논문 14-39A-08-02
The Journal of Korea Information and Communications Society '14-08 Vol.39A No.08
http://dx.doi.org/10.7840/kics.2014.39A.8.445

이상적인 자기 상관 특성을 갖는 4진 수열

장 지 웅◆°

Quaternary Sequence with Ideal Autocorrelation Property

Ji-Woong Jang◆°

요 약

본 연구에서는 짝수 주기와 균형성을 갖는 4진 수열에 대하여 이상적인 자기상관특성을 정의하고, 이것이 이상적인 자기상관특성이 됨을 증명하였다. 또한, 주기가 2^n-1인 이상적인 자기 상관 특성을 갖는 이진 수열과 Gray 사상을 이용하여 주기가 $2\times(2^n-1)$인 이상적인 자기 상관 특성을 갖는 4진 수열의 생성법을 제안한다. 또한 새로 제안된 4진 수열의 자기상관 분포도 유도하였다.

Key Words : Sequences, Quaternary sequences, Ideal autocorrelation property, Gray mapping

ABSTRACT

In this paper, we define ideal autocorrelation property for balanced quaternary sequence with even period. We also prove that our definition is ideal autocorrelation property for balanced quaternary sequence with even period. Furthermore, we propose a generation method of quaternary sequence with ideal autocorrelation property of period $2\times(2^n-1)$ using a binary sequence with ideal autocorrelation of period 2^n-1 and Gray mapping. We also derive the autocorrelation value distribution of the newly proposed quaternary sequence.

Ⅰ. 서 론

우수한 자기상관 특성을 갖는 의사 불규칙 수열은 신호처리 및 통신과 같은 여러 디지털 시스템에서 중요한 역할을 하고 있다. 이러한 수열들에 있어 가장 중요한 특성은 동기점 이외에서의 자기 상관값이 작아야 한다는 것이다. 또한, 이진 및 4진 변조를 이용하는 디지털 통신 시스템에 적용하기 용이한 이점 때문에 이진 및 4진 수열이 다른 수열보다 각광을 받고 있다. 이러한 이유로 현재까지 우수한 상관특성을 갖는 이진 및 4진 수열에 대한 다양한 연구가 진행되어 왔다.

$R_{\max}$가 동기점을 제외한 다른 위상에서의 자기상관특성의 최대값이라 하자. $R_{\max}=0$이면 이를 완전자기상관특성이라 한다. 그러나 몇몇 아주 짧은 주기를 제외하면 완전자기상관특성을 갖는 이진 및 4진 수열이 존재하지 않는다는 것이 현재까지의 가설이며, 수많은 모의실험 결과가 이를 뒷받침 하고 있다[1]. $R_{\max}=1$이면 이를 이상적인 자기상관특성이라 하며, 이진 수열에 있어 현재까지 m-수열[2], GMW수열[3] 방정식의 사상수열[4] 등과 같은 수많은 연구 결과가 알려져 있다.

우수한 상관특성을 갖는 4진 수열에 대해서도 다양한 연구 결과들이 제안되어 왔다[1,5-8]. Sidel'nikov는 우수한 상관특성을 갖는 M진 수열을 제안하였다[5]. 이 수열에는 4진 수열이 그 특정 유형으로 포함된다. Schotten의 상보성에 기반한 수열군은 홀수 주기와 우수한 상관특성을 갖는 4진 수열의 생성법이다[1,6,7]. 또한, Luke와 Schotten, Hadineja-Mahram은 짝수 주기

※ 본 연구는 2013년 울산과학대학교 교내학술연구비 지원에 의해 수행되었습니다.
◆° First and Corresponding Author : Ulsan College Department of Information Technology, stasera.jang@gmail.com, 정회원
논문번호 : KICS2014-04-129, Received April 9, 2014; Revised June 17, 2014; Accepted July 16, 2014

에 대하여 $R_{\max}=2$인 4진 수열의 생성법을 제안하였다. 주기가 $N\equiv 2(\mathrm{mod}4)$ 인 경우에는, Lee의 완전 상관특성을 갖는 수열[9]을 이용하여 생성한 인 수열이 존재한다[1]. 이는 현재까지 알려진 순수한 4진 수열 중 자기상관특성이 가장 우수한 수열이다.

본 연구에서는 짝수 주기를 갖는 4진 수열의 이상적 자기 상관특성을 정의하고 이것이 이상적인 자기상관 특성임을 증명한다. 또한, 이상적인 자기상관특성을 갖는 이진 수열과 Gray 사상을 이용하여 주기가 $2\times(2^n-1)$인 이상적인 자기상관특성을 갖는 4진 수열의 생성법을 제안한다. 또한, 새로 제안된 4진 수열의 자기상관 분포도 유도하였다.

