Constructions of Bent Functions from Two Known Bent Functions

Jennifer Seberry
and
Xian-Mo Zhang

Department of Computer Science
The University of Wollongong
Wollongong
NSW 2522, AUSTRALIA

Dedicated to the memory of Alan Rahilly, 1947 – 1992

Abstract

A (1, -1)-matrix will be called a bent type matrix if each row and each column are bent sequences. A similar description can be found in Carlisle M. Adams and Stafford E. Tavares, Generating and counting binary sequences, *IEEE Trans. Inform. Theory*, vol. 36, no. 5, pp. 1170-1173, 1990, in which the authors use the properties of bent type matrices to construct a class of bent functions. In this paper we give a general method to construct bent type matrices and show that the bent sequence obtained from a bent type matrix is a generalized result of the Kronecker product of two known bent sequences.
Also using two known bent sequences of length 2^{2k-2} we can construct 2^k-2 bent sequences of length 2^{2k}, more than in the ordinary construction, which gives construct 10 bent sequences of length 2^{2k} from two known bent sequences of length length 2^{2k-2}.

Let V_n be the vector space of n tuples of elements from $GF(2)$. Let α, $\beta \in V_n$. Write $\alpha = (a_1, \cdots, a_n)$, $\beta = (b_1, \cdots, b_n)$, where $a_i, b_i \in GF(2)$. Write $\langle\alpha, \beta\rangle = \sum_{j=1}^{n} a_j b_j$ for the scalar product of α and β.

Definition 1 We call the function $h(x) = a_1x_1 + \cdots + a_nx_n + c$, a_j, $c \in GF(2)$, an *affine function,* in particular, $h(x)$ will be called a *linear function if* $c = 0$.

Definition 2 Let $f(x)$ be a function from V_n to $GF(2)$ (simply, a function on V_n). If

$$2^{-\frac{n}{2}} \sum_{x \in V_n} (-1)^{f(x)+\langle \beta, x \rangle} = \pm 1,$$

for every $\beta \in V_n$. We call $f(x)$ a *bent function* on V_n.

From Definition 2, bent functions on V_n only exist for even n. Bent functions were first introduced and studied by Rothaus [13]. Further properties, constructions and equivalence bounds for bent functions can be found in [2], [5], [7], [12], [16]. Kumar, Scholtz and Welch [6] defined and studied the bent functions from Z_q^n to Z_q. Bent functions are useful for digital communications, coding theory and cryptography [3], [1], [4], [7], [8], [10], [9], [11], [12].

We say $\alpha = (a_1, \cdots, a_n) < \beta = (b_1, \cdots, b_n)$ if there exists k, $1 \leqq k \leqq 2^n$, such that $a_1 = b_1, \ldots, a_{k-1} = b_{k-1}$ and $a_k = 0$, $b_k = 1$. Hence we can order all vectors in V_n by the relation $<$

$$\alpha_0 < \alpha_1 < \cdots < \alpha_{2^n-1},$$

where

$$\begin{array}{lcl} \alpha_0 & = & (0, \cdots, 0), \\ \alpha_1 & = & (0, \cdots, 1), \\ & \vdots & \\ \alpha_{2^{n-1}-1} & = & (0, 1, \cdots, 1), \\ \alpha_{2^{n-1}} & = & (1, 0, \cdots, 0), \\ & \vdots & \\ \alpha_{2^n-1} & = & (1, 1, \cdots, 1). \end{array}$$

Definition 3 Let $f(x)$ be a function from V_n to $GF(2)$. We call $(-1)^{f(\alpha_0)}$, $(-1)^{f(\alpha_1)}$, $\ldots$, $(-1)^{f(\alpha_{2^n})}$ the *sequence* of $f(x)$. We call the sequence of $f(x)$ a *bent sequence* if $f(x)$ is bent. A (1, -1)-sequence will be called an *affine sequence* a *(linear sequence)* if it is the sequence of an affine function (a linear function).

Definition 4 A (1, -1)-matrix H of order h will be called an *Hadamard matrix* if $HH^T = hI_h$.

If h is the order of an Hadamard matrix then h is 1, 2 or divisible by 4 [15]. A special kind of Hadamard matrix defined as following will be relevant.

Definition 5 *The Sylvester-Hadamard matrix (* or *Walsh-Hadamard matrix)* of order 2^n, denoted by H_n, is generated by the recursive relation

$$H_n = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix}, \quad n = 1, 2, \ldots, \quad H_0 = 1.$$

Let $f(x)$ be a function from V_n to $GF(2)$, ξ be the sequence (regarded as a row vector) of $f(x)$. Then the following three conditions are equivalent

(i) $f(x)$ is bent,

(ii) $2^{-\frac{1}{2}n}H_n\xi^T$ is a (1, -1)-row vector,

(iii) for any affine sequence l $\langle \xi, l\rangle = \pm 2^{\frac{1}{2}n}$.

The equivalence of (i) and (ii) can be found in many references, for example, [2], [16]. Note that any affine sequence of length 2^n is a row of $\pm H_n$ (see subsection 2.3) thus (ii) and (iii) are equivalent.

Definition 6 We call a (1, -1)-matrix of order $2^m \times 2^n$ a *bent type matrix* if each row is a bent sequence of length of 2^n and each column is a bent sequence of length of 2^m.

For example,

$$\begin{bmatrix} + & + & + & - \\ + & + & - & + \\ - & - & - & + \\ + & + & - & + \end{bmatrix},$$

where $+$ and $-$ denote 1 and -1 respectively, is a bent type matrix of order 4. A similar description can be found in [2, p. 1171].

Definition 7 A (1, -1)-matrix of order $2^m \times 2^n$ will be called *an affine type matrix* if each row is an affine sequence of length of 2^n and each column is an affine sequence of length of 2^m.

For example,

$$\begin{bmatrix} + & + & - & - & - & - & + & + \\ + & + & - & - & + & + & - & - \\ + & + & + & + & + & + & + & + \\ + & + & + & + & - & - & - & - \end{bmatrix}$$

is an affine type matrix of order 4×8. Any Walsh-Hadamard matrix is an affine type matrix (see subsection 2.3).

Definition 8 Let A_1 and A_2 be affine type matrices of order $2^m \times 2^n$. If $A_2 = QA_1P$ where Q and P are diagonal matrices of order 2^m and 2^n whose diagonals consist of ± 1 we say A_1 and A_2 *are equivalent.*

For example $\begin{bmatrix} - & + & + & - \\ - & + & + & - \\ + & - & - & + \\ + & - & - & + \end{bmatrix}$ and $\begin{bmatrix} + & + & + & + \\ + & + & + & + \\ + & + & + & + \\ + & + & + & + \end{bmatrix}$ are equivalent affine type matrices.

