이진 Gold 수열을 이용한 낮은 상관 특성을 갖는 4진 수열군의 생성

*최성태O, *정정수, *노종선, **장지웅, ***정하봉
*서울대학교 전기컴퓨터공학부, 뉴미디어통신공동연구소
**UCSD ***홍익대학교 전자전기공학부

Construction of Quadriphase Sequence Families From Binary Gold Sequences

*Sung-Tai ChoiO, *Jung-Soo Chung, *Jong-Seon No, **Ji-Woong, Jang and ***Habong Chung
*Department of EECS, INMC, Seoul National University
**UCSD ***School of Electronics and Electrical Engineering, Hongik University
{stchoi, integer}@ccl.snu.ac.kr, jsno@snu.ac.kr, stasera.jang@gmail.com, habchung@hongik.ac.kr

요약

주기 2^n-1인 이진 Gold 수열군을 이용해서 주기 2^n-1인 낮은 상관 특성을 갖는 새로운 4진 수열군을 생성한다. 새로운 수열군의 상관 값은 n이 홀수일 때, $2^{\frac{n+2}{2}}+1$의 상계 값을 갖고 n이 2 mod 4일 때, $2^{\frac{n+3}{2}}+1$의 상계를 갖는다. 두 수열군 모두 2^n개의 수열을 포함한다.

1. 서론

좋은 상관 값을 갖는 수열군은 널리 응용될 수 있는데, 특히 확산 스펙트럼 통신시스템의 설계에 쓰인다. 직접수열 부호분할 다중접속방식(DS-CDMA) 시스템에서 낮은 상관 값을 갖는 확산 수열들은 각 사용자들의 신호를 구분하는 역할을 한다.

이진 수열군과 4진 수열군은 변조기에서 구현이 쉽기 때문에 실제 시스템에서 자주 사용된다. 잘 알려진 이진 수열군으로는 Kasami 수열군 [1]–[3], Gold 수열군 [4] 등이 있다. 잘 알려진 최적의 상관 특성을 갖는 4진 수열군으로는 Boztas, Hammons, 그리고 Kumar가 생성한 수열군 $\mathcal{A}$, $\mathcal{B}$ [5]이 있다. 수열군 $\mathcal{A}$는 주기 2^n-1인 2^n+1개의 수열로 구성된다. 수열군 $\mathcal{B}$는 주기 $2(2^n-1)$인 2^{n-1}개의 수열을 포함한다. 또 다른 최적의 상관특성을 갖는 수열군 $\mathcal{C}$ [6]는 $\mathcal{B}$와 같은 성능을 갖는다. 또한 Tang, Udaya는 주기가 $2(2^n-1)$이고 2^n의 크기를 갖는 수열군 $\mathcal{D}$ [7]를 생성하였다. 또한 Kumar, Helleseth, 그리고 Calerbank는 수열군 $\mathcal{S}(0)=\mathcal{A}$, $\mathcal{S}(1)$, 그리고 $\mathcal{S}(2)$를 생성하였다[8].

이 논문에서는 이진 Gold 수열군을 이용해서 주기가 2^n-1인 4진 수열군을 생성한다. 각 수열군들의 상관 값의 크기는 n이 홀수인 경우에 $2^{\frac{n+2}{2}}+1$로 상한되고 n이 2 mod 4 일 때, $2^{\frac{n+3}{2}}+1$로 상한된다. 두 수열군 모두 2^n개의 수열을 포함한다. 각각의 새롭게 생성된 수열군을 $\mathcal{F}_0$, $\mathcal{F}_1$라 할 경우 앞에서 언급한 잘 알려진 4진 수열군과의 성능 비교는 표1과 같다.

2. 사전지식

F_{2^n}에서 F_{2^m}로의 trace 함수는 다음과 같이 정의된다.

$$\mathrm{tr}_m^n(x)=\sum_{i=0}^{n/m-1}x^{2^{mi}}$$

여기서 $x\in F_{2^n}$이고 m은 n의 약수이다.

Gold [4]는 최적의 상관 특성을 갖는 이진 수열군을 생성하였다. 이 수열군을 Gold 수열군이라 부른다. 수열군은 다음과 같이 정의된다.