이후 본 논문의 구성은 다음과 같다. 우선 2장에서는 논문을 이해하는데 필요한 사전지식들을 설명한다. 3장에서는 4진 수열의 이상적인 자기상관특성을 제안하고 제안된 상관특성이 이상적인 값임을 보인다. 4장에서는 이상적인 자기상관특성을 갖는 4진수열을 제안하고, 마지막 5장에서 결론과 함께 논문을 마무리 한다.

Ⅱ. 사전 지식

이번 장에서는 이후 논문에 이용되는 몇몇 정의와 사전지식들에 대하여 간단히 기술할 것이다. 양의 정수 q와 N에 대하여 $g(t)$가 주기가 N인 q진 수열이라 하자. 또한, 집합 A_k를 다음과 같이 정의한다.

$$A_k=\{t \mid g(t)=k,\ 0\le t<N\},\ k=0,1,\cdots,q-1.$$

이 때, 주기가 N인 4진 수열 $g(t)$가 균형성을 갖는다는 것과 임의의 $i,\ j$에 대하여 $|A_i-A_j|\le 1$이라는 것은 동치이다.

$g(t)$의 자기 상관함수는 다음과 같이 정의된다.

$$R_g(\tau)=\sum_{t=0}^{N-1}\omega_q^{g(t)-g(t+\tau)}$$

단, $0\le\tau<N$이고 ω_q는 q차 원시 단위근이다.

수열이 동기 획득을 위한 사전수열 등으로 통신 시스템에서 이용되기 위해서는 다음과 같은 특성들이 요구된다.

동기점 이외의 위상에서 자기 상관함수값의 최대값이 되도록 작아야 한다.

동기점 이외의 위상에서 자기상관 함수값의 최대값이 나타나는 빈도가 되도록 작아야 한다.

수열의 이러한 성질들은 무선통신 시스템의 동기 획득을 위하여 적용될 때, 잘못된 동기 획득의 확률을 줄여주게 된다. 이제 위의 두 가지 특성을 만족하는 수열을 이상적인 자기상관특성을 갖는 수열로 정의하자. 주기가 홀수인 이진 수열에 있어 이상적인 자기상관특성이 다음과 같은 자기상관분포를 갖는 것은 익히 알려진 사실이다.

$$R_g(\tau)=\begin{cases}N, & \text{once}\\ -1, & N-1\ \text{times}\end{cases}$$

이제 Z_{2^n-1}이 $Z_{2^n-1}=\{0,1,2,\cdots,2^n-2\}$과 같이 2^n-1으로 나눈 잉여류의 집합이라고 하자. 또한, 양의 정수 n에 대해 $s(t)$가 주기가 2^n-1인 이상적인 자기상관특성을 갖는 이진 수열이라 하자. 이 때, $s(t-u)$의 특성 집합 D_u는 다음과 같이 정의된다.

$$D_u=\{t \mid s(t-u)=1,\ 0\le t\le 2^n-2\}=D_0+u$$

단, $u\in Z_{2^n-1}$이고 $D_0+u=\{d+u \mid d\in D_0\}$, "+"는 Z_{2^n-1}하에서의 덧셈이다. $s(t)$의 균형성으로부터 다음이 성립함은 자명하다.

$$|D_u|=2^{n-1},\quad |\overline{D_u}|=2^{n-1}-1.$$

또한, $s(t)$가 이상적인 자기상관특성을 가지므로 $u\ne v$에 대하여 다음이 성립한다.

$$\begin{aligned}|D_u\cap D_v|&=2^{n-2}\\ |D_u\cap\overline{D_v}|&=2^{n-2}\\ |\overline{D_u}\cap D_v|&=2^{n-2}\\ |\overline{D_u}\cap\overline{D_v}|&=2^{n-2}-1.\end{aligned}$$

$u=v$인 경우 다음이 성립한다.

$$\begin{aligned}|D_u\cap D_v|&=2^{n-1}\\ |D_u\cap\overline{D_v}|&=0\\ |\overline{D_u}\cap D_v|&=0\\ |\overline{D_u}\cap\overline{D_v}|&=2^{n-1}-1.\end{aligned}\tag{1}$$

중국인의 나머지 정리에 의하면 동형사상

$$\phi : \zeta \mapsto (\zeta \bmod 2,\ \zeta \bmod 2^n - 1)$$

하에 $Z_{2\times(2^n-1)} \cong Z_2 \otimes Z_{2^n-1}$로 나타낼 수 있으므로, 이후 편의상 $\zeta \in Z_{2\times(2^n-1)}$와 $(\zeta \bmod 2, \zeta \bmod 2^n - 1)$를 동일한 의미로 사용한다.