Definition 9 We call each of the four (1, -1)-sequences of length 2 $++$, $+-$, $--$, $-+$ E^1*-constructed.* Recursively, suppose E^n*-constructed* has been defined for $n = 1, \ldots, k-1$. The (1, -1)-sequence l will be said to be E^k*-constructed* if $l = (l', \pm l')$ where l' is E^{k-1}-constructed.

1 Bent Type Matrices

1.1 Bent Type Matrices Constructed from Affine Type Matrices

Lemma 1 *Let $b_0, b_1, \ldots, b_{2^n-1}$ be a bent sequence and $c_0, c_1, \ldots, c_{2^n-1}$ be an affine sequence, then b_0c_0, b_1c_1, $\ldots$, $b_{2^n-1}c_{2^n-1}$ is a bent sequence.*

Proof. Let $b_0, b_1, \ldots, b_{2^n-1}$ be the sequence of a bent function f from V_n to $GF(2)$ and $c_0, c_1, \ldots, c_{2^n-1}$ be the sequence of an affine function from V_n to $GF(2)$. Note that b_0c_0, b_1c_1, $\ldots$, $b_{2^n-1}c_{2^n-1}$ is the sequence of $f+g$. From Property 1 [6, p. 95] $f+g$ is bent. This proves the lemma. □

Bent type matrices can be used to construct bent sequences. For convenience, we quote a part of the Theorem found in [2]

Theorem 1 *Let $B = (b_{ij})$ be a bent type matrix of order $2^m \times 2^n$. Write $\beta_j = (b_{1j}, \ldots, b_{2^m j})$, $j = 1, \ldots, 2^n$ and $\alpha_i = (b_{i1} \ldots b_{i2^n})$, $j = 1, \ldots, 2^m$. Then both*

$$(2^{-\frac{1}{2}m}\beta_1 H_m, \cdots, 2^{-\frac{1}{2}m}\beta_{2^n} H_m)$$

and

$$(2^{-\frac{1}{2}n}\alpha_1 H_n, \cdots, 2^{-\frac{1}{2}n}\alpha_{2^m} H_n)$$

are bent sequences of length 2^{m+n}.

Proof. The proof can be found in [2, p. 1171]. □

Using the three equivalent conditions of bent functions in Section 1, both $2^{-\frac{1}{2}m}\beta_j H_m$ and $2^{-\frac{1}{2}n}\alpha_i H_n$ are bent sequences of length 2^m and 2^n. Hence Theorem 1 gives an example that the concatenation of some bent sequences is also bent. In general this is not true if some extra conditions are not satisfied. For example, each of $+++-$, $++-+$, $+-++$, $-+++$ is bent but the concatenation of the four sequences is not bent. The conditions for bent type matrices are restrictive. In this section we use affine type matrices to construct bent type matrices.

Theorem 2 *Let A be an affine type matrix of order $2^m \times 2^n$, P be a diagonal matrix of order 2^n whose diagonal is a bent sequence of length 2^n, say $a_0, a_1, \ldots, a_{2^n-1}$ and Q be a diagonal matrix of order 2^m whose diagonal is a bent sequence of length 2^m, say $b_0, b_1, \ldots, b_{2^m-1}$. Then QAP is a bent type matrix of order $2^m \times 2^n$.*

Proof. Since each row of A is an affine sequence, by Lemma 1, each row of AP is a bent sequence. Note each column of AP is still an affine sequence. By Lemma 1, each column of QAP is a bent sequence. Note each row of QAP is still a bent sequence. This proves the theorem. $\square$

To find the bent sequences using the special construction mentioned in Theorem 1, we first construct bent type matrices using Theorem 2. In particular, when the affine matrix A in Theorem 2 consists of only ones, the bent type matrix mentioned in Theorem 2 yields a bent sequence which is the Kronecker product (see [15]) of two bent sequences: $2^{-\frac{1}{2}m}\beta_j H_m$ and $2^{-\frac{1}{2}n}\alpha_i H_n$. Thus we have reproved Theorem 1 [16] using a different method.

Corollary 1 *Let τ_n denote the number of different bent sequences on V_n with first entries $+$ and $\sigma_{m\times n}$ denote the number of inequivalent affine type matrices of order $2^m \times 2^n$. Then there exist at least $\tau_m\tau_n\sigma_{m\times n}$ different bent type matrices of order $2^m \times 2^n$.*

Proof. We first note that for a fixed affine type matrix of order $2^m \times 2^n$, we can construct at least $\tau_m\tau_n$ different bent type matrices of order $2^m \times 2^n$ by using Theorem 2. Otherwise suppose B is an affine type matrix of order $2^m \times 2^n$, $Q_1 \neq Q_2$ or $P_1 \neq P_2$ but $Q_1BP_1 = Q_2BP_2$ where each Q_j and each P_j are the matrices mentioned in the proof of Theorem 2 whose first entries on the diagonals are $+$. Thus

$$Q_2Q_1BP_1P_2 = B. \tag{1}$$

Note that both Q_2Q_1 and P_1P_2 are diagonal matrices whose diagonals consist of ± 1. Let $Q_2Q_1 = diag(q_1, \cdots, q_{2^k})$, $P_1P_2 = diag(p_1, \cdots, p_{2^k})$. Let $B_1 = (b_1, \cdots, b_{2^k})^T$ be the first column of B. Compare the first columns on each side of (1) then we have $q_jb_jp_1 = b_j$, $j = 1, \ldots, 2^k$ thus $q_j = p_1$, $j = 1, \ldots, 2^k$ and thus $Q_2Q_1 = \pm I_{2^k}$ according as $p_1 = \pm 1$. Hence $Q_2Q_1 = eI_{2^m}$ and $P_1P_2 = eI_{2^n}$ where $e = \pm 1$. Since the first entries on the diagonals of Q_1, Q_2, P_1, P_2 are $+$, $Q_1 = Q_2$ and $P_1 = P_2$. This contradicts the assumption that $Q_1 \neq Q_2$ or $P_1 \neq P_2$.
Secondly we note that if B_1 and B_2 are inequivalent affine type matrices of order $2^m \times 2^n$, there exist no Q_1, Q_2, P_1, P_2 as mentioned in Theorem 2 such that

