Extended Binary Bent Sequences*

Dong-Joon Shin † and Jong-Seon No ‡

Abstract

The binary bent-lifted sequences with optimal correlation and balance properties are introduced in [8]. During the derivation of these sequences, new phase sequences are obtained. By using these new phase sequences, families of extended binary bent sequences with optimal correlation and balance properties are constructed and it is shown that this construction method gives more design flexibility than the method in [7] in the sense of sequence period.

1 Introduction

There have been many research results on the bent functions and binary bent sequences having optimal correlation and balance properties [1][2][3].

Rothaus [1] defined a *bent function* and gave some important classes of bent functions. Olsen, Scholtz, and Welch [2] constructed *bent sequences* using bent functions, which showed good correlation property such that the correlation values were not bigger than the square root of sequence period in magnitude and met the asymptotic lower bound on the correlation values by Welch [4]. Lempel and Cohn [3] extended the result of Olsen, Scholtz, and Welch to obtain the necessary and sufficient condition for bent functions such that the corresponding bent sequences had the correlation values claimed in [2]. No, Gil, and Shin [8] generalized the construction method of Olsen, Scholtz, and Welch to obtain generalized binary bent sequences and binary bent-lifted sequences.

No introduced No sequences by applying the lifting idea to Kasami sequences in the intermediate field [5][6]. No, Yang, Chung, and Song [7] proposed new construction method for families of binary sequences with optimal correlation property. Their method was to combine a binary sequence with ideal autocorrelation with a special phase sequence $tr_m^n(\alpha^{2t}) + \gamma\beta^t$, where $n = 2m$, α is a primitive element of F_{2^n}, $\beta = \alpha^{2^m+1}$, and $\gamma \in F_{2^m}$. By using their method, some sequences with optimal correlation property could be reinterpreted and also new sequences could be constructed. Since their approach is similarly used in this paper, the main theorem in [7] is given without proof as follows.

Theorem 1 [7] : Assume that $b(t) = \sum_{a\in I} \mathrm{tr}_1^m(\beta^{at})$ has the ideal autocorrelation property. Let $n = 2m$, α a primitive element of F_{2^n}, the finite field with 2^n elements, and $\beta = \alpha^{(2^n-1)/(2^m-1)}$. Define the following sequence family F.

$$F = \{s_\gamma(t) \mid \gamma \in F_{2^m} \text{ and } t = 0, 1, \ldots, 2^n - 2\},$$

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

†D. J. Shin is with Division of Electrical and Computer Engineering, Hanyang University, Seoul 133- 791, Korea (e-mail: djshin@hanyang.ac.kr).

‡J.-S. No is with the School of Electrical Engineering and Computer Science, Seoul National University, Seoul 151-742, Korea (e-mail: jsno@snu.ac.kr).

$$s_\gamma(t) = \sum_{a \in I} \mathrm{tr}_1^m([\mathrm{tr}_m^n(\alpha^{2t}) + \gamma\beta^t]^{ar})$$

where r is relatively prime to $2^m - 1$. Then the family F is optimal with respect to Welch's bound and has the out-of-phase autocorrelation and crosscorrelation values in $\{-1, 2^m - 1, -2^m - 1\}$. □

No sequences can be interpreted as an extension of m-sequence by applying a special phase sequence, $\mathrm{tr}_m^n(\alpha^{2t}) + \gamma\beta^t$ [7]. Besides m-sequence, any sequence with ideal autocorrelation such as the Legendre sequence and Hall's sextic residue sequence can be combined with the same phase sequence to produce a family of binary sequences with optimal correlation property. However, it is clear from Theorem 1 that there is only one phase sequence of $n = 2m$ and this causes the limited design flexibility. Therefore, it is desirable if we can find other phase sequences and if n can be other than $2m$. In this paper, some answers are given for them.

The family of *binary bent-lifted sequences* with optimal correlation and balance properties is obtained in [8]. During the derivation of binary bent-lifted sequences, new phase sequences are obtained and it is also shown that n can be other than $2m$. By using these new phase sequences, families of extended binary bent sequences with optimal correlation and balance properties can be constructed.