이제 $\phi[a,b]$를 다음과 같이 정의되는 Gray 사상이라 하자.

$$\phi[a,b] = \begin{cases} 0, & \text{if } (a,b) = (0,0) \\ 1, & \text{if } (a,b) = (0,1) \\ 2, & \text{if } (a,b) = (1,1) \\ 3, & \text{if } (a,b) = (1,0). \end{cases}$$

이 때, 주기가 N인 두 이진수열 $a(t)$, $b(t)$와 주기가 N이 4진 수열 $q(t) = \phi[a(t), b(t)]$에 대하여 다음이 성립함은 잘 알려진 사실이다[8].

$$\omega_4^{q(t)} = \frac{1+\omega_4}{2}(-1)^{a(t)} + \frac{1-\omega_4}{2}(-1)^{b(t)}. \qquad (2)$$

Ⅲ. 4진 수열의 이상적인 자기상관특성

이번 장에서는 4진 수열의 이상적인 자기상관특성에 대하여 논의한다.

양의 정수 q와 N에 대해, $s_q(t)$가 주기가 N인 q진 수열이라 하자. 이 때, q진 수열 $s_q(t)$의 균형성은 다음 정의와 같이 정의된다.

정의 1: 양의 정수 q와 N에 대해, $s_q(t)$가 주기가 N인 q진 수열이라 하자. 이제 $0 \le t \le N-1$에 대하여 c_i, $i = 0,1,\cdots,q-1$를 다음과 같이 정의하자.

$$c_i = |\{t \mid s_q(t) = i,\ 0 \le t < N\}|.$$

q진 수열 $s_q(t)$가 균형성을 갖는다는 것은 c_i가 다음을 만족하는 것임은 잘 알려진 사실이다.

$$\max\{c_i\} - \min\{c_i\} \le 1$$

단, $\max\{c_i\}$와 $\min\{c_i\}$는 $i = 0,1,\cdots,q-1$에 대해 각각 c_i의 최대값과 최소값이다.

균형성은 문자열의 크기 및 주기와 문자열의 관계에도 영향을 받게 된다. 수열의 주기 $N \equiv 2 \bmod 4$인 4진 수열이 균형성을 갖는 경우, 수열의 한 주기를 더한 무게합(weight sum)은 다음 사전정리와 같이 두 가지 값을 가질 수 있다.

사전정리 2: $q(t)$가 주기가 N인 4진 수열이라 하자. 이 때 $q(t)$가 균형성을 갖는 경우 $q(t)$의 무게합은 다음과 같은 값을 갖는다.

$$\sum_{t=0}^{N-1} \omega_4^{q(t)} = \begin{cases} 0, & \text{for } c_0 = c_2 \text{ and } c_1 = c_3 \\ \pm 1 \pm \omega_4, & \text{for } c_0 \ne c_2 \text{ and } c_1 \ne c_3. \end{cases}$$

증명: 정의 1에 따르면 균형성을 갖기 위해서는 c_i의 최대값과 최소값의 차이가 1 이하여야 한다. 그러므로 주기가 $N \equiv 2 \bmod 4$ 인 4진 수열의 경우 c_i는 다음과 같은 값을 가지게 된다.

$$c_i = \begin{cases} \dfrac{N-2}{4}, & 2 \text{ times} \\ \dfrac{N+2}{4}, & 2 \text{ times}. \end{cases}$$

이 때, $c_0 = c_2$이고 $c_1 = c_3$이면, 무게합이 0 이 되는 것은 자명하다. 또한 $c_0 \ne c_2$이고 $c_1 = c_3$이면, c_0와 c_2가 1 차이가 나고 c_1과 c_3이 1차이가 나는 것이므로 무게합이 $\pm 1 \pm \omega_4$가 됨은 자명하다. □

이제 짝수 주기를 갖고 균형성을 갖는 4진 수열의 이상적인 자기상관특성에 대하여 생각하여 보자. 주기가 짝수이고 균형성을 갖는 4진 수열에 있어 이상적인 자기상관특성은 다음 정리와 같이 정의된다.

정리 3: 짝수 정수 N에 대해 $g(t)$가 균형성을 갖는 주기가 N인 4진 수열이라 하자. 이 때, 이상적인 자기상관특성을 갖는 4진 수열 $g(t)$의 자기상관분포는 무게합에 따라 다음과 같이 두 가지 경우로 주어진다.

Case 1) 무게합이 0인 경우

$$R_g(\tau) = \begin{cases} N, & \text{once} \\ 0, & \dfrac{N}{2} - 1 \text{ times} \\ -2, & \dfrac{N}{2} \text{ times}. \end{cases} \qquad (3)$$

Case 2) 무게합이 0이 아닌 경우

$$R_g(\tau)=\begin{cases}N, & \text{once}\\ 0, & \frac{N}{2}\text{times}\\ -2, & \frac{N}{2}-1\ \text{times}.\end{cases} \quad (4)$$

증명: 4진 수열의 경우 수열이 균형성을 갖는다는 것은 한 주기 동안 수열에서 나타나는 각 문자들의 빈도수가 1이하로 차이남을 의미한다. 그러므로 주기 $N\equiv 0 \bmod 4$ 이거나 $N\equiv 2 \bmod 4$ 이고 무게합이 0인 경우 다음이 성립한다.

