New Family of Binary Sequences with Three- or Five-valued Crosscorrelation Property

Sang-Hyo Kim and Jong-Seon No
School of EECS, Seoul National Univ., Seoul, Korea,
e-mail: kimsh@ccl.snu.ac.kr, jsno@snu.ac.kr

Abstract — **In this paper, new families of binary sequences $\mathcal{S}$ and $\mathcal{U}$ with 3 or 5-valued out-of-phase crosscorrelation property of period 2^n-1 are introduced.**

I. Introduction

Boztas and Kumar discovered a family of sequences, so-called Goldlike sequences[2] with optimal crosscorrelation property. In [4], Udaya introduced a family of binary sequences with five-valued crosscorrelation property. It corresponds to the case in which n is even of the Goldlike seqeunces.

Modifying the theorem partially contributed by Gold, Kasami[1] and Welch[3], we can construct the new family $\mathcal{S}$ of binary sequences with the same correlation property. Also a new family $\mathcal{U}$ of binary sequences associated with the sequences by Udaya is introduced. Special cases of the two newly constructed sequences can become Goldlike sequences and sequences by Udaya, respectively. The new family $\mathcal{S}$ and $\mathcal{U}$ have three and five-valued out-of-phase crosscorrelation property, respectively.

Let $\mathcal{C}$ be a family of M binary sequences of period N given as $\mathcal{C}=\{c_0(t),c_1(t),\cdots,c_{M-1}(t)\}$. The crosscorrelation function of sequences in $\mathcal{C}$ is given as $R_{i,j}(\tau)=\sum_{t=0}^{N-1}(-1)^{c_i(t+\tau)+c_j(t)}$, for $0\le i,j\le M-1$, $0\le\tau\le N-1$.

Let F_{2^n} be the finite field with 2^n elements. Trace function from F_{2^n} to F_{2^m} is denoted by $tr_m^n(\cdot)$. Note that an m-sequence of period 2^n-1 can be given as $tr_1^n(\alpha^t)$, where α is a primitive element of F_{2^n}. *Trace transform* of a function $s(x)$ defined on F_{2^n} and its inverse transform are given by $S(\lambda)=\sum_{x\in F_{2^n}}(-1)^{s(x)+tr_1^n(x\cdot\lambda)}$, $(-1)^{s(x)}=\frac{1}{2^n}\sum_{\lambda\in F_{2^n}}S(\lambda)\cdot(-1)^{tr_1^n(x\cdot\lambda)}$.

The binary m-sequences with three-valued crosscorrelation functions are given in the following theorem, which is in part due to Gold, Kasami and Welch.

Theorem 1 [Gold, Kasami[1] and Welch[3]]: Let $e=\gcd(n,k)$ and n/e be odd. Let $d=2^k+1$ or $d=2^{2k}-2^k+1$. Then the crosscorrelation of m-sequence $tr_1^n(\alpha^t)$ and its decimated sequence $tr_1^n(\alpha^{dt})$ by d takes on the following three values:

$$\begin{cases} -1+2^{(n+e)/2} & ,\ 2^{n-e-1}+2^{(n-e-2)/2} \text{ times} \\ -1 & ,\ 2^n-2^{n-e}-1 \text{ times} \\ -1-2^{(n+e)/2} & ,\ 2^{n-e-1}-2^{(n-e-2)/2} \text{ times.} \end{cases}$$

For the case of $e=1$, the m-sequence and its decimated sequence in Theorem 1 make the preferred pair. Using the above property, a family of sequence with 3-valued out-of-phase crosscorrelation property can be constructed.

II. New Family of Binary Sequences with Low Correlation Property

[1]This work was supported in part by BK21 and ITRC program of the Korean Ministry of Information and Communications.

The new binary sequence families with three or five-valued out-of-phase crosscorrelation property are given in the following theorems.