$Q_1B_1P_1 = Q_2B_2P_2$. Otherwise we would have $Q_2Q_1B_1P_1P_2 = B_2$. This contradicts the assumption that B_1 and B_2 are inequivalent. Hence we have established the corollary. □

1.2 Constructing Affine Type Matrices

Lemma 2 *Write* $H_n = \begin{bmatrix} l_0 \\ l_1 \\ \vdots \\ l_{2^n-1} \end{bmatrix}$ *where l_i is a row of H_n. Then l_i is the sequence of a linear function on V_n.*

Proof. The proof can be found in [14]. □

We can now establish:

Theorem 3 *An (1, -1)-matrix of order $2^m \times 2^n$ is an affine type matrix if and only if each row is E^n-constructed and each column is E^m-constructed.*

Proof. Note that H_n has 2^n rows and there exist 2^n linear sequences of length 2^n. By Lemma 2 each linear sequence is a row of H_n and thus each affine sequence is a row of $\pm H_n$. By the Definition of H_n each *row* of H_n and is E^n-constructed. Hence each affine sequence is E^n-constructed. On the other hand, there exist 2^{n+1} E^n-constructed (1 -1)-sequences and 2^{n+1} affine sequences. Thus each E^n-constructed (1, -1)-sequence is affine. □

Theorem 4 *Let A_1 be an affine type matrix of order $2^{m_1} \times 2^{n_1}$ with rank r_1 and A_2 be an affine type matrix of order $2^{m_2} \times 2^{n_2}$ with rank r_2. Then $A_1 \times A_2$ is an affine type matrix of order $2^{m_1+m_2} \times 2^{n_1+n_2}$ with rank r_1r_2, where $\times$ is the Kronecker product.*

Proof. Note that each row of $A_1 \times A_2$ is $E^{n_1+n_2}$-constructed and each column of $A_1 \times A_2$ is $E^{m_1+m_2}$-constructed. Hence by Theorem 3, $A_1 \times A_2$ is an affine type matrix.
Let C_1 be the invertible submatrix of order r_1 and C_2 be the invertible submatrix of order r_2. Hence by (25) of [16, p. 114], $C_1 \times C_2$ is invertible and thus the rank of $A_1 \times A_2$ is at least r_1r_2.
On the other hand, since the ranks of A_1 and A_2 are r_1 and r_2 respectively, write $\alpha_1, \ldots, \alpha_{r_1}$ for the linearly independent row vectors of A_1, and $\beta_1, \ldots, \beta_{r_2}$ for the linearly independent column vectors of A_2. Note that any row vector of A_1 is a

linear combination of $\alpha_1, \dots, \alpha_{r_1}$ and any row vector of A_2 is a linear combination of $\beta_1, \dots, \beta_{r_2}$. Any row vector of $A_1 \times A_2$ can be written as $\alpha \times \beta$, where α is a row vector of A_1 and β is a row vector of A_1. Write $\alpha = \sum_{j=1}^{r_1} a_j \alpha_j$ and $\beta = \sum_{j=1}^{r_2} b_j \beta_j$, where each a_j and $b_j \in GF(2)$. Hence

$$\alpha \times \beta = \sum_{i=1}^{r_1} \sum_{j=1}^{r_2} a_i b_j (\alpha_i \times \beta_j).$$

This proves that the rank of $A_1 \times A_2$ is at most $r_1 r_2$ and hence it is exactly $r_1 r_2$. □

Corollary 2 *(i) Let A be an affine type matrix of order $2^m \times 2^n$ with rank r and α be the row vector of an affine sequence of length 2^s. Then both $\alpha \times A$ and $A \times \alpha$ are affine type matrices of order $2^m \times 2^{n+s}$ with rank r.*

(ii) Let α be the row vector of an affine sequence of length 2^s. Then both $\alpha \times H_n$ and $H_n \times \alpha$ are affine type matrices of order $2^n \times 2^{n+s}$ with rank 2^n, where H_n is a Walsh-Hadamard matrix.

(iii) Let α be the row vector of an affine sequence of length 2^s and β be the row vector of an affine sequence of length 2^t. Then $\alpha \times \beta^T$ is an affine type matrix of order $2^t \times 2^s$ with rank 1.

Theorem 5 *For any integers k, n, m, $0 \leqq k \leqq n \leqq m$, there exists at least $(2^k - 1)!$ inequivalent (under the meaning in Definition 8) affine type matrices of order $2^m \times 2^n$ with rank 2^k.*

Proof. Write Walsh-Hadamard matrix $H_k = [h_1 \cdots h_{2^k}]$ where each h_j is a column vector of H_k. We first prove that any two $[h_1\, h_{j_2} \cdots h_{j_{2^k}}]$ and $[h_1\, h_{i_2} \cdots h_{i_{2^k}}]$ are inequivalent if $j_2, \cdots, j_{2^k}$ and $i_2, \cdots, i_{2^k}$ are two different rearrangements of $2, \dots, 2^k$. Otherwise if there exist diagonal matrices as mentioned in Definition 8, say $Q = diag(q_1, \cdots, q_{2^k})$, $P = diag(p_1, \cdots, p_{2^k})$, then $Q = \pm I_{2^k}$, $P = \pm I_{2^k}$, since

$$Q[h_1\, h_{j_2} \dots h_{j_{2^k}}]P = [h_1\, h_{i_2} \dots h_{i_{2^k}}], \tag{2}$$

and comparing the first columns on each side of (2), we have $q_j a_j p_1 = a_j$ where $(a_1, \cdots, a_{2^k})^T = h_1$, thus $q_j = p_1$, $j = 1, \dots, 2^k$ and thus $Q = \pm I_{2^k}$ according as $p_1 = \pm 1$. By the same reasoning we can prove that $P = \pm I_{2^k}$, according as $q_1 = \pm 1$. On the other hand, there exists an integer t, $2 \leqq t \leqq 2^k$ such as $j_t \neq i_t$ and thus $h_{j_t} \neq h_{i_t}$. We note that (2) cannot hold by comparing h_{j_t} and h_{i_t}. This proves the above statement.
Let R be the matrix of order $2^{m-k} \times 2^{n-k}$ with elements ones. By Theorem 4 $[h_1\, h_{j_2} \cdots h_{j_{2^k}}] \times R$ is an affine type matrix of order $2^m \times 2^n$ with rank 2^k. Permuting $j_2, \dots, j_{2^k}$ we obtain $(2^k - 1)!$ inequivalent matrices of this kind. □

Note that $0! = 1$ in Theorem 5.

