최적의 자기 상관 성질을 갖는 4진 수열의 생성

*김영식, **장지웅, †김상효O, ‡노종선

*삼성전자, **Dept. ECE UCSD

†성균관대학교 정보통신공학부, ‡서울대학교 전기·컴퓨터공학부

Construction of Quaternary Sequences with Optimal Autocorrelation

*Young-Sik Kim, **Ji-Woong Jang, †Sang-Hyo KimO, and ‡Jong-Seon No

*Samsung Electronics, **Dept. ECE UCSD,

†School of ICE, Sungkyunkwan University, ‡Dept. EECS, Seoul National University

요약

이진 Sidel'nokov 수열의 Gray 사상을 이용하여 새로운 4진 수열을 생성한다. 제안된 수열은 짝수 주기 N에 대해서 최대의 자기상관값 $R_{\max}=2$를 가지며, 거의 균형이다. 새로운 수열은 특히 주기 $N\equiv 0 \bmod 4$인 경우에 대하여 최적인 2의 $R_{\max}$를 갖는 정상적인 4진 수열로 간주될 수 있다. 같은 최대 자기상관값을 갖는 유일한 다른 4진 수열은 S_j [1]로 극단적으로 불균형인 수열이다.

1. 서론

$a(t)$와 $b(t)$를 M진 수열이라하고 주기가 N이라 하자. 여기서, 양의 정수 M이라 하면, $\omega_M^{a(t)}$은 이에 대응되는 신호 공간 수열 혹은 단위 제곱근 수열로 볼 수 있다. 단 여기서, ω_M 은 복소 원시 M차 단위근이며, $\omega_4 = j = \sqrt{-1}$를 예로 들 수 있다. 두 수열 $a(t)$와 $b(t)$의 상호상관 함수 $R_{a,b}(\tau)$ 는 다음과 같이 정의된다.

$$R_{a,b}(\tau)=\sum_{t=0}^{N-1}\omega_M^{a(t)-b(t+\tau)}.$$

만약 $a(t)=b(t)$이면 이것은 자기상관 함수가 되며, $R_a(\tau)$로 표기를 단순화 한다. $R_a(0)=N$ 임은 자명하며 동상(inphase) 자기상관이라 칭한다. 비동상(out-of-phase) 자기상관값은 수열 $a(t)$의 형태에 따라 달라진다.

$R_{\max}$를 수열 $a(t)$의 최대 (비동상) 자기상관값이라 하며 다음과 같이 정의된다.

$$R_{\max}=\max_{1\le\tau\le N-1}|R_a(\tau)|.$$

수열의 $R_{\max}$는 다양한 디지털 통신 시스템을 위한 신호 설계에 있어 매우 중요한 기준이다. 그래서 작은 $R_{\max}$를 갖는 수열의 설계에 관한 연구가 많이 이루어져 왔다 [2], [3], [4], [5], [6].

디지털 통신 시스템에서 직교 변조가 주로 사용되므로, 구현이 간단한 이진 혹은 4진 수열이 더 많은 관심을 일으켜 왔다. 본 논문에서는 논의의 범주를 이진 혹은 4진의 주기 수열 및 그 상관 성질로 한정하기로 한다. 또한 $\omega_4^{a(t)}$와 같이 신호 공간에서 단위 전력을 갖는 수열 만을 고려한다.

Lüke는 좋은 주기 혹은 좋은 비주기 자기상관 성질을 갖는 이진 및 4진 수열에 관한 훌륭한 조사연구를 수행하였다 [7]. 그 조사 결과를 참조하여, 짝수 주기 및 상수의 단위 전력을 갖고 가장 좋은 $R_{\max}$를 갖는 4진 수열들을 표 1에 나열하였다.

