Nonlinearly Balanced Boolean Functions and Their Propagation Characteristics (Extended Abstract)

Jennifer Seberry * Xian-Mo Zhang ** and Yuliang Zheng ***,

Department of Computer Science
University of Wollongong, Wollongong, NSW 2522, Australia
{jennie, xianmo, yuliang}@cs.uow.edu.au

Abstract. Three of the most important criteria for cryptographically strong Boolean functions are the balancedness, the nonlinearity and the propagation criterion. This paper studies systematic methods for constructing Boolean functions satisfying some or all of the three criteria. We show that concatenating, splitting, modifying and multiplying sequences can yield balanced Boolean functions with a very high nonlinearity. In particular, we show that balanced Boolean functions obtained by modifying and multiplying sequences achieve a nonlinearity higher than that attainable by any previously known construction method. We also present methods for constructing highly nonlinear balanced Boolean functions satisfying the propagation criterion with respect to *all but one or three* vectors. A technique is developed to transform the vectors where the propagation criterion is not satisfied in such a way that the functions constructed satisfy the propagation criterion of high degree while preserving the balancedness and nonlinearity of the functions. The algebraic degrees of functions constructed are also discussed, together with examples illustrating the various constructions.

1 Preliminaries

Let f be a function on V_n. The $(1,-1)$-sequence defined by $((-1)^{f(\alpha_0)}, (-1)^{f(\alpha_1)}, \ldots, (-1)^{f(\alpha_{2^n-1})})$ is called the *sequence* of f, and the $(0,1)$-sequence defined by $(f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{2^n-1}))$ is called the ***truth table*** of f, where α_i, $0 \leq i \leq 2^n - 1$, denotes the vector in V_n whose integer representation is i. A $(0,1)$-sequence ($(1,-1)$-sequence) is said ***balanced*** if it contains an equal number of zeros and ones (ones and minus ones). A function is balanced if its sequence is balanced.

* Supported in part by the Australian Research Council under the reference numbers A49130102, A9030136, A49131885 and A49232172.

** Supported in part by the Australian Research Council under the reference number A49130102.

*** Supported in part by the Australian Research Council under the reference number A49232172.

D.R. Stinson (Ed.): Advances in Cryptology - CRYPTO '93, LNCS 773, pp. 49-60, 1994.

The *Hamming weight* of a $(0,1)$-sequence (or vector) α, denoted by $W(\alpha)$, is the number of ones in α. The *Hamming distance* between two sequences α and β of the same length, denoted by $d(\alpha,\beta)$, is the number of positions where the two sequences differ. Given two functions f and g on V_n, the Hamming distance between them is defined as $d(f,g) = d(\xi_f,\xi_g)$, where ξ_f and ξ_g are the truth tables of f and g respectively. The *nonlinearity* of f, denoted by N_f, is the minimal Hamming distance between f and all affine functions on V_n, i.e., $N_f = \min_{i=0,1,\ldots,2^{n+1}-1} d(f,\varphi_i)$ where φ_0, φ_1, $\ldots$, $\varphi_{2^{n+1}-1}$ denote the affine functions on V_n.

A $(1,-1)$-matrix H of order n is called a *Hadamard* matrix if $HH^t = nI_n$, where H^t is the transpose of H and I_n is the identity matrix of order n. It is well known that the order of a Hadamard matrix is 1, 2 or divisible by 4 [11]. A special kind of Hadamard matrix, called *Sylvester-Hadamard matrix* or *Walsh-Hadamard matrix*, will be relevant to this paper. A Sylvester-Hadamard matrix of order 2^n, denoted by H_n, is generated by the following recursive relation

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

where $\otimes$ denotes the Kronecker product. Note that H_n can be represented as $H_n = H_s \otimes H_t$ for any s and t with $s + t = n$.

Sylvester-Hadamard matrices are closely related to linear functions, as is shown in the following lemma.

Lemma 1. *Write* $H_n = \begin{bmatrix} \ell_0 \\ \ell_1 \\ \vdots \\ \ell_{2^n-1} \end{bmatrix}$ *where* ℓ_i *is a row of* H_n. *Then* ℓ_i *is the sequence of* $h_i = \langle \alpha_i, x \rangle$, *a linear function, where* α_i *is a vector in* V_n *whose integer representation is* i *and* $x = (x_1, \ldots, x_n)$. *Conversely the sequence of any linear function on* V_n *is a row of* H_n.

