다. 즉 식(17)에서 m-sequence u와 w를 GMW 수열로 대치하면 그 결과가 No 수열군이 된다.

광통신 시스템에서도 상관성이 우수한 수열군을 이용한 CDMA 시스템을 생각할 수 있다. 현재 광통신 시스템의 변조 방식은 on-off keying의 ASK 위주이므로 이 경우 필요한 이진 수열은 (+1, -1) 수열이 아닌 (0, 1) 수열이 된다. 이러한 수열들을 optical orthogonal codes라고 부르며 이에 대한 참고문헌은 [8]~[10]이다. 그외 확산 대역 통신의 frequency hopping pattern 또는 레이다나 sonar pattern 등에 이용되는 수열들은 공간 상관성(spatial correlation)이 좋은 2차원의 수열 행렬[11]로 볼 수 있다. 이는 다시말해 수평축을 시간축, 수직축을 주파수축으로 보아 시간 이동(time-shift)이나 주파수 이동(frequency-shift)된 행렬간의 이차원 상관관계가 우수한 것을 의미한다고 볼 수 있다. 대표적으로 알려진 1차원, 2차원의 이진 수열, 또는 수열군들은 다음 표 2 [13]에 열거되어 있다. 표 2에서 Class I과 III는 주기 수열군을, Class II와 IV는 비주기 수열군을 지칭하며, 동시에 Class I과 III는 (+1, -1) 수열을, Class III와 IV는 (0, 1) 수열을 뜻한다.

표 2. 일차원, 이차원 이진 수열 및 수열 행렬의 분류표

	일차원 수열	이차원 수열 행렬
Class I	m-sequence GMW sequence Gold 수열군 Kasami 수열군 Bent 수열군 No 수열군	
Class II	Barker sequence	Barker array
Class III	Optical Orthoqonal Codes	Ideal matrix
Class IV	Spanning ruler	Costas array Radar array Sonar array

MPSK를 변조 방식으로 하는 CDMA 시스템을 위해서는 상관성이 우수한 非二進 수열이 필요하다. Sidelnikov의 bound식인 (8)과 (9)는 수열군 내의 수열의 갯수 M이 주기 N 이상일 경우 다음과 같이 근사화 될 수 있다[14].

$$C_{\max}^2 > N\left((2u+1)-\frac{1}{(2u-1)!!}\right),\quad p=2 \quad (18)$$

$$C_{\max}^2 > N\left((u+1) - \frac{1}{u!!}\right), \quad p>2 \qquad (19)$$

위의 식(18)에서 $(2u-1)!!$ 는 $1\cdot3\cdot5\cdots(2u-1)$을 의미한다. 식(18)과 (19)는 非二進 수열군의 $P_{\max}$의 performance가 최적 이진 수열의 그것보다 대략 $\sqrt{2}$ 만큼 우수할 수 있다는 것을 의미한다. 이는 CDMA에의 활용이라는 관점에서 볼 때 signal-to-interference의 3 dB의 개선을 의미한다. 지금까지 알려진 우수한 비이진 수열군들을 표3에 열거하였고 이들의 구체적인 구성 방법들은 제5절의 참고 문헌 [14]~[21]에 자세히 언급되어 있다.

표3. 여러가지 非二進 최적 수열군의 비교표

수열군	q	길이	수열군의 크기	$P_{\max}$	비 고
Gp. Char. seq.[16]	L	L	L-2	$L^{3/2}$ / (L-1)	L은 소수
FZC seq.[17]	2L	L	L-1	$L^{1/2}$	L은 소수
4-phase seq.[18]	L	L	L-1	$L^{1/2}$	L은 소수
3-phase seq.[18]	L	L	L	$L^{1/2}$	L은 소수
Sidelnikov[3]	p	$L=p^n-1$	L+1	$1+(L+1)^{1/2}$	p은 소수
Bent [19]	p	$L=p^{2n}-1$	$(L+1)^{1/2}$	$1+(L+1)^{1/2}$	p은 소수
KM seq. [13]	p	$L=p^n-1$	L+1	$1+(L+1)^{1/2}$	p은 소수

3. Bent 수열

1982년 Olsen, Scholtz, Welch[22]는 이진 bent 수열이라 불리우는 일군의 수열들을 고안하였다. 이 bent 수열군 역시 앞의 표1에서 본 바와 같이 최적 수열군 중의 하나이며 더우기 기존에 알려진 다른 최적 수열군들 보다도 훨씬 큰 linear span을 갖는다는 잇점을 가지고 있다. 이 bent 수열군은 이진 bent 함수라고 불리우는 부울함수를 토대로 구성되며 1976년 Rothaus[23]에 의해 처음 명명된 bent 함수는 다음과 같이 정의된다.