정의 1: [4] α는 F_{2^n}의 원시원이고, $n\geq 3$은 양의 정수라 하자. $k\geq 1$일 때 d는 2^k+1 또는 $2^{2k}-2k+1$이라 놓자. $e=\gcd(n,k)$는 n이 홀수일 때 1이고 n이 2 mod 4일 때 2이다. $s_a(t)=\mathrm{tr}_1^n(a\alpha^t+\alpha^{dt}), a\in F_{2^n}$, $s_\infty(t)=\mathrm{tr}_1^n(\alpha^t)$ 라고 정의하면 Gold 수열군은 다음과 같다.

$$\mathcal{G}=\{\{s_a(t)\}|a\in F_{2^n}\cup\{\infty\}\}$$

수열군의 크기는 2^n+1이고 주기는 2^n-1이다. □

$s_u=\{s_u(t)\}$ 와 $s_v=\{s_v(t)\}$ 를 주기 N인 두 4진 수열이라 놓자. 이 수열들의 $0\leq\tau\leq N-1$에 대한 상관 값 $R_{s_u,s_v}(\tau)$ 은 다음과 같이 표현된다.

$$R_{s_u,s_v}(\tau)=\sum_{t=0}^{N-1}\omega_4^{s_u(t)-s_v(t+\tau)}$$

여기서 $\omega_4=\sqrt{-1}$ 는 1의 원시 4승근이다.

Inverse Gray 사상 $\phi[a,b]$는 다음과 같다.

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

$a(t)$와 $b(t)$를 0과 1로 구성된 주기 N인 이진 수열이라 놓자. $q(t)=\phi[a(t),b(t)]$는 두 수열의 inverse Gray 사상을 이용한 4진 수열이다. 이 때 다음과 같이 표현할 수 있다[9].

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

표 1. 알려진 4진 수열군과의 비교

수열군	주기	수열군 크기	최대 상관 값
$\mathcal{A}$[5]	2^n-1	2^n+1	$2^{\frac{n}{2}}+1$
$\mathcal{B}$[5], $\mathcal{C}$[6]	$2(2^n-1)$	2^{n-1}	$2^{\frac{n+1}{2}}+2$
$\mathcal{D}$[7]	$2(2^n-1)$	2^n	$2^{\frac{n+1}{2}}+2$
$\mathcal{F}_0$(New)	2^n-1	2^n	$2^{\frac{n+2}{2}}+1$
$\mathcal{F}_1$(New)	2^n-1	2^n	$2^{\frac{n+3}{2}}+1$

여기서 $\mathcal{F}_0$는 n이 홀수일 경우 수열군이고 $\mathcal{F}_1$는 n이 2 mod 4일 경우 수열군이다.

Krone, Sarwate는 [9]에서 (1)에서 이진 수열 $a(t)$, $b(t)$와 4진 수열 $q(t)$의 상관 값의 관계를 다음과 같이 정리하였다.

보조정리 1 ([9]): $a(t)$, $b(t)$, $c(t)$, 그리고 $d(t)$를 같은 주기를 갖는 이진 수열들이라 놓자. $p(t)$와 $q(t)$는 $p(t)=\phi[a(t),b(t)]$ 와 $q(t)=\phi[c(t),d(t)]$ 로 각각 정의되는 4진 수열이다. 이 때 $p(t)$와 $q(t)$의 상관 값 $R_{p,q}(\tau)$는 다음과 같이 주어진다.

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

여기서 $R_{a,b}(\tau)$ 는 $a(t)$와 $b(t)$의 상관 값이다. □

$\mathbb{Z}_2\times\mathbb{Z}_2$에서 $\mathbb{Z}_4$ 로의 사상 μ는 다음과 같다.

$$\mu(a,b)\triangleq a+2b \tag{2}$$

여기서 $a,b\in\mathbb{Z}_2$이다.

식 (2)는 inverse Gray 사상을 이용해서 표현하면 다음과 같다.

$$\mu(a,b)=\phi(b,a\oplus b) \tag{3}$$

여기서 $\oplus$는 modulo 2 연산이다.

3. 새로운 수열군의 생성

낮은 상관 특성을 갖는 새로운 4진 수열군은 다음과 같이 생성할 수 있다.