Theorem 2 : Let $e=\gcd(n,k)$ and $\frac{n}{e}=m$ be an odd integer. A family of binary sequences of period 2^n-1 with family size 2^n+1 is defined as $\mathcal{S}=\{s_i(t)\mid 0\le i\le 2^n,\ 0\le t\le 2^n-2\}$, where $s_i(t)$ is given as

$$s_i(t)=\begin{cases} tr_1^n(\alpha^{(t+i)})+\sum_{j=1}^{\frac{m-1}{2}} tr_1^n(\alpha^{(2^{e\cdot j}+1)t}), & \text{for } 0\le i\le 2^n-2 \\ \sum_{j=1}^{\frac{m-1}{2}} tr_1^n(\alpha^{(2^{e\cdot j}+1)t}), & \text{for } i=2^n-1 \\ tr_1^n(\alpha^t), & \text{for } i=2^n. \end{cases}$$

The distribution of correlation values of the new family $\mathcal{S}$ is given as

$$R_{i,j}(\tau)=\begin{cases} 2^n-1, & 2^n+1 \text{ times} \\ -1, & (2^n-2^{n-e}+1)\cdot(2^{2n}-2) \\ -1+2^{(n+e)/2}, & (2^{(n-e-1)}+2^{(n-e-2)/2})\cdot(2^{2n}-2) \\ -1-2^{(n+e)/2}, & (2^{(n-e-1)}-2^{(n-e-2)/2})\cdot(2^{2n}-2). \end{cases}$$

Theorem 3 : Let $e=\gcd(n,k)$ and $\frac{n}{e}=m$ be an even integer. A family of binary sequences of period 2^n-1 with family size 2^n+1 is defined as $\mathcal{U}=\{u_i(t)\mid 0\le i\le 2^n,\ 0\le t\le 2^n-2\}$, where $u_i(t)$ is given as

$$u_i(t)=\begin{cases} tr_1^n(\alpha^{(t+i)})+\sum_{j=1}^{\frac{m}{2}-1} tr_1^n(\alpha^{(2^{e\cdot j}+1)t}) \\ \quad +tr_1^{\frac{n}{2}}(\alpha^{(2^{\frac{n}{2}}+1)t}), & \text{for } 0\le i\le 2^n-2 \\ \sum_{j=1}^{\frac{m}{2}-1} tr_1^n(\alpha^{(2^{e\cdot j}+1)t})+tr_1^{\frac{n}{2}}(\alpha^{(2^{\frac{n}{2}}+1)t}), & \text{for } i=2^n-1 \\ tr_1^n(\alpha^t), & \text{for } i=2^n. \end{cases}$$

The binary sequence family $\mathcal{U}$ has the correlation distribution as follows:

$$R_{i,j}(\tau)=\begin{cases} 2^n-1, & 2^n+1 \text{ times} \\ -1, & 2^{2n-e}\cdot(2^n-2^{n-2e})+(2^{2n}-2) \\ -1+2^{(n+2e)/2}, & 2^{2n-e}\cdot(2^{n-2e-1}+2^{(n-2e-2)/2}) \\ -1-2^{(n+2e)/2}, & 2^{2n-e}\cdot(2^{n-2e-1}-2^{(n-2e-2)/2}) \\ -1+2^{n/2}, & (2^{2n}-2^{2n-e}-2)(2^{n-1}+2^{(n/2)-1}) \\ -1-2^{n/2}, & (2^{2n}-2^{2n-e}-2)(2^{n-1}-2^{(n/2)-1}). \end{cases}$$

References

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

[2] S. Boztas and P.V. Kumar, "Binary sequences with Gold-like correlation but larger linear span," *IEEE Trans. Inform. Theory*, vol. 40, pp. 532-537, Mar. 1994.

[3] H.M. Trachtenberg, "On the crosscorrelation functions of maximal linear recurring sequences," Ph.D. Thesis, Univ. of Southern California, 1970.

[4] P. Udaya, "Polyphase and frequency hopping sequences obtained from finite rings," Ph.D. dissertation, Dept. Elec. Eng., I.I.T., Kanpur, India, 1992.

0-7803-7501-7/02/$17.00©2002 IEEE.