정의 5 : V_m을 m-차원 이진 벡타공간이라 하자. m-차원 이진 bent함수 $f(\underline{x}) : V_m \rightarrow V_1$는 다음과 같이 정의된 Fourier계수 $F(\underline{\lambda})$의 크기가 1인 Boole함수이다.

$$F(\underline{\lambda}) = \frac{1}{\sqrt{2^m}} \sum_{\underline{x} \in V_m} (-1)^{f(\underline{x}) - \underline{\lambda}^T \cdot \underline{x}} \qquad (20)$$

부울함수의 특성상 이진 bent함수는 짝수 차원만을 갖는다. 즉 이진 bent 함수가 존재하기 위해서는 함수의 정의구역 V_m에서 m이 짝수여야 한다. 대표적인 이진 bent 함수로는 Rothaus[23]에 의해 소개된 다음과 같은 형태의 함수들이 있다.

$$Q(\underline{x},\underline{y}) = x_1y_1 + x_2y_2 + \cdots + x_ky_k + P(\underline{x}) \qquad (21)$$

이때 x와 y는 각각 $\underline{x}=(x_1, x_2, \cdots, x_k)$, $\underline{y}=(y_1, y_2, \cdots, y_k)$인 V_k상의 점을 의미하며 $P(x)$는 V_k 상의 임의의 함수를 지칭한다. Bent 함수의 여러 성질과 그 응용분야에 관해서는 다음 절에서 다루기로 하고 이 절에서는 bent 수열에 대해서 알아보기로 하자.

길이가 2^n-1인 bent 수열군을 만들기 위해서는 $k=n/2$인 V_k 상의 *bent*함수 $F(\underline{x})$가 필요하게 되고 이진 *bent* 함수는 k가 짝수일 때만 존재하므로 n 값은 4배의 배수이어야 한다. 이 bent 함수 $F(\underline{x})$로 부터 얻어지는 bent 수열군은 다음 식을 만족하는 수열 $S_z(t)$, $t=0,1,\cdots,2^n-2$, 의 집합 S 즉, $S=\{S_z(t) \mid z \in V_k\}$로 주어지며

$$S_z(t) = (-1)^{F(L(\alpha^t)) + L(\alpha^t)^T \cdot z + tr(\sigma\alpha^t)} \qquad (22)$$

이때 σ는 $GF(2^k)$의 한 원소이고 L은 어떤 특정 성질을 만족하는, $GF(2^n)$에서 V_k로 가는 선형 onto

mapping이다. Bent수열의 구성방법에 대한 좀더 자세한 내용은 [22]를 참조하면 된다. [22]에서의 bent 수열은 하나의 bent 함수로 부터 얻어졌으나 Lempel과 Cohn은 [24]에서 여러개의 bent 함수를 이용하여 bent 수열을 얻는 방법을 제시하였고 이렇게 얻어진 bent 수열군의 $P_{\max}$가 표 1에서 본 바와 같이 그 값이 $2^{n/2}+1$이 되기 위해서는 사용된 각 bent 함수들이 pairwise orthogonal, 즉 사용된 임의의 두 bent 함수를 내적했을 때 그 값이 0이 되어야 한다는 것을 보였다.

식(22)에서 볼수 있듯이 bent수열들은 m-sequence의 비선형 함수(nonlinear operation on m-sequence)로 생각할 수 있고 따라서 bent 수열의 linear span 역시 Key[5]의 방법으로 구할 수 있다. Bent 수열의 linear span의 상한값(upper bound)와 가능한 최대 linear span의 하한값(lower bound)은 Kumar와 Scholtz[25]에 의해 밝혀 졌고 이를 정리하면 다음과 같다.

$$L \le \sum_{i=1}^{d}\binom{n}{i} + \binom{m}{d}2^d - \sum_{i=1}^{\lfloor\frac{d-1}{2}\rfloor}\binom{m}{i} \qquad (23)$$

$$L_d \ge n + \binom{m}{d}2^d + \sum_{i=2}^{d-1}\binom{m}{i}2^{i-1}, \quad d>2 \qquad (24)$$

위에서 L과 L_d는 각각 차수가 d인 m차원 bent 함수로 부터 얻어진 bent 수열의 linear span과 최대 가능한 linear span을 의미한다.