Corollary 3 *For any positive integers n and m, $n \leqq m$, there exist at least $\sum_{k=0}^{n}(2^k - 1)!$ inequivalent (within the meaning of Definition 8) affine type matrices of order $2^m \times 2^n$.*

Proof. We note that if two matrices have different ranks they are inequivalent within the meaning of Definition 8. □

Corollary 4 *For any positive integers $n \leqq m$ there exists at least $\tau_n \tau_m \sum_{k=0}^{n}(2^k - 1)!$ different bent type matrices of order $2^m \times 2^n$.*

Proof. By Corollary 3 $\sigma_{m \times n} \geqq \sum_{k=1}^{n}(2^k - 1)!$. An application of Corollary 1 completes the proof. □

2 Combination of Two Known Bent Sequences

2.1 Enumeration of Nondegenerate Linear Transformations

We replace the real numbers 1, 2, ..., 2^n by the vectors

$$\alpha_0 = (0, \cdots, 0),\ \alpha_1 = (0, \cdots, 0, 1),\ \ldots,\ \alpha_{2^n - 1} = (1, 1, \cdots 1) \in V_n$$

respectively. Let φ be nondegenerate linear transformation on V_n. Set $\beta_j = \varphi(\alpha_j)$, $j = 0, 1, \ldots, 2^n - 1$.

Lemma 3 *If $e_1, e_2, \cdots, e_{2^n}$ i.e. $e_{\alpha_0}, e_{\alpha_1}, \cdots, e_{\alpha_{2^n-1}}$ is an affine sequence then $e_{\beta_0}, e_{\beta_1}, \cdots, e_{\beta_{2^n-1}}$ is also an affine sequence.*

Proof. Let $e_{\alpha_0}, e_{\alpha_1}, \cdots, e_{\alpha_{2^n-1}}$ be the sequence of the affine function $h(x_1, \ldots, x_n)$ on V_n. Set $h(\varphi(x_1, \ldots, x_n)) = g(x_1, \ldots, x_n)$ thus $h(\varphi(\alpha_j)) = g(\alpha_j)$ i.e. $h(\beta_j) = g(\alpha_j)$ and thus $e_{\beta_j} = (-1)^{h(\beta_j)} = (-1)^{g(\alpha_j)}$. Since $g(x_1, \ldots, x_n)$ is an affine function the sequence of g i.e. $e_{\beta_0}, e_{\beta_1}, \cdots, e_{\beta_{2^n-1}}$ is an affine sequence. □

Lemma 4 *There exist exactly $\Pi_{j=0}^{n-1}(2^n - 2^j)$ nondegenerate linear transformations on V_n.*

Proof. An equivalent statement is that there exist exactly $\Pi_{j=0}^{n-1}(2^n - 2^j)$ non-degenerate matrices of order n over $GF(2)$. Write $D = \begin{bmatrix} D_1 \\ \vdots \\ D_{2^n} \end{bmatrix}$, a non-degenerate matrix of order n over GF(2), where D_i is the i-th row of D. Note that D_1 has $2^n - 1$ choices (excluding the case that D_1 is the zero vector). After D_1 is fixed D_2 has $2^n - 2$ choices (excluding $D_2 = d_1 D_1$ where $d_1 = 0, 1$). After D_1 and D_2 are fixed D_3 has $2^n - 2^2$ choices (excluding $D_3 = d_1 D_1 + d_2 D_2$, where $d_1, d_2 = 0, 1$). Continuing this reasoning, after $D_1, \ldots, D_{n-1}$ have been fixed D_n has $2^n - 2^{n-1}$ choices (excluding $D_n = \sum_{j=1}^{n-1} d_j D_j$, where each $d_j = 0, 1$). In total D has $\Pi_{j=0}^{n-1}(2^n - 2^j)$ different choices. □

Lemma 5 *(i) All nondegenerate linear transformations on V_n can be divided into $2^n - 1$ disjoint classes $\Omega_1, \ldots, \Omega_{2^n-1}$ such that φ_1 and φ_2 are in the same class if and only if $\{\varphi_1(\alpha_0), \ldots, \varphi_1(\alpha_{2^{n-1}-1})\} = \{\varphi_2(\alpha_0), \ldots, \varphi_2(\alpha_{2^{n-1}-1})\}$,*

(ii) $|\Omega_j| = 2^{n-1}\Pi_{j=0}^{n-2}(2^{n-1} - 2^j)$, $j = 1, \ldots, 2^n - 1$.

Proof. Fix a nondegenerate linear transformation on V_n, say φ_0. Write $\varphi_0(\alpha_j) = \beta_j^0$, $j = 1, \ldots, 2^n - 1$.
We now count φ such that φ and φ_0 are in the same class i.e. $\{\varphi(\alpha_0), \ldots, \varphi(\alpha_{2^{n-1}-1}\} = \{\varphi_0(\alpha_0), \ldots, \varphi_0(\alpha_{2^{n-1}-1})\} = \{\beta_0, \ldots, \beta_{2^{n-1}-1}\}$. This counting is equivalent to counting the nondegenerate linear transformations on V_n , say ψ, such that $\{\psi(\beta_0), \ldots, \psi(\beta_{2^{n-1}-1})\} = \{\beta_0, \ldots, \beta_{2^{n-1}-1}\}$ because if we set $\varphi = \psi\varphi_0$ then $\{\varphi(\alpha_0), \ldots, \varphi_1(\alpha_{2^{n-1}-1})\} = \{\psi\varphi_0(\alpha_0), \ldots, \psi\varphi_0(\alpha_{2^{n-1}-1})\} = \{\psi(\beta_0), \ldots, \psi(\beta_{2^{n-1}-1})\} = \{\beta_0, \ldots, \beta_{2^{n-1}-1}\} = \{\varphi_0(\alpha_0), \ldots, \varphi_0(\alpha_{2^{n-1}-1})\}$. Since $\{\alpha_0, \ldots, \alpha_{2^{n-1}-1}\}$ contains $\alpha_1, \alpha_2, \alpha_{2^2}, \ldots \alpha_{2^{n-2}}$ but contains no α_j, $j = 2^{n-1}, \ldots, \alpha_{2^n-1}$, the rank of $\{\alpha_0, \ldots, \alpha_{2^{n-1}-1}\}$ is $n-1$. Note that any nondegenerate linear transformation preserves the rank of any set of vectors thus the rank of $\{\beta_0, \ldots, \beta_{2^{n-1}-1}\}$ is also $n-1$. Suppose $\beta_{j_1}, \ldots, \beta_{j_{n-1}} \in \{\beta_0, \ldots, \beta_{2^{n-1}-1}\}$ is a basis for $\{\beta_0, \ldots, \beta_{2^{n-1}-1}\}$. Add an appropriate vector in V_n, say γ, such that $\beta_{j_1}, \ldots, \beta_{j_{n-1}}, \gamma$ form a basis of V_n.
We now determine ψ such that $\{\psi(\beta_0), \ldots, \psi(\beta_{2^{n-1}-1})\} = \{\beta_0, \ldots, \beta_{2^{n-1}-1}\}$. For this purpose a necessary and sufficient condition is