여기서 S_j 은 일반화된 Sidel'nikov 수열을 의미하며, $j=\omega_4$의 값을 단 하나 갖는 수열이다. S_j는 주기 $N\equiv 0 \bmod 4$인 경우에 대하여 최적의 $R_{\max}=2$를 갖는 유일한 수열이었다. $\prod(C,4)$ [7]는 보수 기반 수열 C [8]와 주기 4인 완전한 수열 $(1,1,1,-1)$의 주기적 곱에 해당된다. $N\equiv 0 \bmod 4$인 경우에 대하여 $\prod(C,4)$의 $R_{\max}$는 이진 Sidel'nikov 수열[3]의 그것과 동일하다.

표 1. 낮은 자기상관을 갖는 4진 수열

$N \bmod 4$	Type	N	$R_{\max}$
0	S_j [1]	p^n-1	2
0	$\prod(C,(1,1,1,-1))$[7]	$2(p^n+1)$	4
0	새로운 수열	p^n-1	2
2	P_1 [7]	p^n+1	2
2	$\prod(L_1,(1,j)),\prod(L_j,(1,j))$[7]	$2p_3, 2p_1$	2
2	$\prod(\boldsymbol{m},(1,j))$ [7]	$2(2^n-1)$	2
2	새로운 수열	p^n-1	2

주기 $N\equiv 2 \bmod 4$인 경우, P_1은 Lee [4]가 소개한 완전한 자기상관 성질을 갖는 수열 (단위 전력이 아님)의 첫번째 위치에 $\omega_4^0=1$ 넣어서 만들어진 수열이다.

L_1과 L_j [7]는 Legendre 수열의 신호 공간 수열에 앞에 각각 1과 j를 위치시킨 수열을 의미한다. 고로 L_j는 4진 수열이 된다. 이 수열들과 $(1,j)$과의 주기적 곱은 $R_{\max}=2$인 4진 수열을 생성한다. $\boldsymbol{m}$은 이상적인 자기상관 성질을 갖는 이진 m 수열을 의미한다. 사실상 $\boldsymbol{m}$과 $(1,j)$와의 주기적 곱 수열에서 $\boldsymbol{m}$수열은 Gordon-Mills-Welch (GMW) 수열 [9]과 같은 이상적인 자기 상관 성질을 갖는 다른 수열로도 대체될 수 있다.

본 논문에서는 새로운 단위 전력 4진 주기 수열의 생성법을 제안한다. 새로운 4진 수열은 서로 다른 한 쌍의 Sidel'nikov 수열의 Gray 사상을 이용하여 생성된다. S_j는 4진 수열이라 주장되었지만, 실제로 이 수열은 3개의 위상 $\omega_4^0,\omega_4^1,\omega_4^2$ 만을 가지며 극단적으로 불균형이다. 그러므로, 지금까지 전형적인 4진 수열로 $N\equiv 0 \bmod 4$에서 가장 작은 최대 자기상관값을 갖는 수열은 $\prod(C,(1,1,1,-1))$ 이었다고 볼 수 있다. 새로운 생성법은 주기 $N\equiv 0 \bmod 4$에 대하여 S_j가 가졌던 $R_{\max}=2$를 가지고 거의 균형인 4진 수열을 제공한다. 이런 관점에서 볼 때, 새로운 4진 수열은 최적의 $R_{\max}=2$를

만족시키는 최초의 4진 수열로 간주될 수 있다. 새로운 4진 수열의 생성법은 주기 N이 $2 \bmod 4$인 경우에도 $R_{\max} = 2$를 제공하며, 이는 기존에 알려진 가장 좋은 결과와 동일한다.

2. 사전지식

Sidel'nikov [3] 는 다음과 같이 M진 수열을 정의하였다.

정의 1 (Sidel'nikov [3]): p는 홀소수이고, α는 유한체 F_{p^n}의 원시원이다. $M|p^n-1$을 가정하고 $\mathcal{S}_k$, $k = 0, 1, \ldots, M-1$은 서로 공통원소를 갖지 않는 F_{p^n}의 부분집합이며, 다음과 같이 정의된다.

$$\mathcal{S}_k = \{\alpha^{Mi+k} - 1 \mid 0 \le i < \frac{p^n-1}{M}\}.$$

p^n-1의 주기를 갖는 M진 Sidel'nikov 수열 $s(t)$은

$$s(t) = \begin{cases} k, & \text{if } \alpha^t \in \mathcal{S}_k, \quad 0 \le k \le M-1 \\ k_0, & \text{if } t = \frac{p^n-1}{2} \end{cases}$$

와 같이 정의된다. 단, k_0 는 $\{0, 1, 2, \cdots, M-1\}$의 원소이다.

