Extended Binary Bent Sequences with Optimal Correlation and Balance Properties

Dong-Joon Shin
Division of ECE
Hanyang Univ., Seoul, Korea
e-mail: djshin@hanyang.ac.kr

Jong-Seon No
School of EECS
Seoul Nat'l Univ., Seoul, Korea
e-mail: jsno@snu.ac.kr

Abstract — **The generalized binary bent sequences and bent-lifted binary sequences with optimal correlation and balance properties are introduced in [1]. In this paper, it is shown that new extended binary bent sequences can be derived from the bent-lifted binary sequences by applying the similar method used to find extended binary sequences from No sequences [2].**

I. Bent-lifted Binary Sequences

Let $V_{2^e}^k$ be a k-dimensional vector space over F_{2^e}. Then the modified trace transform is defined as follows:

Definition 1 : 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

$$\hat{f}(\underline{\lambda}) = \frac{1}{\sqrt{2^{ek}}} \sum_{\underline{x} \in V_{2^e}^k} (-1)^{f(\underline{x}) + tr_1^e(\underline{\lambda} \cdot \underline{x}^T)},$$

and the inverse modified trace transform is given as

$$(-1)^{f(\underline{x})} = \frac{1}{\sqrt{2^{ek}}} \sum_{\underline{\lambda} \in V_{2^e}^k} \hat{f}(\underline{\lambda}) \cdot (-1)^{tr_1^e(\underline{\lambda} \cdot \underline{x}^T)}.$$

□

Let $m = ek$ and $f(\underline{x}) = tr_1^e(u(\underline{x}))$, 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} for 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 $f_i(\underline{x}) = tr_1^e(u_i(\underline{x}))$ and $u_i(\underline{x})$'s are functions consisting of terms with the same degree of $2^i \bmod 2^e - 1$ and 2^a is a maximum degree of function $u(\underline{x})$. Let $L(x)$ be an onto linear mapping from F_{2^n} to $V_{2^e}^{2k}$ defined as

$$L(x) = (tr_e^n(\beta_1 \sigma x), tr_e^n(\beta_2 \sigma x), \cdots, tr_e^n(\beta_{2k} \sigma x)), \quad (1)$$

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}. Some of generalized binary bent sequences can be rewritten as

$$s_\eta(t) = tr_1^e(\sum_{i=0}^{a} u_i(L(\alpha^t))) + tr_1^n((\eta\sigma + \delta) \cdot \alpha^t)), \quad (2)$$

where $n = 2m = 4ek$, $\eta \in F_{2^m}, \delta \in F_{2^m}^*$ and $\sigma \in F_{2^n} \backslash F_{2^m}$. These sequences have the out-of-phase autocorrelation and crosscorrelation values in $\{-2^m - 1, -1, 2^m - 1\}$ with balance property. Let us define 2^a-*homogeneous generalized binary bent sequences* as follows:

$$s_\eta^h(t) = f^h(L(\alpha^t)) + tr_1^e([tr_e^n((\eta\sigma + \delta) \cdot \alpha^t)]^{2^a})$$
$$= \sum_{i=0}^{a} tr_1^e(u_i(L(\alpha^t))^{2^{a-i}}) + tr_1^e(tr_e^n((\eta\sigma + \delta) \cdot \alpha^t)^{2^a}).$$

These are exactly the same as the generalized binary bent sequences in (2) and thus their correlation property is optimal in terms of Welch's lower bound.

Theorem 1 : Let $n = 2m = 4ek$, where m, e and k are positive integers. Let L be an onto linear mapping from F_{2^n} to $V_{2^e}^{2k}$ defined in (1) and $\delta \in F_{2^m}^*$. Let r be an integer relatively prime to $2^e - 1$, $1 \le r \le 2^e - 2$. Assume that the modified trace transform of $tr_1^e(u_i(\underline{x}))$ defined on $V_{2^e}^{2k}$ takes on $+1$ or -1. Then a family of bent-lifted binary sequences defined by

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

$$s_\eta^r(t) = tr_1^e([\sum_{i=0}^{a} [u_i(L(\alpha^t))]^{2^{a-i}} + [tr_e^n((\eta\sigma + \delta) \cdot \alpha^t)]^{2^a}]^r)$$

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

II. Extended Binary Bent Sequences

The extended binary bent sequences are obtained from the bent-lifted binary sequences as in the following theorem.

Theorem 2 : Consider the bent-lifted binary sequences defined in Theorem 1. Suppose that $b(t) = \sum_{d \in I} tr_1^e(\beta^{dt})$ has the ideal autocorrelation property for an index set I. The family of *extended binary bent sequences* is defined as

$$\{e_\eta(t) = \sum_{d \in I} tr_1^e\{[\sum_{i=0}^{a} u_i(L(\alpha^t))^{2^{a-i}} + tr_e^n((\eta\sigma + \delta) \cdot \alpha^t)^{2^a}]^{rd}\}\}.$$

where $0 \le t \le 2^n - 2, \eta \in F_{2^m}$. Then, it has the same correlation and balance properties as those for the family of bent-lifted binary sequences. □

References

[1] J.S. No, G.M. Gil and D.J. Shin, " Generalized construction of binary bent sequences with optimal correlation property," submitted to *IEEE Trans. Inform. Theory*

[2] 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, no. 5, pp. 1596-1602, Sept. 1997.

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

0-7803-7728-1/03/$17.00 ©2003 IEEE.