$$
\begin{aligned}
\psi(\beta_{j1}) &= c_{11}\beta_{j_1} + c_{12}\beta_{j_2} + \cdots + c_{1n-1}\beta_{j_{n-1}} \\
\psi(\beta_{j2}) &= c_{21}\beta_{j_1} + c_{22}\beta_{j_2} + \cdots + c_{2n-1}\beta_{j_{n-1}} \\
&\vdots \\
\psi(\beta_{jn-1}) &= c_{n-11}\beta_{j_1} + c_{n-12}\beta_{j_2} + \cdots + c_{n-1n-1}\beta_{j_{n-1}} \\
\psi(\gamma) &= d_1\beta_{j_1} + d_2\beta_{j_2} + \cdots + d_{n-1}\beta_{j_{n-1}} + e\gamma
\end{aligned}
$$

where (c_{ij}) is a nondegenerate matrix of order $n-1$ on V_{n-1} and $e = 1$ since ψ is a nondegenerate linear transformation. By Lemma 4 (c_{ij}) has $\Pi_{j=0}^{n-2}(2^{n-1} - 2^j)$ choices. On the other hand $(d_1, \cdots, d_{n-1})$ has 2^{n-1} choices. In total ψ has $2^{n-1}\Pi_{j=0}^{n-2}(2^{n-1} - 2^j)$ choices. This proves that $|\Omega_j| = 2^{n-1}\Pi_{j=0}^{n-2}(2^{n-1} - 2^j)$, $j = 1, \ldots, 2^n - 1$. By Lemma 4 there exist $\Pi_{j=0}^{n-1}(2^n - 2^j)$ nondegenerate linear transformations on V_n. Thus we have $\Pi_{j=0}^{n-1}(2^n - 2^j)/2^{n-1}\Pi_{j=0}^{n-2}(2^{n-1} - 2^j) = 2^n - 1$ disjoint classes. □

2.2 Combination of Two Known Bent Functions

In this section we replace 1, 2, ..., 2^{2k-1} by vectors in V_{2k-1}: $\alpha_0 = (0,\cdots,0)$, $\alpha_1 = (0,\cdots,0,1)$, ..., $\alpha_{2^{2k-1}-1} = (1,1,\cdots,1)$ respectively.
Let φ be a nondegenerate linear transformation on V_{2k-1}. Set $\beta_j = \varphi(\alpha_j)$, $j = 0,1,\ldots$, $2^{2k-1}-1$. Suppose $\xi_1 = (a_1,\cdots,a_{2^{2k-2}})$ and $\xi_2 = (b_1,\cdots,b_{2^{2k-2}})$ are two bent sequences of length 2^{2k-2}. We now construct a (1, -1)-sequence of length 2^{2k}, denoted by $\eta = (\eta_1,\ \eta_2)$ where each η_j is of length 2^{2k-1}, by using ξ_1, ξ_2 and φ.

Construction 1 Let the β_0-th, the β_1-th, ... , and the $\beta_{2^{2k-2}-1}$-th entries of η_1 be $a_1,a_2,\ldots,a_{2^{2k-1}}$ respectively and let the $\beta_{2^{2k-2}}$-th, the $\beta_{2^{2k-2}+1}$-th, ... , and the $\beta_{2^{2k-1}-1}$-th entries of η_1 be $b_1,b_2,\ldots,b_{2^{2k-1}}$ respectively.
Next let the β_0-th, the β_1-th, ... , and the $\beta_{2^{2k-2}-1}$-th entries of η_2 be $a_1,a_2,\ldots,a_{2^{2k-1}}$ respectively and let the $\beta_{2^{2k-2}}$-th, the $\beta_{2^{2k-2}+1}$-th, ... , and the $\beta_{2^{2k-1}-1}$-th entries of η_2 be $-b_1,-b_2,\ldots,-b_{2^{2k-1}}$ respectively.
Set $\eta = (\eta_1,\ \eta_2)$.

Lemma 6 *η, in Construction 1, is a bent sequence of length 2^{2k}.*

Proof. Let L be an affine sequence of length 2^{2k}. By Theorem 3 $L = (l,\ \pm l)$ where l is an affine sequence of length 2^{2k-1}. Write $l = (e_1,e_2,\cdots,e_{2^{2k-1}})$ i.e. $l = (e_{\alpha_0},e_{\alpha_1},\cdots,e_{\alpha_{2^{2k-1}-1}})$. Write $l = (l_1,\ l_2)$ where each l_j is of length 2^{2k-2}. By Theorem 3, each l_j is an affine sequence of length 2^{2k-2} and $l_2 = \pm l_1$.
We now consider $\langle\eta,L\rangle = \langle\eta_1,l_1\rangle + \langle\eta_2,l_2\rangle$.
Case 1: $L = (l,\ l)$. By Construction 1

$$\langle\eta,L\rangle = \langle\eta_1,l\rangle + \langle\eta_2,l\rangle$$

where

$$\langle\eta_1,l\rangle = \sum_{j=1}^{2^{2k-2}} a_j e_{\beta_{j-1}} + \sum_{j=1}^{2^{2k-2}} b_j e_{\beta_{2^{2k-2}+j-1}}$$

and

$$\langle\eta_2,l\rangle = \sum_{j=1}^{2^{2k-2}} a_j e_{\beta_{j-1}} - \sum_{j=1}^{2^{2k-2}} b_j e_{\beta_{2^{2k-2}+j-1}}.$$

Thus

$$\langle\eta,L\rangle = 2\sum_{j=1}^{2^{2k-2}} a_j e_{\beta_{j-1}}. \tag{3}$$

Write $l^* = (e_{\beta_0},e_{\beta_1},\cdots,e_{\beta_{2^{2k}-1}})$, by Lemma 3, it is an affine sequence of length 2^{2k-1}. Write $l^* = (l_1^*,\ l_2^*)$ where each l_j^* is of length 2^{2k-2}. By Theorem 3 each l_j^* is an affine sequence of length 2^{2k-2}.