Bent 수열이 가진 또 하나의 특징은 수열 내의 +1과 −1의 갯수가 같다는 점이다(엄밀히는 수열의 길이가 홀수이므로 하나의 차이가 있다). 많은 응용 분야에서, 사용되는 수열들이 되도록 무작위성(pseudo-randomness)을 갖는 것이 유리하다는 점에서 이 balancedness 성질은 bent 수열이 가진 또 하나의 정점이다.

4. Bent 함수의 성질

이 절에서는 이진 bent 함수와 그것을 확장한 多進 bent 함수의 성질 및 응용범위에 대해서 알아보자.

이진 bent 함수의 가장 대표적인 성질은 이 함수가 Hadamard difference set의 특성함수(characteristic function)가 된다는 점이다. 즉, $P(x)$가 V_m상의 bent 함수이면 $H=(-1)^{P(x+y)}$로 주어지는 $(2^m\times 2^m)$ 행렬 H는 Hadamard 행렬이 되고 즉, $HH^t=2^mI$이고 그 역도 성립한다. Bent 함수로 나타낼 수 있는 Hadamard difference set에 관해서는 Dillon의 [26]에 잘 나타나 있다.

앞에서도 언급했듯이 bent 함수가 존재할 수 있는 벡터 공간 V_m은 $m=2k$인 짝수일 때 만이다. 그리고 이때 bent 함수의 최대 차수는 k를 넘을 수 없다는 것이 알려져 있다. Rothaus[23]는 이러한 성질로 부터 이진 bent 함수가 가질 수 있는 두개의 커다란 일반적 형태에 대하여 알아내었다. 그러나 이진 bent 함수의 완전한 classification은 아직도 해결되지 않은 주요 연구과제이다.

Bent 함수가 Hadamard difference set의 특성함수라는 성질은 또 다른 각도에서 해석될 수 있다. 이는 선형 부울함수들로 부터 가장 멀리 떨어져 있는 부울함수, 다시 말해 어떤 부울함수에서 개개 선형 부울함수들을 각각 빼준 함수 집합에서 각 원소의 Hamming weight의 최소값이 최대가 되는 함수가 바로 bent 함수라는 것이다(Bent라는 이름도 이런 시각에서 연유된 것으로 생각된다). 이진 bent 함수의 이러한 성질은 오류 정정부호(Error-correcting codes)에서도 응용된다. 즉 bent 함수는 1차 Reed-Muller code의 coset중 coset leader의 weight가 최대인 coset에 해당하고 이러한 성질을 이용, bent 함수는 비선형 Kerdock code를 만드는 데 사용되기도 한다[27].

이진 bent 함수가 이진 bent 수열의 구성에 이용되었듯이 다진(m-ary)bent 수열을 만들기 위해서는 bent 함수의 일반화, 즉 m-ary bent 함수의 고안이 필요하다. 이러한 목적으로 이진 bent 함수를 일반화한 것을 일반 bent 함수(generalized bent function)라 부르며 이는 1985년 Kumar, Scholtz, Welch [28]에 의해 처음 정의되었다.

정의 6 : V_q^m을 m-차원 q-ary 벡타공간이라 하자. w를 1의 q승근이라 할 때 m-차원 q-ary bent 함수 $f(\underline{x}) : V_q^m \to V_q^1$는 다음과 같이 정의된 Fourier 계수 $F(\underline{\lambda})$의 크기가 1인 함수이다.

$$F(\underline{\lambda})=\frac{1}{\sqrt{q^m}}\sum_{\underline{x}\in V_q^m}\omega^{f(\underline{x})-\underline{\lambda}^T\cdot\underline{x}} \quad (25)$$

이진 bent 함수와 마찬가지로 q-ary bent 함수 $f(\underline{x}): V_q^m \rightarrow V_q^1$ 역시 Hadamard 행렬로 특성지어진다. 즉, $f(\underline{x})$가 V_q^m 상의 bent 함수일 때 (x,y) 성분이 $\omega^{f(x-y)}$로 주어지는 matrix H는 $HH^*=q^mI$인 Hadamard 행렬이 된다. 일반 bent 함수가 이진 bent 함수와 다른 점은 이진 bent 함수는 정의구역인 V_m에서 m이 짝수일 때만 존재하나 일반 bent 함수의 경우 m값의 제한이 없다는 점이다. 특히 $m=1$인 V_q^1 상의 일반 bent 함수는, V_q^m, V_q^n 상의 bent 함수로부터 쉽게 V_q^{m+n}상의 함수를 만들 수 있다는 성질로 인해 그 구성 및 classification이 주요 연구 대상이다.