$\alpha^{\frac{p^n-1}{2}} = -1$ 임을 주지하라. 또한, $\bigcup_{k=0}^{M-1} \mathcal{S}_k = F_{p^n} \backslash \{-1\}$ 이고, $0 \in \mathcal{S}_0$이다. N_k는 한 주기의 Sidel'nikov 수열에서 k가 발생하는 횟수

$$N_k = |\{t \mid s(t) = k, \quad 0 \le t \le p^n - 2\}|$$

이다. 만약, $k_0 \neq 0$이면,

$$N_k = \begin{cases} \frac{p^n-1}{M}, & \text{if } k \neq 0, k_0 \\ \frac{p^n-1}{M} + 1, & \text{if } k = k_0 \\ \frac{p^n-1}{M} - 1, & \text{if } k = 0. \end{cases}$$

가 된다. $k_0 = 0$이 완전하게 균형인 수열을 생성함은 자명하다.

M진 Sidel'nikov 수열의 정의는 M차의 원분수 [11]와 밀접한 연관을 갖는다.

정의 2: α를 유한체 F_{p^n}의 원시원이라한다. F_{p^n}의 순환 클래스 C_u, $0 \le u \le M-1$는

$$C_u = \{\alpha^{Ml+u} \mid 0 \le l < \frac{p^n-1}{M}\}.$$

와 같이 정의된다. 고정된 양의 정수 u와 v에 대해서 원분수 $(u, v)_M$는 $1 + z_u \in C_v$를 만족시키는 $z_u \in C_u$의 수로 정의된다.

M진 Sidel'nikov수열은 정의함수 및 F_{p^n} 곱셈지표를 이용하여 표현된다.

정의 3: 정의함수 $I(x)$는 다음과 같이 정의된다.

$$I(x) = \begin{cases} 1, & \text{if } x = 0 \\ 0, & \text{if } x \neq 0. \end{cases}$$

정의 4: F_{p^n}의 M차 곱셈지표는

$$\psi_M(\alpha^t) = e^{j\frac{2\pi t}{M}}, \quad \text{for } \alpha^t \in F_{p^n}^*$$

및

$$\psi_M(0) = 0$$

로 정의된다. 여기서 α는 F_{p^n}의 원시원이며, $M|p^n-1$이고, $0 \le t \le p^n - 2$이다.

이제 M진 Sidel'nikov 수열은

$$\omega_M^{s(t)} = \omega_M^{k_0} I(\alpha^t + 1) + \psi_M(\alpha^t + 1). \tag{1}$$

와 같이 표현된다. $\phi[a, b]$를 Gray 사상이라 하며

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

와 같이 정의한다. 주기 N인 이진 수열 $a(t)$와 $b(t)$가 있다. $q(t) = \phi[a(t), b(t)]$와 같이 4진 수열 $q(t)$를 정의하자. 그러면, $q(t)$에 대응되는 신호공간 수열은 다음과 같이 이진 수열$a(t), b(t)$를 이용하여 표시할 수 있다[10].

$$\omega_4^{q(t)} = \frac{1+\omega_4}{2}(-1)^{a(t)} + \frac{1-\omega_4}{2}(-1)^{b(t)}. \tag{3}$$

Krone과 Sarwate는 이진 수열 $a(t), b(t)$와 생성된 4진 수열 $q(t)$의 상관함수의 관계(3)을 구하였다.