From Lemma 1 the rows of H_n comprise the sequences of all linear functions on V_n. Consequently the rows of $\pm H_n$ comprise the sequences of all *affine* functions on V_n.

The following notation is very useful in obtaining the functional representation of a concatenated sequence. Let $\delta = (i_1, i_2, \ldots, i_p)$ be a vector in V_p. Then D_δ is a function on V_p defined by

$$D_\delta(y_1, y_2, \ldots, y_p) = (y_1 \oplus i_1 \oplus 1) \cdots (y_p \oplus i_p \oplus 1).$$

We now introduce the concept of bent functions.

Definition 2. A function f on V_n is called a *bent* function if

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

for all $\beta \in V_n$. Here $f(x) \oplus \langle \beta, x \rangle$ is regarded as a real-valued function. The sequence of a bent function is called a bent sequence.

From the definition we can see that bent functions on V_n exist only when n is even. It was Rothaus who first introduced and studied bent functions in 1960s, although his pioneering work was not published in the open literature until some ten years later [10]. Applications of bent functions to digital communications, coding theory and cryptography can be found in such as [2, 4, 7].

The following result can be found in an excellent survey of bent functions by Dillon [5].

Lemma 3. *Let f be a function on V_n, and let ξ be the sequence of f. Then the following four statements are equivalent:*

(i) f is bent.
(ii) $\langle \xi, \ell \rangle = \pm 2^{\frac{1}{2}n}$ for any affine sequence ℓ of length 2^n.
(iii) $f(x) \oplus f(x \oplus \alpha)$ is balanced for any non-zero vector $\alpha \in V_n$.
(iv) $f(x) \oplus \langle \alpha, x \rangle$ assumes the value one $2^{n-1} \pm 2^{\frac{1}{2}n-1}$ times for any $\alpha \in V_n$.

By (iv) of Lemma 3, if f is a bent function on V_n, then $f(x) \oplus h(x)$ is also a bent function for any affine function h on V_n. This property will be employed in constructing highly nonlinear balanced functions to be described in Section 4.

In this paper we are concerned with the propagation criterion whose formal definition follows (see also [1, 9]).

Definition 4. Let f be a function on V_n. We say that f satisfies

1. the *propagation criterion with respect to a non-zero vector α in V_n* if $f(x) \oplus f(x \oplus \alpha)$ is a balanced function.
2. the *propagation criterion of degree k* if it satisfies the propagation criterion with respect to all $\alpha \in V_n$ with $1 \leq W(\alpha) \leq k$.

Note that the SAC is equivalent to the propagation criterion of degree 1. Also note that the *perfect nonlinearity* studied by Meier and Staffelbach [6] is equivalent to the propagation criterion of degree n.

2 Properties of Balancedness and Nonlinearity

This section presents a number of results related to balancedness and nonlinearity. These include upper bounds for nonlinearity and properties of concatenated and split sequences. Due to the limit on space, proofs for some of the results are left to the full version of the paper [13].

The following lemma is very useful in calculating the nonlinearity of a function.

Lemma 5. *Let f and g be functions on V_n whose sequences are ξ_f and ξ_g respectively. Then the distance between f and g can be calculated by $d(f, g) = 2^{n-1} - \frac{1}{2}\langle \xi_f, \xi_g \rangle$.*

Corollary 6. *A function on V_n attains the upper bound for nonlinearities, $2^{n-1} - 2^{\frac{1}{2}n-1}$, if and only if it is bent.*

From Corollary 6, balanced functions can not attain the upper bound for nonlinearities, namely $2^{n-1} - 2^{\frac{1}{2}n-1}$. A slightly improved upper bound for the nonlinearities of balanced functions can be obtained by noting the fact that a balanced function assumes the value one an even number of times.

Corollary 7. *Let f be a balanced function on V_n ($n \geq 3$). Then the nonlinearity N_f of f is given by*

$$N_f \leq \begin{cases} 2^{n-1} - 2^{\frac{1}{2}n-1} - 2, & n \text{ even} \\ \lfloor\lfloor 2^{n-1} - 2^{\frac{1}{2}n-1} \rfloor\rfloor, & n \text{ odd} \end{cases}$$

where $\lfloor\lfloor x \rfloor\rfloor$ denotes the maximum even integer less than or equal to x.

The following lemma, first proved in [12], gives the lower bound of the nonlinearity of a function obtained by concatenating the sequences of two functions.