정리 1: n은 3 이상인 정수이고 d는 2^k+1 또는 $2^{2k}-2^k+1$이다. 또한 n은 홀수일 때 $e=\gcd(n,k)=1$ 이고 n은 2 mod 4일 때 $e=2$이다. $\mathcal{F}$는 주기 2^n-1인 4진 수열군으로 다음과 같이 정의된다.

$$\mathcal{F}=\{s_u(t)=\mu(\mathrm{tr}_1^n(x),\mathrm{tr}_1^n(ux)+\mathrm{tr}_1^n(x^d))|u\in F_{2^n}\}. \tag{4}$$

식 (4)의 수열군 $\mathcal{F}$에 속하는 수열들의 상관 값은 다음과 같이 상한된다.

$$|R_{s_u,s_v}(\tau)|\le 2^{\frac{n+e+1}{2}}+1.$$

증명: 수열군 $\mathcal{F}$에 속하는 두 수열 $s_u(t)$, $s_v(t)$를 다음과 같이 표현할 수 있다.

$$s_u(t)=\mu(\mathrm{tr}_1^n(x),\mathrm{tr}_1^n(ux)+\mathrm{tr}_1^n(x^d)) \tag{5}$$
$$s_v(t)=\mu(\mathrm{tr}_1^n(x),\mathrm{tr}_1^n(vx)+\mathrm{tr}_1^n(x^d)). \tag{6}$$

식 (3)로부터, (5)과 (6)는 inverse Gray 사상을 이용하여 다음과 같이 다시 쓸 수 있다.

$$\begin{aligned}s_u(t)&=\phi[a(t),b(t)]\\s_v(t)&=\phi[c(t),d(t)]\end{aligned}$$

여기서 $a(t)$, $b(t)$, $c(t)$, 그리고 $d(t)$는 다음과 같다.

$$a(t)=\mathrm{tr}_1^n(ux)+\mathrm{tr}_1^n(x^d) \tag{7}$$
$$b(t)=\mathrm{tr}_1^n((1+u)x)+\mathrm{tr}_1^n(x^d) \tag{8}$$
$$c(t)=\mathrm{tr}_1^n(vx)+\mathrm{tr}_1^n(x^d) \tag{9}$$
$$d(t)=\mathrm{tr}_1^n((1+v)x)+\mathrm{tr}_1^n(x^d). \tag{10}$$

보조정리 1로부터, 두 수열 $s_u(t)$와 $s_v(t)$의 상관 값 $R_{s_u,s_v}(\tau)$은 다음과 같이 쓸 수 있다.

$$\begin{aligned}R_{s_u,s_v}(\tau)=&\frac{1}{2}\big\{R_{a,c}(\tau)+R_{b,d}(\tau)\big\}\\&+\frac{\omega_4}{2}\big\{R_{a,d}(\tau)-R_{b,c}(\tau)\big\}.\end{aligned} \tag{11}$$

이 식의 우변의 상관 값 $R_{a,c}(\tau)$, $R_{b,d}(\tau)$, $R_{a,d}(\tau)$, 그리고 $R_{b,c}(\tau)$는 (7)-(10)의 상관 값을 의미한다. $a(t)$, $b(t)$, $c(t)$, 그리고 $d(t)$는 모두 이진 Gold수열이기 때문에 우변에 있는 4개의 상관 값들은 모두 다음의 분포를 갖는다[4].

$$R_{a,b}(\tau)\in\{-1-2^{\frac{n+e}{2}},-1,-1+2^{\frac{n+e}{2}}\}.$$

$u\neq v$, $\tau=0$인 경우에, (11)의 우변의 4개의 상관 값들은 다음과 같이 정리된다.

$$\begin{aligned}R_{a,c}(0)&=\sum_{x\in F_{2^n}^*}(-1)^{\mathrm{tr}_1^n((u+v)x)}=-1\\R_{b,d}(0)&=\sum_{x\in F_{2^n}^*}(-1)^{\mathrm{tr}_1^n((u+v)x)}=-1\\R_{a,d}(0)&=R_{b,c}(0)\\&=\sum_{x\in F_{2^n}^*}(-1)^{\mathrm{tr}_1^n((u+v+1)x)}\in\{-1,2^n-1\}.\end{aligned}$$

따라서 구하고자 하는 상관 값 (11)은 다음과 같다.

$$\begin{aligned}R_{s_u,s_v}(\tau)&=\frac{1}{2}\big(-1-1\big)+\frac{\omega_4}{2}\big(R_{a,d}(0)-R_{a,d}(0)\big)\\&=-1.\end{aligned}$$

$\tau\neq 0$인 경우에, (11)의 우변에 있는 상관 값 $R_{a,c}(\tau)$, $R_{b,d}(\tau)$, $R_{a,d}(\tau)$, 그리고 $R_{b,c}(\tau)$는 모두 $\{-1-2^{\frac{n+e}{2}},-1,-1+2^{\frac{n+e}{2}}\}$의 분포를 갖는다. 그러므로 (11)의

값 중 절대값의 크기가 가장 큰 경우는 $-1-2^{\frac{n+e}{2}} \pm j2^{\frac{n+e}{2}}$ 이다.