Thus (3) becomes $\langle \eta, L\rangle = 2\langle \xi_1, l_1^*\rangle$. Note that ξ_1 is a bent sequence of length 2^{2k-2} and l_1^* is an affine sequence of length 2^{2k-2}. Thus $\langle \xi_1, l_1^*\rangle = \pm 2^{k-1}$ and hence $\langle \eta, L\rangle = \pm 2^k$.
Case 2: $L = (l, \ -l)$. By Construction 1

$$\langle \eta, L\rangle = \langle \eta_1, l\rangle - \langle \eta_2, l\rangle$$

where

$$\langle \eta_1, l\rangle = \sum_{j=1}^{2^{2k-2}} a_j e_{\beta_{j-1}} + \sum_{j=1}^{2^{2k-2}} b_j e_{\beta_{2^{2k-2}+j-1}}$$

and

$$\langle \eta_2, l\rangle = \sum_{j=1}^{2^{2k-2}} a_j e_{\beta_{j-1}} - \sum_{j=1}^{2^{2k-2}} b_j e_{\beta_{2^{2k-2}+j-1}}.$$

Thus

$$\langle \eta, L\rangle = 2\sum_{j=1}^{2^{2k-2}} b_j e_{\beta_{2^{2k-2}+j-1}} = 2\langle \xi_2, l_2^*\rangle. \tag{4}$$

Note that ξ_2 is a bent sequence of length 2^{2k-2} and l_2^* is an affine sequence of length 2^{2k-2}. Thus $\langle \xi_2, l_2^*\rangle = \pm 2^{k-1}$ and hence (4) becomes $\langle \eta, L\rangle = \pm 2^k$.
Since L is arbitrary, by the three equivalent conditions of bent functions, η is a bent sequence. □

Construction 2 let the β_0-th, the β_1-th, ... , and the $\beta_{2^{2k-2}-1}$-th entries of η_1 be $a_1, a_2, \ldots, a_{2^{2k-1}}$ respectively and let the $\beta_{2^{2k-2}}$-th, the $\beta_{2^{2k-2}+1}$-th, ... , and the $\beta_{2^{2k-1}-1}$-th entries of η_1 be $b_1, b_2, \ldots, b_{2^{2k-1}}$ respectively.
Next let the β_0-th, the β_1-th, ... , and the $\beta_{2^{2k-2}-1}$-th entries of η_2 be $-a_1, -a_2, \ldots,$ $-a_{2^{2k-1}}$ respectively and let the $\beta_{2^{2k-2}}$-th, the $\beta_{2^{2k-2}+1}$-th, ... , and the $\beta_{2^{2k-1}-1}$-th entries of η_2 be $b_1, b_2, \ldots, b_{2^{2k-1}}$ respectively.
Set $\eta = (\eta_1 \ \eta_2)$.

Lemma 7 *η, in Construction 2, is a bent sequence of length 2^{2k}.*

Proof. The proof is similar to the proof of Lemma 6. □

2.3 Enumeration of Bent Sequences by Construction 1 and 2

Lemma 8 *Let Ξ_{2k}^1 denote the set of bent sequences of length 2^{2k} obtained via Construction 1 and Ξ_{2k}^2 denote the set of bent sequences of length 2^{2k} obtained via Construction 2. Then $\Xi_{2k}^1 \cap \Xi_{2k}^2 = \phi$ where ϕ denotes the empty set.*

Proof. Suppose we construct the bent sequence of length 2^{2k}, say $\eta = (\eta_1, \eta_2)$, by using the bent sequences $\xi_1 = (a_1, \cdots, a_{2^{2k-2}})$, $\xi_2 = (b_1, \cdots, b_{2^{2k-2}})$ and the nondegenerate linear transformation on V_{2k-1}, denoted by φ, in Construction 1. Similarly we suppose in Construction 2 we construct a bent sequence of length 2^{2k}, say $\eta' = (\eta_1', \eta_2')$, by using bent sequences $\xi_1 = (a_1', \cdots, a_{2^{2k-2}}')$, $\xi_2 = (b_1', \cdots, b_{2^{2k-2}}')$ and a nondegenerate linear transformation on V_{2k-1}, denoted by φ'.
Set $\beta_j = \varphi(\alpha_j)$, $\beta_j' = \varphi'(\alpha_j)$ where $j = 0, 1, \ldots, 2^{2k-1} - 1$. Note that $\beta_0 = \varphi(\alpha_0)$, $\beta_0' = \varphi'(\alpha_0)$ and $\alpha_0 = (0, 0, \cdots, 0)$ thus $\beta_0 = \beta_0' = (0, 0, \cdots, 0)$ since both φ and φ' are linear transformations.
In Construction 1 a_1 occurs in the β_0-th place of η_1 also a_1 occurs in the β_0-th place of η_2. Thus the first entries in η_1 and η_2 are the same.
In Construction 2 a_1' occurs in the β_0-th place of η_1' also $-a_1'$ occurs in the β_0-th place of η_2'. Thus the first entries in η_1' and η_2' are negatives each other. This proves that $\eta \neq \eta'$. Since both η and η' are arbitrary, $\Xi_{2k}^1 \cap \Xi_{2k}^2 = \phi$. □

By Lemma 5 we divide all nondegenerate linear transformations on V_{2k-1} into $2^{2k-1}-1$ disjoint classes: $\Omega_1, \ldots, \Omega_{2^{2k-1}-1}$ such that φ_1 and φ_2 are in the same class if and only if $\{\varphi_1(\alpha_0), \ldots, \varphi_1(\alpha_{2^{2k-2}-1})\} = \{\varphi_2(\alpha_0), \ldots, \varphi_2(\alpha_{2^{2k-2}-1})\}$.
We fix a $\varphi_s \in \Omega_s$, $s = 1, \ldots, 2^{2k-1} - 1$.