Lemma 8. *Let f_1 and f_2 be functions on V_n, and let g be a function on V_{n+1} defined by*

$$g(u, x_1, \ldots, x_n) = (1 \oplus u) f_1(x_1, \ldots, x_n) \oplus u f_2(x_1, \ldots, x_n). \tag{1}$$

Suppose that ξ_1 and ξ_2, the sequences of f_1 and f_2 respectively, satisfy $\langle \xi_1, \ell \rangle \leq P_1$ and $\langle \xi_2, \ell \rangle \leq P_2$ for any affine sequence ℓ of length 2^n, where P_1 and P_2 are positive integers. Then the nonlinearity of g satisfies $N_g \geq 2^n - \frac{1}{2}(P_1 + P_2)$.

As bent functions do not exist on V_{2k+1}, an interesting question is what functions on V_{2k+1} are highly nonlinear. The following result, as a special case of Lemma 8, shows that such functions can be obtained by concatenating bent sequences. This construction has also been discovered by Meier and Staffelbach in [6].

Corollary 9. *In the construction (1), if both f_1 and f_2 are bent functions on V_{2k}, then $N_g \geq 2^{2k} - 2^k$.*

A similar result can be obtained when sequences of four functions are concatenated.

Lemma 10. *Let f_0, f_1, f_2 and f_3 be functions on V_n whose sequences are ξ_0, ξ_1, ξ_2 and ξ_3 respectively. Assume that $\langle \xi_i, \ell \rangle \leq P_i$ for each $0 \leq i \leq 3$ and for each affine sequence ℓ of length 2^n, where each P_i is a positive integer. Let g be a function on V_{n+2} defined by*

$$g(y, x) = \bigoplus_{i=0}^{3} D_{\alpha_i}(y) f_i(x) \tag{2}$$

where $y = (y_1, y_2)$, $x = (x_1, \ldots, x_n)$ and α_i is a vector in V_2 whose integer representation is i. Then $N_g \geq 2^{n+1} - \frac{1}{2}(P_0 + P_1 + P_2 + P_3)$. In particular, when n is even and f_0, f_1, f_2 and f_3 are all bent functions on V_n, $N_g \geq 2^{n+1} - 2^{\frac{1}{2}n+1}$.

We have discussed the concatenation of sequences of functions including bent functions. The following lemma deals with the other direction, namely splitting bent sequences.

Lemma 11. *Let $f(x_1, x_2, \ldots, x_{2k})$ be a bent function on V_{2k}, η_0 be the sequence of $f(0, x_2, \ldots, x_{2k})$, and η_1 be the sequence of $f(1, x_2, \ldots, x_{2k})$. Then for any affine sequence ℓ of length 2^{2k-1}, we have $-2^k \leq \langle \eta_0, \ell \rangle \leq 2^k$ and $-2^k \leq \langle \eta_1, \ell \rangle \leq 2^k$.*

A consequence of Lemma 11 is that the nonlinearity of $f(0, x_2, \ldots, x_{2k})$ and $f(1, x_2, \ldots, x_{2k})$ is at least $2^{2k-2} - 2^{k-1}$. It is interesting to note that concatenating and splitting bent sequences both achieve the same nonlinearity.

Splitting bent sequences can also result in balanced functions. Let ℓ_i be the ith row of H_k where $i = 0, 1, \ldots, 2^k - 1$. Note that ℓ_0 is an all-one sequence while ℓ_1, ℓ_2, ..., ℓ_{2^k-1} are all balanced sequences. The concatenation of the rows, $(\ell_0, \ell_1, \ldots, \ell_{2^k-1})$, is a bent sequence [1]. Denote by $f(x_1, x_2, \ldots, x_{2k})$ the function corresponding to the bent sequence. Let ξ be the second half of the bent sequence, namely, $\xi = (\ell_{2^{k-1}}, \ell_{2^{k-1}+1}, \ldots, \ell_{2^k-1})$. Then ξ is the sequence of $f(1, x_2, \ldots, x_{2k})$. Since all ℓ_i, $i = 2^{k-1}, 2^{k-1}+1, \ldots, 2^k - 1$, are balanced, $f(1, x_2, \ldots, x_{2k})$ is a balanced function. The nonlinearity of the function is at least $2^{2k-2} - 2^{k-1}$.