$$\sum_{t=0}^{N-1}\omega_4^{g(t)}=0.$$

이 때, 자기 상관분포의 정의와 위 수식의 결과로부터 다음의 식이 성립함은 자명하다.

$$\begin{aligned}\sum_{\tau=0}^{N-1}R_g(\tau)&=\sum_{\tau=0}^{N-1}\sum_{t=0}^{N-1}\omega_4^{g(t)-g(t+\tau)}\\&=\sum_{t=0}^{N-1}\sum_{\tau=0}^{N-1}\omega_4^{g(t)-g(t+\tau)}\\&=\sum_{t=0}^{N-1}\omega_4^{g(t)}\sum_{\tau=0}^{N-1}\omega_4^{-g(t+\tau)}=0.\end{aligned}$$

즉, 모든 위상에 대해서 자기상관함수값을 더하면 0이 된다는 것이다. 이 때, 동기점 $\tau=0$에서 자기상관함수값은 N이 되므로 다음이 성립한다.

$$\sum_{\tau=1}^{N-1}R_g(\tau)=-N.$$

4진 수열의 자기상관함수의 특성상 자기상관값의 합이 항상 자연수로만 나와야 하므로 자기상관 함수의 값이 실수로만 이루어졌을 때의 값은 자기상관 함수의 값에 복소수가 있는 경우보다 절대값이 항상 작게 된다. 그러므로 위 수식으로부터 자기상관함수 값이 최소가 되는 경우는 다음과 같이 됨을 생각할 수 있다.

$$R_g(\tau)=\begin{cases}N, & \tau=0\\ -\frac{N}{N-1}, & \text{othewise}.\end{cases}$$

그러나 4진 수열의 자기상관 함수값의 실수 부분은 항상 정수가 되어야 하므로 위의 수식이 성립하는 것은 불가능하다. 따라서 자기상관 함수가 가질 수 있는 최소의 자기상관 함수값의 절대값은 $\left\lfloor -\frac{N}{N-1}\right\rfloor =-2$의 절대값인 2가 된다.

또한, 짝수 주기의 특성상 자기상관값의 실수부가 홀수로 나오는 것은 불가능 하므로 이상을 고려할 때, 짝수 정수 N에 대하여 균형성을 갖는 4진 수열 $g(t)$가 완전 자기상관 특성을 갖지 않는 경우 가질 수 있는 최상의 자기 상관 특성인 이상적 자기상관 특성은 다음과 같게 된다.

$$R_g(\tau)=\begin{cases}N, & \text{once}\\ 0, & \frac{N}{2}-1\,\text{times}\\ -2, & \frac{N}{2}\,\text{times}.\end{cases}$$

무게합이 0이 아닌 경우 사전정리 2에 따라 다음이 성립한다.

$$\sum_{t=0}^{N-1}\omega_4^{g(t)}=\pm 1\pm\omega_4.$$

이 때, 자기 상관분포의 정의와 위 수식의 결과로부터 다음의 식이 성립함은 자명하다.

$$\begin{aligned}\sum_{\tau=0}^{N-1}R_g(\tau)&=\sum_{\tau=0}^{N-1}\sum_{t=0}^{N-1}\omega_4^{g(t)-g(t+\tau)}\\&=\sum_{t=0}^{N-1}\sum_{\tau=0}^{N-1}\omega_4^{g(t)-g(t+\tau)}\\&=\sum_{t=0}^{N-1}\omega_4^{g(t)}\sum_{\tau=0}^{N-1}\omega_4^{-g(t+\tau)}=2.\end{aligned}$$

즉, 모든 위상에 대해서 자기상관함수값을 더하면 2가 된다는 것이다.

이 후 무게합이 0인 경우와 동일한 과정을 거치면, 무게합이 0이 아니고 균형성을 갖는 경우 4진 수열이 가질 수 있는 최적의 상관분포는 다음을 알 수 있다.

$$R_g(\tau)=\begin{cases}N, & \text{once}\\ 0, & \frac{N}{2}\,\text{times}\\ -2, & \frac{N}{2}-1\ \text{times}.\end{cases}$$

□

Ⅳ. 이상적인 자기상관특성을 갖는 새로운 4진 수열

이번 장에서는 이상적인 자기상관특성을 갖는 이진 수열로부터 4진 수열을 생성하는 생성법을 제안한다. 새로 제안된 4진 수열의 자기상관함수는 동기점을 제외한 나머지 위상에서 0과 -2만을 가지며, 이는 주기가 $N \equiv 2 \bmod 4$ 인 4진 수열에 대하여 현재까지 알려진 최상의 결과이다. 또한, 새로 제안된 4진 수열의 자기상관분포 역시 유도하였다.