2 Generalized Binary Bent Sequences and Binary Bent-Lifted Sequences

In this section, the basic facts about generalized binary bent sequences and binary bent-lifted sequences [8] are summarized. Also, some results are explained without proofs. For more details and proofs, the readers are referred to [8]. Let $V_{2^e}^k$ be a k-dimensional vector space over F_{2^e}, whose element is expressed by $\underline{x} = (x_1, x_2, \cdots, x_k)$, $x_i \in F_{2^e}$. Let $f(\underline{x})$ be a function from $V_{2^e}^k$ to F_2. Then the modified trace transform of $f(\underline{x})$ is defined as follows:

Definition 2 : Let $f(\underline{x})$ be a function from $V_{2^e}^k$ to F_2. The modified trace transform of $f(\underline{x})$ is defined as

$$\hat{f}(\underline{\lambda}) = \frac{1}{\sqrt{2^{ek}}} \sum_{\underline{x} \in V_{2^e}^k} (-1)^{f(\underline{x}) + \mathrm{tr}_1^e(\underline{\lambda} \cdot \underline{x}^T)} \qquad (1)$$

where $\underline{x} = (x_1, x_2, \cdots, x_k)$ and $\underline{\lambda} = (\lambda_1, \lambda_2, \cdots, \lambda_k)$ are in $V_{2^e}^k$ and $\underline{\lambda} \cdot \underline{x}^T$ means the inner product of $\underline{\lambda}$ and $\underline{x}$. Then the inverse modified trace transform is given as

$$(-1)^{f(\underline{x})} = \frac{1}{\sqrt{2^{ek}}} \sum_{\underline{\lambda} \in V_{2^e}^k} \hat{f}(\underline{\lambda})(-1)^{\mathrm{tr}_1^e(\underline{\lambda} \cdot \underline{x}^T)}.$$

□

By using a function which has 1 or -1 as its modified trace transform values, new binary sequences with optimal correlation and balance properties, called *generalized binary bent sequences*, can be obtained as in the following theorem.

Theorem 3 [8] : Let $n = 2m = 4ek$, where m, e, and k are positive integers, α a primitive element of F_{2^n}, and $\delta \in F_{2^m}^* = F_{2^m} \backslash \{0\}$. Let $L(x)$ be an onto linear mapping from F_{2^n} to $V_{2^e}^{2k}$ defined as

$$L(x) = (\mathrm{tr}_e^n(\beta_1 \sigma x), \mathrm{tr}_e^n(\beta_2 \sigma x), \cdots, \mathrm{tr}_e^n(\beta_{2k} \sigma x)) \qquad (2)$$

where $\sigma \in F_{2^n} \backslash F_{2^m}$ and $\{\beta_1, \beta_2, \cdots, \beta_{2k}\}$ is a basis of F_{2^m} over F_{2^e}. Assume that the modified trace transform of $f(\underline{x})$ which is a function from $V_{2^e}^{2k}$ to F_2 takes on the values +1 or

-1. Then a family of *generalized binary bent sequences* defined by

$$\mathrm{S} = \{s_\eta(t) \mid \eta \in F_{2^m},\ 0 \le t \le 2^n - 2\},$$

$$s_\eta(t) = f\left(L(\alpha^t)\right) + \mathrm{tr}_1^n\left((\eta\sigma + \delta)\alpha^t\right) \quad (3)$$

has the out-of-phase autocorrelation and cross-correlation values in $\{-2^m-1, -1, 2^m-1\}$ with balance property. □

Let $m = 2ek$ and $f(\underline{x}) = \mathrm{tr}_1^e(u(\underline{x}))$ where $u(\underline{x})$ is a function from $V_{2^e}^k$ to F_{2^e}. Whenever each term of the function $u(\underline{x})$ has the degree $d = 2^i \bmod 2^e - 1$ for some integer i, we can modify it into 2^a-homogeneous function $f^h(\underline{x})$ by raising the power 2^{a-i} to each term, which can be given as follows:

$$f(\underline{x}) = \sum_{i=0}^{a} f_i(\underline{x}) = \sum_{i=0}^{a} [f_i(\underline{x})]^{2^{a-i}} = f^h(\underline{x})$$