예비정리 5 (Krone 과 Sarwate [10]): $a(t)$, $b(t)$, $c(t)$ 및 $d(t)$는 같은 주기를 갖는 이진 수열이다. Gray 사상을 이용하여 4진 수열 $p(t)$와 $q(t)$를 정의한다.

$$p(t) = \phi[a(t), b(t)], \quad q(t) = \phi[c(t), d(t)].$$

그러면, $p(t)$와 $q(t)$의 상호상관 함수 $R_{p,q}(\tau)$는

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

와 같이 주어진다. 여기서 $R_{a,b}(\tau)$는 이진 수열 $a(t)$와 $b(t)$의 상호상관 함수이다.

3. 이진 SIDEL'NIKOV 수열을 이용한 새로운 4진 수열의 생성

역 Gray 사상을 이용하여 2개의 이진 Sidel'nikov로부터 최적의 최대 자기상관값을 4진 수열을 각각 $k_0 = 0$와 $k_0 = 1$인 이진 Sidel'nikov 수열이라 하자. 이 때, $s_0(t)$는 균형이고 $s_1(t)$는 불균형이다. 새로운 4진 수열은 다음과 같이 정의된다.

$$q(t) = \phi[s_0(t), s_1(t + N/2)].$$

그러면, 4진 수열 $q(t)$의 자기상관값 분포는 다음의 정리와 같이 결정된다.

정리 6: 4진 수열 $q(t)$의 자기상관 함수는 주기 $N = p^n - 1 \equiv 0 \bmod 4$에 대하여

$$R_q(\tau) = \begin{cases} p^n - 1, & \text{once} \\ -2, & \frac{p^n-1}{2} - 1 \text{ times} \\ -j2, & \frac{p^n-1}{4} \text{ times} \\ j2, & \frac{p^n-1}{4} \text{ times} \end{cases}$$

의 분포를 갖고, $N \equiv 2 \bmod 4$에 대하여

$$R_q(\tau) = \begin{cases} p^n - 1, & \text{once} \\ -2, & \frac{p^n-1}{2} \text{ times} \\ -j2, & \frac{p^n-3}{4} \text{ times} \\ j2, & \frac{p^n-3}{4} \text{ times} \end{cases}$$

의 분포를 갖는다.

증명: $R_q(0) = p^n - 1$는 자명한다. 그러므로, $\tau \neq 0$인 경우의 자기상관값 분포를 구하면 된다. 사전정리 5로부터 $q(t)$의 자기상관 함수는

$$\begin{aligned} R_q(\tau) &= \frac{1}{2}[R_{s_0}(\tau) + R_{s_1}(\tau)] + \frac{j}{2}[R_{s_0,s_1}(\tau + N/2) \\ &\quad -R_{s_1,s_0}(\tau - N/2)]. \end{aligned}$$

와 같이 다시 쓰여진다. [11]에서는 $\tau \neq 0$에 대하여 $R_{s_0}(\tau)$ 및 $R_{s_1}(\tau)$를 다음과 같이 전개하였다.

$$R_{s_0}(\tau) = \psi_2(-\alpha^\tau + 1) + \psi_2(-\alpha^{-\tau} + 1) - \psi_2(\alpha^{-\tau}) - 1$$
$$R_{s_1}(\tau) = -\psi_2(-\alpha^\tau + 1) - \psi_2(-\alpha^{-\tau} + 1) - \psi_2(\alpha^{-\tau}) - 1.$$

그리고, $R_{s_0}(0) = R_{s_1}(0) = N$임은 명백하다. $R_{s_0}(\tau)$의 표현을 이용하여 $R_{s_1}(\tau)$, $s_0(t)$과 $s_1(t)$의 상호상관 함수를 구하면,

$$\begin{aligned} R_{s_0,s_1}\left(\tau + \frac{N}{2}\right) &= \sum_{t=0}^{N-1} (-1)^{s_0(t) - s_1(t+\tau+N/2)} \\ &= \sum_{t=0}^{N-1} \left\{(-1)^{s_1(t)} + 2I(\alpha^t + 1)\right\} (-1)^{-s_1(t+\tau+N/2)} \\ &= R_{s_1}(\tau + N/2) + 2(-1)^{s_1(\tau)} \\ &= R_{s_1}(\tau + N/2) + 2\left\{-I(\alpha^\tau + 1) + \psi_2(\alpha^\tau + 1)\right\} \end{aligned}$$