Krone와 Sarwate는 이진 수열과 이를 이용하여 (2)과 같이 생성한 4진 수열의 상관함수 간에 다음과 같은 관계가 성립함을 보였다.

예비정리 4 (Krone and Sarwate[8]): $a(t)$와 $b(t)$, $c(t)$, $d(t)$가 동일한 주기를 갖는 이진 수열이고, $p(t)$와 $q(t)$가 각각 $p(t)=\phi[a(t),b(t)]$, $q(t)=\phi[c(t),d(t)]$와 같이 정의되는 4진 수열이라 하자. 이 때, $p(t)$와 $q(t)$간의 상호상관함수 $R_{p,q}(\tau)$는 다음과 같이 주어진다.

$$R_{p,q}(\tau) = \frac{1}{2}\{R_{ac}(\tau)+R_{b,d}(\tau)\} + \frac{\omega_4}{2}\{R_{ad}(\tau)-R_{bc}(\tau)\}$$

단, $R_{ac}(\tau)$는 두 이진수열 $a(t)$와 $c(t)$간의 상호상관함수이다.

이상적인 자기상관특성을 갖는 이진 수열과 Gray 사상을 이용하여 다음 정리와 같이 정리 3의 자기상관분포를 갖는 4진 수열을 생성할 수 있다.

정리 5 (Jang, Kim, Kim, and No[5]): 양의 정수 n에 대해, $s(t)$가 이상적인 자기상관특성을 갖는 주기가 2^n-1인 이진 수열이라 하고 D_0는 $s(t)$의 특성집합이라 하자. 또한 4진 수열 $q(t)$를 다음과 같이 정의하자.

$$q(t)=\phi[a(t),b(t)]$$

단, $a(t)$와 $b(t)$는 다음과 같이 정의되는 주기가 $2^{n+1}-2$인 이진 수열이다.

$$a(t)=\begin{cases}1, & \text{if } t\in\{0,1\}\otimes D_0\\ 0, & \text{if } t\in\{0,1\}\otimes \overline{D_0}\end{cases}$$
$$b(t)=\begin{cases}1, & \text{if } t\in\{0\}\otimes D_0\cup\{1\}\otimes \overline{D_0}\\ 0, & \text{if } t\in\{0\}\otimes \overline{D_0}\cup\{1\}\otimes D_0\end{cases}$$

이 때, 주기가 $2^{n+1}-2$인 4진 수열 $q(t)$는 다음과 같은 자기상관특성을 갖는다.

$$R_q(\tau)=\begin{cases}2^{n+1}-2, & \text{for } \tau=0\\ 0, & \text{for } \tau\equiv 1 \bmod 2\\ -2, & \text{for } \tau\equiv 0 \bmod 2 \text{ and } \tau\neq 0\end{cases}$$

증명: $\tau=0$일 때, $R_q(\tau)=2^{n+1}-2$임은 자명하다. 예비정리 4로부터, $R_q(\tau)$를 다음과 같이 정리할 수 있다.

$$R_q(\tau)=\frac{1}{2}\{R_a(\tau)+R_b(\tau)\}+\frac{\omega_4}{2}\{R_{ab}(\tau)-R_{ba}(\tau)\}.$$

그러므로 $R_a(\tau)$와 $R_b(\tau)$, $R_{ab}(\tau)$, $R_{ba}(\tau)$를 구하는 것으로 $R_q(\tau)$를 구할 수 있다.

$a(t)$의 정의로부터 $a(t)$를 다음과 같이 나타낼 수 있다.

$$a(t)=s(t \bmod 2^n-1).$$

그러므로 다음이 성립함은 자명하다.

$$R_a(\tau)=\begin{cases}2^{n+1}-2, & \text{for } \tau=0 \text{ or } \tau=2^n-1\\ -2, & \text{otherwise}\end{cases} \quad (5)$$

이제 $t_0,\tau_0\in Z_2$ 와 $t_1,\ \tau_1\in Z_{2^n-1}$에 대해, $t=(t_0,t_1)$과 $\tau=(\tau_0,\tau_1)$을 정의하면 정리 3에서 정의된 $a(t)$와 $b(t)$의 정의로부터 $b(t)$를 다음과 같이 나타낼 수 있다.

$$b(t)=\begin{cases}a(t), & \text{if } t_0=0\\ a(t)+1 \bmod 2, & \text{if } t_0=1.\end{cases}$$

이 때, $b(t)$의 자기상관함수 $R_b(\tau)$는 다음과 같이 정리할 수 있다.

$$R_b(\tau)=\sum_{t=0}^{2^{n+1}-3}(-1)^{b(t)+b(t+\tau)}=\sum_{t_0=0}^{1}\sum_{t_1=0}^{2^n-2}(-1)^{b(t_0,t_1)+b(t_0+\tau_0,t_1+\tau_1)}. \quad (6)$$