따라서 새로운 수열군 $\mathcal{F}$의 모든 상관 값은 $2^{\frac{n+e+1}{2}}+1$로 상한된다. □

4. 모의실험 결과

$n=9$인 경우와 $n=10$인 경우에 위의 생성방법에 대한 모의실험을 통해서 실제 상관 분포를 구하였다. 각각에 대해서 앞에서 구한 상계를 만족하는지 확인하였다.

예시 1: $n=9$인 경우에 위에서 제안한 방식으로 주기 $2^9-1=511$이고 크기 $2^9=512$인 수열군을 생성할 수 있다. 생성된 수열군의 상관 분포는 다음과 같다.

$$R_{s_u,s_v} \in \{511,-1,31,-33,-17\pm 16j, 15\pm 16j, \\ -1\pm 32j, 31\pm 32j, -33\pm 32j\}.$$

위의 수열군 $\mathcal{F}$의 상관 값은 $2\times\sqrt{512}+1 \approx 46.3$로 상한됨을 확인할 수 있다.

예시 2: $n=10$인 경우에 위에서 제안한 방식으로 주기 $2^{10}-1=1023$이고 크기 $2^{10}=1024$인 수열군을 생성할 수 있다. 생성된 수열군의 상관 분포는 다음과 같다.

$$R_{s_u,s_v} \in \{1023,-1,31,-33,63,-65, \\ -1\pm 32j, -1\pm 64j, -33\pm 32j, \\ 31\pm 32j, 63\pm 64j, -65\pm 64j\}.$$

위의 수열군 $\mathcal{F}$의 상관 값은 $2\sqrt{2}\times\sqrt{1024}+1 \approx 91.5$로 상한됨을 확인할 수 있다.

5. 결론

본 논문에서는 주기 2^n-1인 이진 Gold 수열군을 이용해서 주기 2^n-1인 낮은 상관 특성을 갖는 크기가 2^n인 새로운 4진 수열군을 제안하였다. 새로운 수열군의 상관 값은 n이 홀수일 때 $2^{\frac{n+2}{2}}+1$, n이 2 mod 4일 때 $2^{\frac{n+3}{2}}+1$로 상한된다.

6. 감사의 글

본 연구는 지식경제부 및 정보통신연구진흥원의 IT 핵심기술개발사업의 일환으로 수행하였음. [2008-F-007-01, 3차원 환경에서의 지능형 무선 통신 시스템]

7. 참고문헌

[1] T. Kasami, "Weight distribution formular for some class of cyclic codes," Technical Report R-285 (AD 632574), Coordinated Science Laboratory, Univ. of Illinois, Urbana, Apr. 1966.

[2] T. Kasami, "Weight distribution of Bose-Chaudhuri-Hocquenghem codes," in *Cambinatorial Mathematics and Its Applications.* Chapel Hill, NC: Univ. of North Carolina Press, 1969.

[3] S.-C. Liu and J. F. Komo, "Nonbinary Kasami sequences over $GF(p)$," *IEEE Trans. Inf. Theory,* vol. 38, pp. 1409–1412, Jul. 1992.

[4] R. Gold, "Maximal recursive sequences with 3-valued recursive crosscorrelation functions," *IEEE Trans. Inf. Theory,* vol. 14, pp. 154–156, Jan. 1968.

[5] S. Boztas, R. Hammons, P. V. Kumar, "4-Phases Sequence with Near-Optimum Correlation Properties," *IEEE Trans. Inf. Theory,* vol. 38, no.3, pp. 1101–1113, May. 1992.

[6] P. Udaya, "Optimal and suboptimal quadriphase sequences derived from maximal length sequenes over $\mathbf{Z}_4$," *Appl. Algebra Eng. Commun Comput.,* vol. 9, no.2, pp. 161–191, 1998.

[7] X. H. Tang, P. Udaya, and P. Z. Fan, "A note on the optimal quadriphase sequences families," *IEEE Trans. Inf. Theory,* vol. 53, pp. 433–436, Jan. 2007.

[8] P. V. Kumar, T. Helleseth, and A. R. Calderbank, "Larger Families of Quaternary Sequences with Low Correlation," *IEEE Trans. Inf. Theory,* vol. 53, pp. 433–436, Jan. 2007.

[9] 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.