이 된다. $\tau = N/2$에 대하여 $R_{s_0,s_1}(\tau + N/2) = N - 2$가 되고, $\tau \neq N/2$에 대해서는

$$R_{s_0,s_1}(\tau + N/2) = \psi_2(\alpha^\tau + 1) - \psi(\alpha^{-\tau} + 1) - \psi_2(-\alpha^{-\tau}) - 1$$

를 얻을 수 있다. 이와 유사하게 $\tau = N/2$에 대하여 $R_{s_1,s_0}(\tau - N/2) = N - 2$ 를 얻을 수 있고, $\tau \neq N/2$에 대해서는

$$R_{s_1,s_0}(\tau - N/2) = -\psi_2(\alpha^\tau + 1) + \psi(\alpha^{-\tau} + 1) - \psi_2(-\alpha^{-\tau}) - 1$$

가 얻어진다.

경우 1) $p^n - 1 \equiv 0 \bmod 4$;

$p^n - 1 \equiv 0 \bmod 4$이면, $\psi_2(-1) = \psi_2(\alpha^{(p^n-1)/2}) = 1$이다. 그러면,

$$R_q(\tau) = -(\psi_2(\alpha^{-\tau}) + 1) + j[\psi_2(\alpha^\tau + 1) - \psi_2(\alpha^{-\tau} + 1)]$$

임을 알 수 있다. $\psi_2(\alpha^{-\tau} + 1) = \psi_2(\alpha^\tau + 1)/\psi_2(\alpha^\tau)$이므로, 짝수의 $\tau \neq N/2$에 대해서

$$R_q(\tau) = -(1 + 1) + j[\psi_2(\alpha^\tau + 1) - \psi_2(\alpha^\tau + 1)] = -2$$

을 얻을 수 있고, $R_q(N/2) = -2$임은 명백하다. 홀수의 τ에 대해서

$$\begin{aligned} R_q(\tau) &= -(-1 + 1) + j[\psi_2(\alpha^\tau + 1) + \psi_2(\alpha^\tau + 1)] \\ &= j2\psi_2(\alpha^\tau + 1) \end{aligned}$$

가 얻어진다. 만약 홀수 τ에 대해서 $\alpha^\tau + 1$가 QR에 속한다면, (QR는 Z_p의 제곱잉여를 의미) $R_q(\tau) = j2$이고, 그렇지 않으면 $R_q(\tau) = -j2$이다. 2차의 원분수가 $p^n - 1 \equiv 0 \bmod 4$에 대해서 $(0,0)_2 = (p^n - 5)/4$, $(0,1)_2 = (1,0)_2 = (1,1)_2 = (p^n - 1)/4$ 로 주어지므로[12] 자기상관값 분포는

$$R_q(\tau) = \begin{cases} p^n - 1, & \text{once} \\ -2, & \frac{p^n-1}{2} - 1 \text{ times} \\ -j2, & \frac{p^n-1}{4} \text{ times} \\ j2, & \frac{p^n-1}{4} \text{ times.} \end{cases}$$

로 주어지게 된다.

경우 2) $p^n - 1 \equiv 2 \bmod 4$;

만약 $p^n - 1 \equiv 2 \bmod 4$이고, $\psi_2(-1) = \psi_2(\alpha^{(p^n-1)/2}) = -1$이면, 위의 경우와 유사하게 $\tau \neq N/2$에 대해서

$$R_q(\tau) = -(\psi_2(\alpha^{-\tau}) + 1) + j\left[\psi_2(\alpha^\tau + 1) - \frac{\psi_2(\alpha^\tau + 1)}{\psi_2(\alpha^\tau)}\right]$$

임을 알 수 있다. 짝수의 τ에 대해서

$$R_q(\tau) = -(1 + 1) + j[\psi_2(\alpha^\tau + 1) - \psi_2(\alpha^\tau + 1)] = -2$$