where $f_i(\underline{x}) = \mathrm{tr}_1^e(u_i(\underline{x}))$, $u_i(\underline{x})$'s are functions consisting of terms with the same degree of $2^i \bmod 2^e - 1$, and 2^a is the maximum degree of the function $u(\underline{x})$. Some of generalized binary bent sequences defined in (3) can be rewritten as

$$s_\eta(t) = \mathrm{tr}_1^e\left(\sum_{i=0}^{a} u_i\left(L(\alpha^t)\right) + \mathrm{tr}_1^n\left((\eta\sigma + \delta)\alpha^t\right)\right) \quad (4)$$

where $n = 2m = 4ek$, $\eta \in F_{2^m}, \delta \in F_{2^m}^*$, and $\sigma \in F_{2^n} \backslash F_{2^m}$. Define *$2^a$-homogeneous generalized binary bent sequences* as follows:

$$\begin{aligned} s_\eta^h(t) &= f^h\left(L(\alpha^t)\right) \\ &\quad + \mathrm{tr}_1^e\left(\left[\mathrm{tr}_e^n\left((\eta\sigma + \delta)\alpha^t\right)\right]^{2^a}\right) \\ &= \sum_{i=0}^{a} \mathrm{tr}_1^e\left(\left[u_i\left(L(\alpha^t)\right)\right]^{2^{a-i}}\right) \\ &\quad + \mathrm{tr}_1^e\left(\left[\mathrm{tr}_e^n\left((\eta\sigma + \delta)\alpha^t\right)\right]^{2^a}\right) \quad (5) \end{aligned}$$

which are the same as the generalized binary bent sequences in (4).

Let t_1 and t_2 be the digits occurring in the base-T expansion of t, i.e., $t = t_1 T + t_2$, $0 \le t_1 \le 2^e - 2$, $0 \le t_2 \le T - 1$, where $T = \frac{2^n-1}{2^e-1}$. Let $L(\cdot)$ be the onto linear mapping defined in (2). Then the 2^a-homogenous generalized binary bent sequences (5) can be rewritten as

$$\begin{aligned} s_\eta^h(t) &= \mathrm{tr}_1^e\left(\alpha^{2^a T t_1}\left\{\sum_{i=0}^{a}\left[u_i\left(L(\alpha^{t_2})\right)\right]^{2^{a-i}}\right.\right. \\ &\quad \left.\left. + \left[\mathrm{tr}_e^n\left((\eta\sigma + \delta)\alpha^{t_2}\right)\right]^{2^a}\right\}\right) \quad (6) \end{aligned}$$

which is exactly the same as the generalized binary bent sequences in (4) and thus their correlation property is optimal in terms of Welch's lower bound.

Equation (6) can be rewritten as follows.

$$s_\eta^h(t) = \mathrm{tr}_1^e\left(\beta^{2^a(t_1 + g_\eta(t_2))}\right) \quad (7)$$

where

$$\begin{aligned} \beta^{2^a g_\eta(t_2)} &= \sum_{i=0}^{a}\left[u_i\left(L(\alpha^{t_2})\right)\right]^{2^{a-i}} \\ &\quad + \left[\mathrm{tr}_e^n\left((\eta\sigma + \delta)\alpha^{t_2}\right)\right]^{2^a} \quad (8) \end{aligned}$$

where $\beta = \alpha^T$. Note that the subsequence of $s_\eta^h(t)$ for a fixed value of t_2, $0 \le t_2 \le T - 1$, is either all-zero sequence if $g_\eta(t_2) = -\infty$ (i.e., $\beta^{2^a g_\eta(t_2)} = 0$) or a cyclic shift of the binary m-sequence $\mathrm{tr}_1^e(\beta^{2^a t_1})$ of period $2^e - 1$, otherwise. This result is summarized in the following lemma

Lemma 4 [8] : The number of zero columns in the two-dimensional expression of the 2^a-homogeneous generalized binary bent sequences (6) can be obtained as:

$$Z = \frac{2^{n-e} - 1}{2^e - 1}. \quad (9)$$

□

The correlation function $R(\tau)$ of the two binary sequences $s_\eta^h(t)$ and $s_\mu^h(t)$ is defined as

$$R(\tau) = \sum_{t=0}^{2^n-2} (-1)^{s_\eta^h(t) - s_\mu^h(t+\tau)}. \quad (10)$$

The possible correlation values are given in the following lemma and the family of binary bent-lifted sequences is defined in the following theorem.