$\tau_0=0$인 경우, (2)으로부터 위 식의 $R_b(\tau)$는 다음과 같이 정리할 수 있다.

$$\begin{aligned}R_b(\tau)&=\sum_{t_0=0}^{1}\sum_{t_1=0}^{2^n-2}(-1)^{b(t_0,t_1)+b(t_0+\tau_0,t_1+\tau_1)}\\&=\sum_{t_0=0}^{1}\sum_{t_1=0}^{2^n-2}(-1)^{a(t_0,t_1)+a(t_0+\tau_0,t_1+\tau_1)}\\&=\sum_{t=0}^{2^{n+1}-3}(-1)^{a(t)+a(t+\tau)}=R_a(\tau).\end{aligned} \quad (7)$$

$\tau_0=1$인 경우, (2)으로부터 위 식의 $R_b(\tau)$는 다음과 같이 정리할 수 있다.

$$\begin{aligned}R_b(\tau)&=\sum_{t_0=0}^{1}\sum_{t_1=0}^{2^n-2}(-1)^{b(t_0,t_1)+b(t_0+\tau_0,t_1+\tau_1)}\\&=-\sum_{t_0=0}^{1}\sum_{t_1=0}^{2^n-2}(-1)^{a(t_0,t_1)+a(t_0+\tau_0,t_1+\tau_1)}\\&=-\sum_{t=0}^{2^{n+1}-3}(-1)^{a(t)+a(t+\tau)}=-R_a(\tau).\end{aligned} \quad (8)$$

이제 (8)과 (9)로부터 $R_b(\tau)$를 다음과 같이 계산할 수 있다.

$$R_b(\tau)=\begin{cases}2^{n+1}-2, & \text{for}\ \tau=0\\ -2^{n+1}-2, & \text{for}\ \tau=2^n-1\\ -2, & \text{for}\ \tau\equiv 0\ \bmod 2\\ & \quad \text{and}\ \tau\neq 0\\ 2, & \text{for}\ \tau\equiv 1\ \bmod 2\\ & \quad \text{and}\ \tau\neq 2^n-1.\end{cases} \quad (9)$$

이와 유사한 방식으로 $a(t)$와 $b(t)$간의 상호상관 함수 $R_{ab}(\tau)$는 다음과 같이 나타낼 수 있다.

$$R_{ab}(\tau)=\sum_{t=0}^{2^{n+1}-3}(-1)^{a(t)+b(t+\tau)}=\sum_{t_0=0}^{1}\sum_{t_1=0}^{2^n-2}(-1)^{a(t_0,t_1)+b(t_0+\tau_0,t_1+\tau_1)}.$$

$\tau=0$인 경우, (2)으로부터 위 식을 다음과 같이 정리할 수 있다.

$$\begin{aligned}R_{ab}(\tau)&=\sum_{t_0=0}^{1}\sum_{t_1=0}^{2^n-2}(-1)^{a(t_0,t_1)+b(t_0,t_1+\tau_1)}\\&=\sum_{t_1=0}^{2^n-2}(-1)^{a(t_0,t_1)+a(0,t_1+\tau_1)}\\&\quad+\sum_{t_1=0}^{2^n-2}(-1)^{a(t_0,t_1)+a(1,t_1+\tau_1)+1}.\end{aligned} \quad (10)$$

(2)을 이용하면 위 식이 아래와 같이 됨은 자명하다.

$$\begin{aligned}\sum_{t_1=0}^{2^n-2}(-1)^{a(0,t_1)+a(0,t_1+\tau_1)}&=\sum_{t_1=0}^{2^n-2}(-1)^{s(t)+s(t+\tau)}\\&=R_s(\tau)\\\sum_{t_1=0}^{2^n-2}(-1)^{a(1,t_1)+a(1,t_1+\tau_1)+1}&=-\sum_{t_1=0}^{2^n-2}(-1)^{s(t)+s(t+\tau)}\\&=-R_s(\tau).\end{aligned}$$

그러므로 $\tau_0=0$일 때, $R_{ab}(\tau)=0$이 된다. 또한 $\tau_0=1$인 경우, $R_{ab}(\tau)$는 다음과 같이 정리된다.

$$\begin{aligned}R_{ab}(\tau)&=\sum_{t_0=0}^{1}\sum_{t_1=0}^{2^n-2}(-1)^{a(t_0,t_1)+b(t_0+1,t_1+\tau_1)}\\&=\sum_{t_1=0}^{2^n-2}(-1)^{a(t_0,t_1)+a(1,t_1+\tau_1)+1}\\&\quad+\sum_{t_1=0}^{2^n-2}(-1)^{a(t_0,t_1)+a(0,t_1+\tau_1)}\\&=0.\end{aligned} \quad (11)$$

$R_{ab}(\tau)$와 유사한 과정을 통하여 $R_{ba}(\tau)=0$임을 알 수 있다.

