Generalized Construction of Binary Bent Sequences with Optimal Correlation Property

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

Gang-Mi Gil
School of EECS
Seoul Nat'l Univ., Seoul, Korea
e-mail: cominkil@ccl.snu.ac.kr

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

Abstract — **In this paper, we generalize the construction method of the family of binary bent sequences introduced by Olsen, Scholtz and Welch [1] to obtain a family of** *generalized binary bent sequences* **and** *bent-lifted binary sequences* **with optimal correlation and balance property by introducing the modified trace transform.**

I. Generalization of Binary Bent Sequences

Let $V_{2^e}^k$ be a k-dimensional vector space over F_{2^e}. Then we can modify the trace transform as:

Definition 1 : Let $f(\underline{x})$ be a function from $V_{2^e}^k$ to F_2. The modified trace transform of $f(\underline{x})$ and its inverse transform are defined as

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

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

where $\underline{x} = (x_1, x_2, \cdots, x_k)$ and $\underline{\lambda} = (\lambda_1, \lambda_2, \cdots, \lambda_k)$ in $V_{2^e}^k$.

Let $L(x)$ be an onto linear mapping from F_{2^n} to a $2k$-dimensional vector space $V_{2^e}^{2k}$, where $n = 4ek$. Let L^* denote an adjoint of L defined as: there is a unique ζ in F_{2^n} such that $tr_e^n(\zeta\cdot x) \equiv L(x)\cdot\underline{u}^T$. The mapping L^* is defined as $L^*(\underline{u}) = \zeta$.

Theorem 2 : Let $f(\underline{x})$ be a function from $V_{2^e}^{2k}$ to F_2. Then, the trace transform of the function $f(L(x))$ is given as

$$\hat{F}(\lambda) = \begin{cases} 0, & \lambda \notin \text{range}(L^*) \\ 2^{\frac{m}{2}}\cdot\hat{f}(\underline{u}), & \lambda\in\text{range}(L^*), L^*(\underline{u}) = \lambda, \end{cases}$$

where $\hat{f}(\underline{u})$ is the modified trace transform of $f(\underline{x})$ defined in Definition 1. □

Assume that the linear mapping $L(x)$ is defined as

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

and the range of L^* as range$(L^*) = \{\zeta\cdot\sigma \mid \zeta\in F_{2^m}\}$.

Using Theorem 2, we can construct a new family of binary sequences with balance and optimal correlation property as in the following theorem.

Theorem 3 : 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

$$\mathbf{S} = \{s_{\underline{z}}(t) \mid \underline{z}\in V_{2^e}^{2k},\ 0\le t\le 2^n-2\}$$

$$s_{\underline{z}}(t) = f(L(\alpha^t)) + tr_1^e(L(\alpha^t)\cdot\underline{z}^T) + tr_1^n(\delta\cdot\alpha^t) \qquad (1)$$

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

II. Family of Bent-lifted Binary Sequences

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 $u(\underline{x})$. Some of generalized binary bent sequences defined in (1) can be rewritten as

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

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

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

which are the same as the generalized binary bent sequences in (2).

Theorem 4 : 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.

References

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

[2] 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, no. 2, pp. 371-379, Mar. 1989.

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