Lemma 5 [8] : The number of occurrences of $g_\eta(t_2) = g_\mu(t_2+\tau), 0 \le t_2 \le T-1$, for $\tau \neq 0$ or $\eta \neq \mu$, that is, zero columns in the two-dimensional expression of the correlation function (10) of generalized binary bent sequences (3) or the 2^a-homogeneous generalized binary bent sequences (5) can be given as:

$$A = \begin{cases} \frac{2^{n-e}-2^m+2^{m-e}-1}{2^e-1} & \Leftrightarrow R(\tau) = -2^m - 1 \\ \frac{2^{n-e}-1}{2^e-1} & \Leftrightarrow R(\tau) = -1 \\ \frac{2^{n-e}+2^m-2^{m-e}-1}{2^e-1} & \Leftrightarrow R(\tau) = 2^m - 1. \end{cases} \quad (11)$$

□

Theorem 6 [8]: Let $n = 2m = 4ek$, where m, e, and k are positive integers. Let L be the onto linear mapping from F_{2^n} to $V_{2^e}^{2k}$ defined in (2), $\delta \in F_{2^m}^*$, $\sigma \in F_{2^n} \backslash F_{2^m}$, and r an integer relatively prime to 2^e-1, $1 \le r \le 2^e-2$. Assume that the modified trace transform of $\mathrm{tr}_1^e(u_i(\underline{x}))$ defined on $V_{2^e}^{2k}$ takes on +1 or −1. Then the family of *binary bent-lifted sequences* defined by

$$\mathbf{S}^r = \left\{ s_\eta^r(t) \mid \eta \in F_{2^m},\ 0 \le t \le 2^n - 2 \right\},$$

$$s_\eta^r(t) = \mathrm{tr}_1^e\left(\left[\sum_{i=0}^{a} \left[u_i\left(L(\alpha^t)\right)\right]^{2^{a-i}} + \left[\mathrm{tr}_e^n\left((\eta\sigma+\delta)\alpha^t\right)\right]^{2^a} \right]^r \right) \quad (12)$$

has the out-of-phase autocorrelation and cross-correlation values in $\{-2^m-1, -1, 2^m-1\}$ with balance property. □

3 Extended Binary Bent Sequences

Using the results from the binary bent-lifted sequences, new families of extended binary bent sequences with optimal correlation and balance properties are obtained as in the following theorem.

Theorem 7 : Consider the binary bent-lifted sequences defined in Theorem 6. Suppose that $b(t) = \sum_{d\in I} \mathrm{tr}_1^e(\beta^{dt})$ has the ideal autocorrelation property for an index set I. A family of extended binary bent sequences is defined as

$$E = \{ e_\eta(t) \mid 0 \le t \le 2^n - 2, \eta \in F_{2^m} \},$$

$$e_\eta(t) = \sum_{d\in I} \mathrm{tr}_1^e\left\{ \left[\sum_{i=0}^{a} \left[u_i\left(L(\alpha^t)\right)\right]^{2^{a-i}} + \left[\mathrm{tr}_e^n\left((\eta\sigma+\delta)\alpha^t\right)\right]^{2^a} \right]^{rd} \right\} \quad (13)$$

where r, $1 \le r \le 2^e-2$, is relatively prime to 2^e-1. Then, it has the same correlation and balance properties as those for the family of binary bent-lifted sequences.

Proof :

Let t_1 and t_2 be the digits occurring in the base-T expansion of t, i.e., $t = t_1 T + t_2$, $0 \le t_1 \le 2^e-2$, $0 \le t_2 \le T-1$, where $T = \frac{2^n-1}{2^e-1}$. Using the function $g_\eta(t_2)$ in (8), the two-dimensional representation of the above binary sequence can be written as:

$$e_\eta(t) = \sum_{d\in I} \mathrm{tr}_1^e(\beta^{2^a r(t_1 + g_\eta(t_2))d})$$

where the subsequence of $e_\eta(t)$ for a fixed value of t_2, $0 \le t_2 \le T-1$, is either all-zero sequence if $g_\eta(t_2) = -\infty$ (i.e., $\beta^{2^a g_\eta(t_2)} = 0$) or a decimated and shifted one of $b(t) = \sum_{d\in I} \mathrm{tr}_1^e(\beta^{dt})$, otherwise. Using the number of occurrence $g_\eta(t_2) = -\infty$ given in (9), it is easy to derive the balance property of the new binary sequences.