(6)과 (9), (10), (11)로부터 $R_q(\tau)$는 다음과 같이 계산된다.

$$\begin{aligned}R_q(\tau)&=\frac{1}{2}\{R_a(\tau)+R_b(\tau)\}+\frac{\omega_4}{2}\{R_{ab}(\tau)-R_{ba}(\tau)\}\\&=\begin{cases}2^{n+1}-2, & \text{for}\ \tau=0\\ 0, & \text{for}\ \tau\equiv 1 \bmod 2\\ -2, & \text{for}\ \tau\equiv 0\ \bmod 2\ \text{and}\ \tau\neq 0.\end{cases}\end{aligned} \quad (12)$$

□

이진 m-수열을 이용하여 다음과 같이 정리 3의 예제를 보일 수 있다.

예제 6: $s(t)$가 다음과 같이 주어지는 주기가 15인 이진 m-수열이라 하자.

$$s(t) = 0,0,0,1,0,0,1,1,0,1,0,1,1,1,1.$$

이 때, 정리 5에서 정의된 $a(t)$와 $b(t)$는 다음과 같이 주어진다.

$$\begin{aligned} a(t) &= 0,0,0,1,0,0,1,1,0,1,0,1,1,1,1, \\ &\quad 0,0,0,1,0,0,1,1,0,1,0,1,1,1,1 \\ b(t) &= 0,1,0,0,0,1,1,0,0,0,0,0,1,0,1, \\ &\quad 1,0,1,1,1,0,0,1,1,1,1,1,0,1,0. \end{aligned}$$

정리 5에서 정의된 $q(t)$의 정의로부터 $q(t)$가 다음과 같이 생성됨을 알 수 있다.

$$\begin{aligned} q(t) = {} & 0,1,0,3,0,1,2,3,0,3,0,3,2,3,2, \\ & 1,0,1,2,1,0,3,2,1,2,1,2,3,2,3. \end{aligned}$$

이 때, $q(t)$의 자기상관함수 $R_q(\tau)$는 다음과 같은 값을 갖는다.

$$\begin{aligned} R_q(\tau) = {} & 30,0,-2,0,-2,0,-2,0,-2,0,-2,0,-2,0,-2, \\ & 0,-2,0,-2,0,-2,0,-2,0,-2,0,-2,0,-2,0, \\ & -2,0,-2,0,-2,0,-2,0,-2,0,-2,0,-2,0,-2, \\ & 0,-2,0,-2,0,-2,0,-2,0,-2,0,-2,0,-2,0. \end{aligned}$$

정리 5의 $q(t)$의로부터 새로 제안된 4진 수열 $q(t)$의 균형성에 대한 다음 정리를 도출할 수 있다.

정리 7: $q(t)$가 정리 5에서 정의된 4진 수열이라 하자. 이 때, $q(t)$는 다음과 같은 균형성을 갖는다.

$$q(t) = \begin{cases} 0, & 2^{n-1}-1 \text{ times} \\ 1, & 2^{n-1}-1 \text{ times} \\ 2, & 2^{n-1} \text{ times} \\ 3, & 2^{n-1} \text{ times}. \end{cases}$$

증명: $q(t)$의 정의로부터 다음이 성립한다.

$$q(t) = \begin{cases} 0, & \text{for } t \in \{0\} \otimes (\overline{D_0} \cap \overline{D_0}) \\ & \text{or } t \in \{1\} \otimes (\overline{D_0} \cap D_0) \\ 1, & \text{for } t \in \{0\} \otimes (\overline{D_0} \cap D_0) \\ & \text{or } t \in \{1\} \otimes (\overline{D_0} \cap \overline{D_0}) \\ 2, & \text{for } t \in \{0\} \otimes (D_0 \cap D_0) \\ & \text{or } t \in \{1\} \otimes (D_0 \cap \overline{D_0}) \\ 3, & \text{for } t \in \{0\} \otimes (D_0 \cap \overline{D_0} \\ &) \text{ or } t \in \{1\} \otimes (D_0 \cap D_0). \end{cases}$$

이 때, $D \cap \overline{D} = \varnothing$이고, $D \cap D = D$이므로 $q(t)$를 다음과 같이 정리할 수 있다.

$$q(t) = \begin{cases} 0, & \text{for } t \in \{0\} \otimes \overline{D_0} \\ 1, & \text{for } t \in \{1\} \otimes \overline{D_0} \\ 2, & \text{for } t \in \{0\} \otimes D_0 \\ 3, & \text{for } t \in \{1\} \otimes D_0. \end{cases}$$

(1)로부터 $q(t)$가 다음의 분포를 가짐은 자명하다.

$$q(t) = \begin{cases} 0, & 2^{n-1}-1 \text{ times} \\ 1, & 2^{n-1}-1 \text{ times} \\ 2, & 2^{n-1} \text{ times} \\ 3, & 2^{n-1} \text{ times}. \end{cases}$$

위의 분포로부터 $q(t)$가 균형성을 가짐을 알 수 있다. □

정리 7의 결과에 따라 정리 5에서 제안된 수열은 균형성을 가지나 그 무게합이 0이 아님을 알 수 있다. 또한 정리 5에서 제안된 수열의 자기상관분포는 정리 3에서 균형성을 가지나 무게합이 0이 아닌 경우의 자기상관분포값과 동일하므로 이상적인 자기상관특성을 가졌다고 볼 수 있다.