V_q^1 상의 q-ary bent 함수 $f(t)$, $t\in Z_q$, 는 다음 식을 만족하므로

$$\sum_{t=0}^{q-1}\omega^{f(t\oplus\tau)-f(t)}=0 \quad (26)$$

ω를 1의 q승근이라 할때 $\omega^{f(t)}$자체는 주기가 q인, 완벽한 자기상관성을 갖는 q-ary 수열로 볼 수 있다[29]. 이 성질로 인해 일반 bent 함수는 다진(q-ary) bent 수열의 구성 이외에도 frequency-hopping pattern이나 radar, sonar pattern 등에 쓰이는 상관성이 우수한 이차원 수열행렬의 고안에도 이용되고 있다[12].

최근에는 비화(cryptographic) 시스템에 쓰이는 data 암호 표준(DES)의 S-box에 대한 연구[30]로 인해 bent 함수가 다른 각도에서 조명받고 있다. 즉, S-box의 내부 변환함수가 선형구조를 가지면 밖으로부터의 공격(attack)에 약하게 되고 이런 관점에서 보면 선형 부울함수로부터 가장 멀리 떨어진 이진 bent 함수는 소위 완전 비선형(perfect nonlinear) S-box의 내부 변환함수로서의 일차적 조건을 만족한다고 볼 수 있다[31]. 단, 이진 bent 함수를 내부 변환함수로 채택한 S-box의 경우는 이진 bent 함수의 성질상 출력의 bit 수가 입력 bit 수의 반을 넘을 수 없다는 단점이 있다. S-box가 가져야할 기타 조건들(예를 들어 balancedness)을 만족시키며 더불어 앞의 단점을 효과적으로 극복하기 위해 현재 일반 bent 함수를 이용한 S-box의 구현에 관한 연구가 진행되고 있다.

5. 참 고 문 헌

1. D.V. Sarwate and M.B. Pursley, "Cross-correlation properties of pseudorandom and related sequences," *Proceedings IEEE*, Vol.68, pp.593-618, May 1980.

2. L.R. Welch, "Lower bounds on the maximum crosscorrelation of signals," *IEEE Transactions on Information Theory*, Vol.IT-20, pp.397-399, May 1974.

3. V.M. Sidelnikov, "On mutual correlation of sequences," *Soviet Math. Dokl.*, Vol.12, No.1, pp.197-201, 1971.

4. D.V. Sarwate and M.B. Pursley, "Applications of coding theory to spread spectrum multiple-access communications," *Proceeding 1976 IEEE Canadian Communications and Power Conf.*, pp.72-75, 1976.

5. E.L. Key, "An analysis of the structure and complexity of nonlinear binary sequence generators," *IEEE Transactions on Information Theory*, Vol.22, No.6, pp.723-736, Nov.1976.

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 Transactions on Information Theory*, Vol.35, No.2, pp.371-379, March 1989.

7. R.A. Scholtz and L.R. Welch, "GMW sequences," *IEEE Transactions on Information Theory*, Vol.30, No.3, pp.548-553, May 1984.

8. F.R.K. Chung, J.A. Salehi, and V.K. Wei, "Optical orthogonal codes : Design, analysis, and applications" *IEEE Transactions on Information Theory*, Vol.35, No.3, pp.595-604, May 1989.

9. H. Chung and P.V. Kumar, "Optical orthogonal codes -- New bounds and an optimal

construction," *IEEE Transactions on Information Theory*, Vol.36, No.4, pp.866-873, July 1990.

10. J.A. Salehi and C.A. Brackett, "Code division multiple access techniques in optical fiber networks," *IEEE Transactions on Information Theory*, Vol.37, No.8, pp.834-873, Aug. 1989.