By permuting $\{\ell_{2^{k-1}}, \ell_{2^{k-1}+1}, \ldots, \ell_{2^k-1}\}$, we obtain a new balanced sequence $\xi' = (\ell'_{2^{k-1}}, \ell'_{2^{k-1}+1}, \ldots, \ell'_{2^k-1})$ that has the same nonlinearity as that of ξ. Now let $\xi'' = (e_{2^{k-1}}\ell'_{2^{k-1}}, e_{2^{k-1}+1}\ell'_{2^{k-1}+1}, \ldots, e_{2^k-1}\ell'_{2^k-1})$, where each e_i is independently selected from $\{1, -1\}$. ξ'' is also a balanced sequence with the same nonlinearity. The total number of balanced sequences obtained by permuting and changing signs is $2^{2^{k-1}} \cdot 2^{k-1}!$. These sequences are all different from one another but have the same nonlinearity.

3 Highly Nonlinear Balanced Functions

Note that a bent sequence on V_{2k} contains $2^{2k-1} + 2^{k-1}$ ones and $2^{2k-1} - 2^{k-1}$ zeros, or vice versa. As is observed by Meier and Staffelbach [6], changing 2^{k-1} positions in a bent sequence yields a balanced function having a nonlinearity of at least $2^{2k-1} - 2^k$. This nonlinearity is the same as that obtained by concatenating four bent sequences of length 2^{2k-2} (see Lemma 10).

It is well-known that the maximum nonlinearity of functions on V_n coincides with the covering radius of the first order binary Reed-Muller code $R(1, n)$ of length 2^n, many results on covering radius of $R(1, n)$ (see [3]) have direct implications on the nonlinearity of functions. In particular, using a result of [8], we can construct unbalanced functions on V_{2k+1}, $k \geq 7$, whose nonlinearity is at least $2^{2k} - \frac{108}{128}2^k$, a higher value than $2^{2k} - 2^k$ achieved by the construction in Corollary 9. One might tempt to think that modifying the sequences in [8] would result in balanced functions with a higher nonlinearity than that obtained by concatenating or splitting bent sequences. We find that it is not the case. We

take V_{15} for an example. The Hamming weight of the sequences on V_{15}, which have the largest nonlinearity of 16276, is 16492. Changing 54 positions makes them balanced. The nonlinearity of the resulting functions is 16222, smaller than 16256 achieved by concatenating two bent sequences of length 2^{14} (see Corollary 9).

In the following we show how to modify bent sequences of length 2^{2k} constructed from Hadamard matrices in such a way that the resulting functions are balanced and have a much higher nonlinearity than that attainable by concatenating four bent sequences. This result, in conjunction with sequences in [8], allows us to construct balanced functions on V_{2k+15}, $k \geq 7$, that have a higher nonlinearity than that achieved by concatenating or splitting bent sequences.

3.1 On V_{2k}

Note that an even number $n \geq 4$ can be expressed as $n = 4t$ or $n = 4t+2$, where $t \geq 1$. As the first step towards our goal, we have the following lemma whose proof is left to the full paper [13]:

Lemma 12. *For any integer $t \geq 1$ there exists*

(i) a balanced function f on V_{4t} such that $N_f \geq 2^{4t-1} - 2^{2t-1} - 2^t$,
(ii) a balanced function f on V_{4t+2} such that $N_g \geq 2^{4t+1} - 2^{2t} - 2^t$.

With the above result as a basis, we consider an iterative procedure to further improve the nonlinearity of a function constructed. Note that an even number $n \geq 4$ can be expressed as $n = 2^m$, $m \geq 2$, or $n = 2^s(2t+1)$, $s \geq 1$ and $t \geq 1$.

Consider the case when $n = 2^m$, $m \geq 2$. We start with the bent sequence obtained by concatenating the rows of $H_{2^{m-1}}$. The sequence consists of $2^{2^{m-1}}$ sequences of length $2^{2^{m-1}}$. Now we replace the all-one leading sequence with a bent sequence of the same length, which is obtained by concatenating the rows of $H_{2^{m-2}}$. The length of the new leading sequence becomes $2^{2^{m-2}}$. It is replaced by another bent sequence of the same length. This replacing process is continued until the length of the all-one leading sequence is $2^2 = 4$. To finish the procedure, we replace the leading sequence $(1,1,1,1)$ with $(1,-1,1,-1)$. The last replacement makes the entire sequence balanced. By induction on $s = 2,3,4,\ldots$, it can be proved that the nonlinearity of the function obtained is at least

$$2^{2^m-1} - \frac{1}{2}(2^{2^{m-1}} + 2^{2^{m-2}} + \cdots + 2^{2^2} + 2 \cdot 2^2).$$