V. 결 론

본 논문에서는 짝수 주기와 균형성을 갖는 4진 수열에 대하여 무게합에 따라 이상적인 자기상관특성을 정의하고, 이것이 이상적인 자기상관특성이 됨을 증명하였다. 또한, 이상적인 자기상관 특성을 갖는 이진 수열과 Gray 사상을 이용하여 이상적인 자기상관특성을 갖는 4진 수열을 생성하는 방법을 제시하였다. 새로 제안된 생성법을 통해 이상적인 자기 상관 특성을 갖는 이진 수열이 존재하는 경우, 이를 이용하여 이상적인 자기상관특성을 갖는 4진 수열을 만들 수 있다.

본 논문의 결과인 이상적인 자기상관 특성을 갖는 4진 수열은 향후 통신의 다양한 분야에서 이용될 수 있을 것으로 기대된다[11-13].

References

[1] H. D. Luke, H. D. Schotten, and H. Hadinejad-Mahram, “Binary and quadriphase sequences with optimal autocorrelation

properties: a survey," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3271-3282, Dec. 2003.

[2] J. F. Dillon and H. Dobbertin, "New cyclic difference sets with singer parameters," *Finite Fields Appl.*, vol. 10, no. 3, pp. 342-389, Jul. 2004.

[3] B. Gordon, W. H. Mills, and L. R. Welch, "Some new difference sets," *Canadian J. Math.*, vol. 14, no. 4, pp. 614-625, 1962.

[4] J.-S. No, H. Chung, and M. S. Yun, "Binary pesudorandom sequences of period with ideal autocorrelation generated by the polynomial," *IEEE Trans. Inf. Theory*, vol. 44, no. 3, pp. 1278-1282, May 1998.

[5] V. M. Sidel'nikov, "Some -valued pseudo-random sequences and nearly equidistant codes," *Probl. Info. Trans.*, vol. 5, no. 1, pp. 12-16, 1969.

[6] H. D. Schotten, "New optimum ternary compelmentary sets and almost quadriphase, perfect sequences," in *Proc. Int. Conf. Neural Netw. Signal Process.'95*, pp. 1106-1109, Nanjing, China, Dec. 1995.

[7] H. D. Schotten, "Optimum complementary sets and quadriphase sequences derived from q-ary m-sequences," in *Proc. IEEE Int. Symp. Inf. Theory'97,* P. 485, Ulm Germany, Jun.-Jul. 1997.

[8] S. M. Krone and D. V. Sarwate, "Quadriphase sequences for spread spectrum multiple-access communication," *IEEE Trans. Inf. Theory*, vol. 30, no. 3, pp. 520-529, May 1984.

[9] C. E. Lee, "Perfect *q*-ary sequences form multiplicative characters over GF(*p*)," *Electron. Lett.*, vol. 28, no. 9, pp. 833-835, Apr. 1992.

[10] J.-W. Jang, Y.-S. Kim, S.-H. Kim, and J.-S. No, "New quaternary sequences with ideal autocorrelation constructed binary sequences with ideal autocorrelation," in *Proc. IEEE Inf. Theory*, pp. 278-281, Seoul, Korea, Jul. 2009.

[11] Y.-S. Kim, "New secure network coding scheme with low complexity," *J. KICS*, vol. 38A, no. 4, pp. 295-302, Apr. 2013.

[12] Y.-J. Cho, J.-S. No, and D.-J. Shin, "Low complexity PTS scheme for reducing PAPR in OFDM systems," *J. KICS*, vol. 38A, no. 2, pp. 201-208, Feb. 2013.

[13] N. Kim, "Information potential and blind algorithms using a biased distribution of random-order symbols," *J. KICS*, vol. 38A, no. 1, pp. 26-32, Jan. 2013.

장 지 웅 (Ji-Woong Jang)

2000년 2월 : 서울대학교 전기공학부 졸업

2002년 2월 : 서울대학교 전기컴퓨터공학부 석사

2006년 2월 : 서울대학교 전기컴퓨터공학부 박사

2006년 3월~2008년 6월 : 삼성전자 책임연구원

2008년 8월~2009년 7월 : University of California, San Diego PostDoc.

2009년 9월~2012년 8월 : LG전자 책임연구원

2012년 9월 : 울산과학대학교 컴퓨터정보학부 조교수

<관심분야> 이동통신, 통신이론, 정보이론, 정보보안