Lemma 9 *Suppose we construct the bent sequence of length 2^{2k}, say $\eta = (\eta_1, \eta_2)$, by using the bent sequences $\xi_1 = (a_1, \cdots, a_{2^{2k-2}})$, $\xi_2 = (b_1, \cdots, b_{2^{2k-2}})$ and the nondegenerate linear transformation on V_{2k-1}, denoted by φ_s where $\varphi_s \in \Omega_s$, in Construction 1 (2). Also in Construction 1 (2) we construct a bent sequence of length 2^{2k}, say $\eta' = (\eta_1', \eta_2')$, by using bent sequences $\xi_1 = (a_1', \cdots, a_{2^{2k-2}}')$, $\xi_2 = (b_1', \cdots, b_{2^{2k-2}}')$ and a nondegenerate linear transformation on V_{2k-1}, denoted by φ_t where $\varphi_t \in \Omega_t$. If $t \neq s$ then $\eta \neq \eta'$.*

Proof. Set $\beta_j = \varphi_s(\alpha_j)$, $\beta_j' = \varphi_t(\alpha_j)$ where $j = 0, 1, \ldots, 2^{2k-1} - 1$. Since $\{\varphi_s(\alpha_0), \ldots, \varphi_1(\alpha_{2^{2k-2}-1})\} \neq \{\varphi_t(\alpha_0), \ldots, \varphi_2(\alpha_{2^{2k-2}-1})\}$ i.e. $\{\beta_0, \ldots, \beta_{2^{2k-2}-1}\} \neq \{\beta_0', \cdots, \beta_{2^{2k-2}-1}'\}$ there exists a β such that $\beta \in \{\beta_0, \ldots, \beta_{2^{2k-2}-1}\}$ but $\beta \notin \{\beta_0', \ldots, \beta_{2^{2k-2}-1}'\}$.
In Construction 1 we note that $\beta \in \{\beta_0, \ldots, \beta_{2^{2k-2}-1}\}$ and we can suppose a_{i_0} occurs in the β-th place of η_1 and a_{i_0} also occurs in the β-th place of η_2. Thus the entry in the β-th place of η_1 and the entry in the β-th place of η_2 are the same.
For η', in Construction 1, we note that $\beta \notin \{\beta_0', \cdots, \beta_{2^{2k-2}-1}'\}$ thus $\beta \in \{\beta_{2^{2k-2}}', \ldots, \beta_{2^{2k-1}-1}'\}$ and we can suppose b_{j_0} occurs in the β-th place of η_1' and $-b_{j_0}'$ occurs in the β-th place of η_2'. Thus the entry in the β-th place of η_1' and the entry in the β-th place of η_2' are negatives of each other. This proves $\eta \neq \eta'$. Similarly we can prove the lemma for Construction 2. □

Lemma 10 *We fix $\varphi_s \in \Omega_s$. Suppose we construct the bent sequence of length 2^{2k}, say $\eta = (\eta_1, \eta_2)$, by using the bent sequences $\xi_1 = (a_1, \cdots, a_{2^{2k-2}})$, $\xi_2 = (b_1, \cdots, b_{2^{2k-2}})$ and the nondegenerate linear transformation on V_{2k-1}, say φ_s, in Construction 1*

(2). Also in Construction 1 (2) we construct a bent sequence of length 2^{2k}, say $\eta' = (\eta'_1, \eta'_2)$, by using bent sequences $\xi_1 = (a'_1, \cdots, a'_{2^{2k-2}})$, $\xi_2 = (b'_1, \cdots, b'_{2^{2k-2}})$ and the same nondegenerate linear transformation φ_s. If $(\xi'_1, \xi'_2) \neq (\xi_1, \xi_2)$ then $\eta \neq \eta'$.

Proof. Without any loss of generality suppose $a_{j_0} \neq a'_{j_0}$ for some j_0. By Construction 1, a_{j_0} occurs in the β_{j_0-1}-th place of η_1.
On the other hand, by Construction 1, a'_{j_0} occurs in the β_{j_0-1}-th place of η'_1. Thus $\eta_1 \neq \eta'_1$ and thus $\eta \neq \eta'$. Similarly we can prove the lemma for Construction 2. □

Theorem 6 *(i) Using two bent sequences of length 2^{2k-2}, say ξ_1 and ξ_2, we can construct $2^{2k} - 2$ different bent sequences of length 2^{2k}.*

(ii) Let τ_{2k} denote the number of the bent sequences of length 2^{2k}. Then $\tau_{2k} \geqq (2^{2k} - 2)\tau_{2k-2}^2$ for $k \geqq 2$.

Proof. (i) For the two bent sequences of length of 2^{2k-2} in Construction 1 (2), φ has $2^{2k-1} - 1$ choices. By Lemma 9, we can construct $2^{2k-1} - 1$ different bent sequences from the two known bent sequences of length of 2^{2k-2}. By Lemma 8, we have $2^{2k} - 2$ different bent sequences of length of 2^{2k} in Construction 1 and 2 in total.
(ii) Two bent sequences of length $2^{2k} - 2$ have τ_{2k-2}^2 choices. By Lemma 10 and (i) of the theorem, $\tau_{2k} \geqq (2^{2k} - 2)\tau_{2k-2}^2$ for $k \geqq 2$. □

We note that (i) of Theorem 6 gives many more bent sequences of length 2^{2k} from two known bent sequences of length 2^{2k-2} than the ordinary construction, which gives 10 bent sequences of length 2^{2k} from two known bent sequences of length 2^{2k-2} (see [2]).

2.4 Examples

Example 1 Since $\tau_2 = 8$, by Theorem 1, $\tau_4 \geqq (2^4 - 2)8^2 = 896$ and $\tau_6 \geqq (2^6 - 2)\tau_4^2 = 62 \cdot 896^2 = 62 \cdot 802816 = 49774592$.
Previously Adams and Tavares [2] estimated 48201728 as the number of bent sequences of length 2^6 including linear-based bent sequences and those constructed from four bent sequences of length 2^4.