The modifying procedure for the case of $n = 2^s(2t+1)$, $s \geq 1$ and $t \geq 1$, is the same as that for the case of $n = 2^m$, $m \geq 2$, except for the last replacement. In this case, the replacing process is continued until the length of the all-one leading sequence is 2^{2t+1}. The last leading sequence is replaced by $\ell_0^* = (e_{2^t}, e_{2^t+1}, \ldots, e_{2^{t+1}-1})$, the second half of the bent sequence $(e_0, e_1, \ldots, e_{2^{t+1}-1})$, where each e_i is a row of H_{t+1}. Again by induction on $s = 1,2,3,\ldots$, it can be proved that the nonlinearity of the resulting function is at least

$$2^{2^s(2t+1)-1} - \frac{1}{2}(2^{2^{s-1}(2t+1)} + 2^{2^{s-2}(2t+1)} + \cdots + 2^{2(2t+1)} + 2^{2t+1} + 2^{t+1}).$$

We have completed the proof for the following

Theorem 13. *For any even number $n \geq 4$, there exists a balanced function f^* on V_n whose nonlinearity is*

$$N_{f^*} \geq \begin{cases} 2^{2^m-1} - \frac{1}{2}(2^{2^{m-1}} + 2^{2^{m-2}} + \cdots + 2^{2^2} + 2 \cdot 2^2), & n = 2^m, \\ 2^{2^s(2t+1)-1} - \frac{1}{2}(2^{2^{s-1}(2t+1)} + 2^{2^{s-2}(2t+1)} + \cdots + 2^{2(2t+1)} + 2^{2t+1} + 2^{t+1}), & n = 2^s(2t+1). \end{cases}$$

Let $\zeta = (\zeta_0, \zeta_1, \ldots, \zeta_{2^k-1})$ be a sequence of length 2^{2k} obtained by modifying a bent sequence. Permuting and changing signs discussed in Section 2 can also be applied to ζ. In this way we obtain in total $2^{2^k} \cdot 2^k!$ different balanced functions, all of which have the same nonlinearity. Even more functions can be obtained by observing the fact that the leading sequence ζ_0 has exactly the same structure as the large sequence ζ, and hence permuting and changing signs can also be applied to ζ_0.

3.2 On V_{2k+1}

Lemma 14. *Let f_1 be a function on V_s and f_2 be a function on V_t. Then $f_1(x_1, \ldots, x_s) \oplus f_2(y_1, \ldots, y_t)$ is a balanced function on V_{s+t} if either f_1 or f_2 is balanced.*

Let ξ_1 be the sequence of f_1 on V_s and ξ_2 be the sequence of f_2 on V_t. Then it is easy to verify that the Kronecker product $\xi_1 \otimes \xi_2$ is the sequence of $f_1(x_1, \ldots, x_s) \oplus f_2(y_1, \ldots, y_t)$.

Lemma 15. *Let f_1 be a function on V_s and f_2 be a function on V_t. Let g be a function on V_{s+t} defined by*

$$g(x_1, \ldots, x_s, y_1, \ldots, y_s) = f_1(x_1, \ldots, x_s) \oplus f_2(y_1, \ldots, y_t).$$

Suppose that ξ_1 and ξ_2, the sequences of f_1 and f_2 respectively, satisfy $\langle \xi_1, \ell \rangle \leq P_1$ and $\langle \xi_2, \ell \rangle \leq P_2$ for any affine sequence ℓ of length 2^n, where P_1 and P_2 are positive integers. Then the nonlinearity of g satisfies $N_g \geq 2^{s+t-1} - \frac{1}{2}P_1 \cdot P_2$.

Let ξ_1 be a balanced sequence of length 2^{2k} that is constructed using the method in the proof of Theorem 13, where $k \geq 2$, Let ξ_2 be a sequence of length 2^{15} obtained by the method of [8]. Note that the nonlinearity of ξ_2 is 16276, and there are 13021 such sequences. Denote by f_1 the function corresponding to ξ_1 and by f_2 the function corresponding to ξ_2. Let

$$f(x_1, \ldots, x_{2k}, x_{2k+1}, \ldots, x_{2k+15}) = f_1(x_1, \ldots, x_{2k}) \oplus f_2(x_{2k+1}, \ldots, x_{2k+15}) \quad (3)$$