가 얻어지며, 홀수의 $\tau \neq N/2$에 대해서는

$$\begin{aligned} R_q(\tau) &= -(-1 + 1) + j[\psi_2(\alpha^\tau + 1) + \psi_2(\alpha^\tau + 1)] \\ &= j2\psi_2(\alpha^\tau + 1) \end{aligned}$$

를 얻을 수 있다. $R_q(N/2) = -2$는 쉽게 확인된다. 홀수 $\tau \neq N/2$에 대해서 $\alpha^\tau + 1$가 QR에 포함된다면, $R_q(\tau) = j2$이고, $\alpha^\tau + 1$가 QR에 포함되지 않으면, $R_q(\tau) = -j2$이다.

$p^n \equiv 3 \bmod 4$에 대해서 2차의 원분수가 $(0,0)_2 = (1,0)_2 = (1,1)_2 = (p^n - 3)/4$ and $(0,1)_2 = (p^n + 1)/4$와 같이 주어지고[12], 결국 자기상관값 분포는

$$R_q(\tau) = \begin{cases} p^n - 1, & \text{once} \\ -2, & \frac{p^n-1}{2} \text{ times} \\ -j2, & \frac{p^n-3}{4} \text{ times} \\ j2, & \frac{p^n-3}{4} \text{ times} \end{cases}$$

와 같이 주어진다. □

4. 참고문헌

[1] H. D. Lüke, H. D. Schotten, and H. Hadinejad-Mahram, "Generalised Sidelnokov sequences with optimal autocorrelation peroperties," *Electron. Lett*, vol. 36, no. 6, pp. 525–527, Mar. 2000.

[2] T. Helleseth and P. V. Kumar, "Sequences with low correlation," in *Handbook of Coding Theory*, V. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier Science, 1998.

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

[4] C. E. Lee, "Perfect q-ary sequences from multiplicative characters over GF(p)," *Electron. Lett.*, vol. 28, pp. 833–835, 1992.

[5] J.-S. No, H. Chung, and M. S. Yun, "Binary pseudorandom sequences of period $2^n - 1$ with ideal autocorrelation generated by the polynomial $z^d + (z + 1)^d$," *IEEE Trans. inf. Theory,* vol. 44, no. 3, pp. 1278–1282, May 1998.

[6] J.-S. No, H. Chung, H.-Y. Song, K. Yang, J.-D. Lee, and T. Helleseth, "New construction for binary sequences of period $p^m - 1$ with optimal autocorrelation using $(z+1)^d + az^d + b$," *IEEE Trans. inf. Theory,* vol. 47, no. 4, pp. 1638–1644, May 2001.

[7] H. D. Lüke, 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.

[8] H. D. Schotten, "Optimum complementary sets and quadriphase sequences derived from q-ary m-sequences," in *Proc. IEEE Int. Symp. inf. Theory '97*, Ulm, Germany, 1997, p. 485.
[9] B. Gordon, W. H. Mills, and L. R. Welch, "Some new difference sets," *Canadian J. Math.,* vol. 14, no. 4, pp. 614–625, 1962.
[10] S. M. Krone and D. V. Sarwate, "Quadriphse sequences for spread-spectrum multiple-access communication," *IEEE Trans. Inf. Theory*, vol. IT-30, no. 3, pp. 520–529, May 1984.
[11] Y.-S. Kim, J.-S. Chung, J.-S. No, and H. Chung, "On the autocorrelation distributions of Sidel'nikov sequences," *IEEE Trans. Inf. Theory*, vol. 51, no. 9, pp. 3303–3307, Sep. 2005.
[12] T. Storer, *Cyclotomy and Difference Sets, Lectures in Advanced Mathematics*. Chicago, IL: Markham Publishing Company, 1967.
[13] W. H. Mow, "A unified construction of perfect polyphase sequences," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT'95)*, Whistler, Canada, 1995, p. 459.