The correlation function $R(\tau)$ of the two new binary sequences $e_\eta(t)$ and $e_\mu(t)$ is

$$R(\tau) = \sum_{t_2=0}^{T-1} \sum_{t_1=0}^{2^e-2} (-1)^{\sum_{d\in I} \mathrm{tr}_1^e(f(t_1,t_2))}$$

where
$f(t_1,t_2)=\beta^{2^a r(t_1+g_\eta(t_2))d}-\beta^{2^a r(t_1+g_\mu(t_2+\tau))d}$.

Let $R_{sub}(\tau,t_2)$ be the autocorrelation function of subsequence of period 2^e-1 for a fixed t_2, $0\le t_2\le T-1$ defined as

$$R_{sub}(\tau,t_2)=\sum_{t_1=0}^{2^e-2}(-1)^{\sum_{d\in I}\mathrm{tr}_1^e(f(t_1,t_2))}.$$

Since $gcd(r,2^e-1)=1$, the subsequence is also a decimated and shifted version of $b(t)$. Therefore, we get the following autocorrelation function of the subsequence.

$$R_{sub}(\tau,t_2)=\begin{cases}2^e-1, & \text{if } g_\eta(t_2)=g_\mu(t_2+\tau)\\ -1, & \text{if } g_\eta(t_2)\neq g_\mu(t_2+\tau).\end{cases} \quad (14)$$

Then the correlation function of the sequences $e_\eta(t)$ and $e_\mu(t)$ can be represented as a summation of $R_{sub}(\tau,t_2)$ over t_2, $0\le t_2\le T-1$, that is,

$$R(\tau)=\sum_{t_2=0}^{T-1}R_{sub}(\tau,t_2).$$

Assume that for any nonzero τ or $\eta\neq\mu$, as t_2 varies from 0 to $T-1$, $g_\eta(t_2)=g_\mu(t_2+\tau)$ occurs A times. Then the correlation function of the sequences $s_\eta^r(t)$ and $s_\mu^r(t)$ can be derived as follows:

$$R(\tau)=2^eA-T.$$

Using the number of occurrences of the all-zero subsequences in (11), it is easy to derive that the out-of-phase autocorrelation and crosscorrelation functions take the values on $\{-2^m-1,-1,2^m-1\}$, which are the same as those for the binary bent-lifted sequences of the same period.

□

References

[1] O. S. Rothaus, "On bent functions," *J. Combin. Theory*, Series A. vol. 20, pp. 300-305, 1976.

[2] J. D. Olsen, R. A. Scholtz, and L. R. Welch, "Bent-function sequences," *IEEE Trans. Inform. Theory*, vol. 28, pp. 858-864, Nov. 1982.

[3] A. Lempel and M. Cohn, "Maximal families of bent sequences," *IEEE Trans. Inform. Theory*, vol.28, pp. 865-868, Nov. 1982.

[4] L. R. Welch, "Lower bounds on the maximal cross correlation of signals," *IEEE Trans. Inform. Theory*, vol. 20, pp. 396-399, May 1974.

[5] J. S. No and P. V. Kumar, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span," *IEEE Trans. Inform. Theory*, vol. 35, pp. 371-379, Mar. 1989.

[6] J. S. No, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span," Ph.D. Dissertation, University of Southern California, May 1988.

[7] J. S. No, K. C. Yang, H. B. Chung, and H. Y. Song, "New construction for families of binary sequences with optimal correlation properties," *IEEE Trans. Inform. Theory*, vol. 43, pp. 1596-1602, Sept. 1997.

[8] J. S. No, G. M. Gil, and D. J. Shin, "Generalized construction of binary bent sequences with optimal correlation property," *IEEE Trans. Inform. Theory*, vol. 49, pp. 1769-1780, July 2003.