Example 2 Let $k = 3$ in Construction. Let φ be a nondegenerate linear transformation on V_5. Write $\alpha_0 = (0,0,0,0,0)$, $\alpha_1 = (0,0,0,0,1)$, $\ldots$, $\alpha_{2^5-1} = (1,1,1,1,1)$. Define φ, a nondegenerate linear transformation on V_5 as follows

$$\varphi(\alpha_1) = (0,0,0,1,1), \quad \varphi(\alpha_2) = (0,0,1,1,0), \quad \varphi(\alpha_4) = (0,1,1,0,0),$$
$$\varphi(\alpha_8) = (1,1,0,0,0), \quad \varphi(\alpha_{16}) = (1,0,0,0,0).$$

Obviously, $\{\alpha_1,\ \alpha_2,\ \alpha_4,\ \alpha_8,\ \alpha_{16}\}$ is a basis of V_5.
Write $\varphi(\alpha_j) = \beta_j$ where $j = 0, 1, \ldots, 31$. Hence we have

$$\begin{array}{llll}
\beta_0 = (0,0,0,0,0), & \beta_1 = (0,0,0,1,1), & \beta_2 = (0,0,1,1,0), & \beta_3 = (0,0,1,0,1), \\
\beta_4 = (0,1,1,0,0), & \beta_5 = (0,1,1,1,1), & \beta_6 = (0,1,0,1,0), & \beta_7 = (0,1,0,0,1), \\
\beta_8 = (1,1,0,0,0), & \beta_9 = (1,1,0,1,1), & \beta_{10} = (1,1,1,1,0), & \beta_{11} = (1,1,1,0,1), \\
\beta_{12} = (1,0,1,0,0), & \beta_{13} = (1,0,1,1,1), & \beta_{14} = (1,0,0,1,0) & \beta_{15} = (1,0,0,0,1), \\
\beta_{16} = (1,0,0,0,0), & \beta_{17} = (1,0,0,1,1), & \beta_{18} = (1,0,1,1,0), & \beta_{19} = (1,0,1,0,1), \\
\beta_{20} = (1,1,1,0,0), & \beta_{21} = (1,1,1,1,1), & \beta_{22} = (1,1,0,1,0), & \beta_{23} = (1,1,0,0,1), \\
\beta_{24} = (0,1,0,0,0), & \beta_{25} = (0,1,0,1,1), & \beta_{26} = (0,1,1,1,0), & \beta_{27} = (0,1,1,0,1), \\
\beta_{28} = (0,0,1,0,0), & \beta_{29} = (0,0,1,1,1), & \beta_{30} = (0,0,0,1,0) & \beta_{31} = (0,0,0,0,1).
\end{array}$$

Choose two bent sequences of length 2^4:

$$\xi_1 = (++++++--+-+-+--+) = (a_1, \cdots, a_{16})$$

and

$$\xi_2 = (+++-+++-+++-----+) = (b_1, \cdots, b_{16}).$$

Let the β_0-th, the β_1-th, ..., the β_{15}-th entries of η_1 be $a_1,\ a_2, \ldots, a_{16}$ respectively and the β_{16}-th, the β_{17}-th, ..., the β_{31}-th entries of η_1 be $b_1,\ b_2, \ldots, b_{16}$ respectively. We have now constructed η_1:

$$\eta_1 = (++-+-++-+--++-++++-++-+-+-+-++).$$

Also let the β_0-th, the β_1-th, ..., the β_{15}-th entries of η_2 be $a_1,\ a_2, \ldots, a_{16}$ respectively and the β_{16}-th, the β_{17}-th, ..., the β_{31}-th entries of η_2 be $-b_1,\ -b_2, \ldots, -b_{16}$ respectively. We have now constructed η_2:

$$\eta_2 = (+-++++++----++-+-+--++---++-----+-).$$

Finally set $\eta = (\eta_1,\ \eta_2)$. By Lemma 6, this is a bent sequence of length of 2^6 by using ξ_1, ξ_2 and φ in Construction 1.
Similarly we can construct another bent sequence by using ξ_1, ξ_2 and φ in Construction 2. To do this set $\eta_1' = \eta_1$ and $\eta_2' = -\eta_2$. $\eta' = (\eta_1',\ \eta_2')$. By Lemma 7, this is a bent sequence of length of 2^6 by using ξ_1, ξ_2 and φ in Construction 2.

References

[1] C. M. Adams. On immunity against Biham and Shamir's "differential cryptanalysis". *Information Processing Letters*, 41:77–80, 1992.

[2] C. M. Adams and S. E. Tavares. Generating and counting binary bent sequences. *IEEE Transactions on Information Theory*, IT-36 No. 5:1170–1173, 1990.

[3] C. M. Adams and S. E. Tavares. The use of bent sequences to achieve higher-order strict avalanche criterion. Technical Report, TR 90-013, Department of Electrical Engineering, Queen's University, 1990.

[4] J. Detombe and S. Tavares. Constructing large cryptographically strong S-boxes. In *Advances in Cryptology - AUSCRYPT'92*. Springer-Verlag, Berlin, Heidelberg, New York, 1993. To appear.

[5] P. V. Kumar and R. A. Scholtz. Bounds on the linear span of bent sequences. *IEEE Transactions on Information Theory*, IT-29 No. 6:854–862, 1983.

[6] P. V. Kumar, R. A. Scholtz, and L. R. Welch. Generalized bent functions and their properties. *Journal of Combinatorial Theory*, Ser. A, 40:90–107, 1985.

[7] A. Lempel and M. Cohn. Maximal families of bent sequences. *IEEE Transactions on Information Theory*, IT-28 No. 6:865–868, 1982.

[8] V. V. Losev. Decoding of sequences of bent functions by means of a fast Hadamard transform. *Radiotechnika i elektronika*, 7:1479–1492, 1987.

[9] W. M. and O. Staffelbach. Nonlinearity criteria for cryptographic functions. In *Advances in Cryptology - EUROCRYPT'89*, volume 434, Lecture Notes in Computer Science, pages 549–562. Springer-Verlag, Berlin, Heidelberg, New York, 1990.

[10] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes.* New York: North-Holland, 1977.

[11] K. Nyberg. Perfect nonlinear S-boxes. In *Advances in Cryptology - EUROCRYPT'91*, volume 547, Lecture Notes in Computer Science, pages 378–386. Springer-Verlag, Berlin, Heidelberg, New York, 1991.

[12] J. D. Olsen, R. A. Scholtz, and L. R. Welch. Bent-function sequences. *IEEE Transactions on Information Theory*, IT-28 No. 6:858–864, 1982.

[13] O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory*, Ser. A, 20:300–305, 1976.

[14] J. Seberry and X. M. Zhang. Highly nonlinear 0-1 balanced functions satisfying strict avalanche criterion. In *Advances in Cryptology - AUSCRYPT'92*. Springer-Verlag, Berlin, Heidelberg, New York, 1993. To appear.

[15] W. D. Wallis, A. Penfold Street, and J. Seberry Wallis. *Combinatorics: Room Squares, sum-free sets, Hadamard Matrices*, volume 292 of Lecture Notes in Mathematics. Springer-Verlag, Berlin, Heidelberg, New York, 1972.

[16] R. Yarlagadda and J. E. Hershey. Analysis and synthesis of bent sequences. *IEE Proceeding (Part E)*, 136:112–123, 1989.

(Received 26/11/92)