11. S.W. Golomb and H. Taylor, "Two-dimensional synchronization patterns for minimum ambiguity," *IEEE Transactions on Information Theory*, Vol.28, No.4, pp.600-604, July 1982.

12. P.V. Kumar, "On the existence of square dot-matrix patterns having a specific 3-valued periodic correlation function," *IEEE Transactions on Information Theory*, Vol.34, No.2, pp.271-277, March 1988.

13. H. Chung, "New general constructions for (i) Generalized bent functions and (ii) Optical orthogonal codes," Ph.D. Dissertation, University of Southern California, 1988.

14. P.V. Kumar and O. Moreno, "Polyphase sequences with periodic correlation properties better than binary sequences," *IEEE Transactions on Information Theory*, Vol.37, No.3, pp.603-616, May 1991.

15. S. Boztas, R. Hammons, and P.V. Kumar, "4-Phase Sequences with Near-Optimum Correlation Properties," *IEEE Transactions on Information Theory*, Vol.38, No.3, pp.1101-1113, May 1992.

16. R.A. Scholtz and L.R. Welch, "Group characters: Sequences with good correlation properties," *IEEE Transactions on Information Theory*, Vol.24, No.5, pp.537-545, Sep. 1978.

17. D.V. Sarwate, "Bound on cross-correlation and auto-correlation of sequences," *IEEE Transactions on Information Theory*, Vol.25, No.6, pp.720-724, Nov.1979.

18. W.O. Alltop, "Complex sequences with low periodic correlations," *IEEE Transactions on Information Theory*, Vol.26, No.3, pp.350-354, May 1980.

19. P.V. Kumar, "On bent sequences and generalized bent functions," Ph.D. Dissertration, University of Southern California, 1983.

20. H.M. Trachtenberg, "On the cross-correlation functions of maximal recurring sequences," Ph.D. Dissertration, University of Southern California, 1970.

21. I.F. Blake and J.W. Mark, "A note on complex sequences with low correlations," *IEEE Transactions on Information Theory*, Vol.28, No.5, pp.814-816, Sep.1982.

22. J.D. Olsen, R.A. Scholtz, and L.R. Welch, "Bent function sequences," *IEEE Transactions on Information Theory*, Vol.28, No.6, pp.858-864, Nov. 1982.

23. O.S. Rothaus, "On 'bent' functions," *Journal of Combinatorial Theory(A)*, Vol.20, pp.300-305, 1976.

24. A. Lempel and M. Cohn, "Maximal families of bent sequences," *IEEE Transactions on Information Theory*, Vol.28, No.6, pp.865-868, Nov.1982.

25. P.V. Kumar and R.A. Scholtz, "Bounds on the linear span of bent sequences," *IEEE Transactions on Information Theory*, Vol.29, No.6, pp.854-862, Nov.1983.

26. J.F. Dillon, "Elementary Hadamard difference sets," Ph.D. Dissertation, University of Maryland, 1974.

27. F.J. McWilliams and N.J.A. Sloane, "The theory of error-correcting Codes," Amsterdam, The Netherlands: North-Holland, 1977.

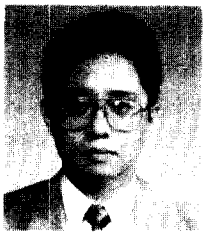
28. P.V. Kumar, R.A. Scholtz, and L.R. Welch, "Generalized bent functions and their properties," *Journal of Combinatorial Theory(A)*, Vol.40, No.1, pp.90-107, Sep.1985.

29. H. Chung and P.V. Kumar, "A new general construction for generalized bent functions," *IEEE Transactions on Information Theory*, Vol.35, No.1, pp.206-209, Jan. 1989.

30. E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," Proceedings of Eurocrypt '90.

31. W. Meier and O. Staffelbach, "Nonlinear criteria for cryptographic functions," Proceedings of Eurocrypt '89, pp. 549-562. Springer 1990.

□ 著者紹介



정 하 봉

1958년생
1981년 2월 서울대학교 공과대학 전자공학과(학사)
1985년 1월 미국 남가주대학(USC) 전기공학과(석사)
1988년 7월 미국 남가주대학(USC) 전기공학과(박사)
1988년 8월~1991년 8월 미국 뉴욕주립대(SUNY Buffalo) 전기공학과 조교수
1991년 8월~현재 홍익대학교 공과대학 전자공학과 조교수
주관심 분야 : 통신이론, 부호이론, 정보이론 등