Then

Theorem 16. *The function f defined by (3) is a balanced function on V_{2k+15}, $k \geq 2$, whose nonlinearity is at least*

$$N_f \geq \begin{cases} 2^{2^m+14} - 108(2^{2^{m-1}} + 2^{2^{m-2}} + \cdots + \\ \qquad 2^{2^2} + 2 \cdot 2^2), & 2k = 2^m, \\ 2^{2^s(2t+1)+14} - 108(2^{2^{s-1}(2t+1)} + 2^{2^{s-2}(2t+1)} + \cdots + \\ \qquad 2^{2(2t+1)} + 2^{2t+1} + 2^{t+1}), & 2k = 2^s(2t+1). \end{cases}$$

Proof. Let $\xi = \xi_1 \otimes \xi_2$. Then ξ is the sequence of f. Let ℓ be an arbitrary affine sequence of length 2^{2k+15}. Then $\ell = \pm \ell_1 \otimes \ell_2$, where ℓ_1 is a linear sequence of length 2^{2k} and ℓ_2 is a linear sequence of length 2^{15}. Thus

$$\langle \xi_1, \ell_1 \rangle \leq \begin{cases} 2^{2^{m-1}} + 2^{2^{m-2}} + \cdots + 2^{2^2} + 2 \cdot 2^2, & 2k = 2^m, \\ 2^{2^{s-1}(2t+1)} + 2^{2^{s-2}(2t+1)} + \cdots + 2^{2(2t+1)} + 2^{2t+1} + 2^{t+1}, & 2k = 2^s(2t+1). \end{cases}$$

and

$$\langle \xi_2, \ell_2 \rangle \leq 2 \cdot (2^{14} - 16276) = 216$$

By Lemma 15, the theorem is true. □

The nonlinearity of a function on V_{2k+15} constructed in this section is larger than that obtained by concatenating or splitting bent sequences for all $k \geq 7$.

4 Constructing Highly Nonlinear balanced Functions Satisfying High Degree Propagation Criterion

This section presents two methods for constructing highly nonlinear balanced functions satisfying the propagation criterion.

4.1 Basic Construction

On V_{2k+1} Let f be a bent function on V_{2k}, and let g be a function on V_{2k+1} defined by

$$\begin{aligned} & g(x_1, x_2, \ldots, x_{2k+1}) \\ & = (1 \oplus x_1) f(x_2, \ldots, x_{2k+1}) \oplus x_1 (1 \oplus f(x_2, \ldots, x_{2k+1})) \\ & = x_1 \oplus f(x_2, \ldots, x_{2k+1}). \end{aligned} \tag{4}$$

Lemma 17. *The function g defined in (4) satisfies the propagation criterion with respect to all non-zero vectors $\gamma \in V_{2k+1}$ with $\gamma \neq (1, 0, \ldots, 0)$.*

Proof. Let $\gamma = (a_1, a_2, \ldots, a_{2k+1}) \neq (1, 0, \ldots, 0)$ and let $x = (x_1, x_2, \ldots, x_{2k+1})$. Then $g(x) \oplus g(x \oplus \gamma) = a_1 \oplus f(x_2, \ldots, x_{2k+1}) \oplus f(x_2 \oplus a_2, \ldots, x_{2k+1} \oplus a_{2k+1})$. Since f is a bent function, $f(x_2, \ldots, x_{2k+1}) \oplus f(x_2 \oplus a_2, \ldots, x_{2k+1} \oplus a_{2k+1})$ is balanced for all $(a_2, \ldots, a_{2k+1}) \neq (0, \ldots, 0)$ (see (iii) of Lemma 3). Thus $g(x) \oplus g(x \oplus \gamma)$ is balanced for all $\gamma = (a_1, a_2, \ldots, a_{2k+1}) \neq (1, 0, \ldots, 0)$. □

From Corollary 9, the nonlinearity of the function g defined by (4) satisfies $N_g \geq 2^{2k} - 2^k$. Furthermore, by Lemma 14, g is balanced. Thus we have

Corollary 18. *The function g defined by (4) is balanced and satisfies the propagation criterion with respect to all non-zero vectors $\gamma \in V_{2k+1}$ with $\gamma \neq (1, 0, \ldots, 0)$. The nonlinearity of g satisfies $N_g \geq 2^{2k} - 2^k$.*

On V_{2k} Let f be a bent function on V_{2k-2} and let g be a function on V_{2k} obtained from f in the following way:

$$\begin{aligned} & g(x_1, x_2, x_3, \ldots, x_{2k}) \\ & = (1 \oplus x_1)(1 \oplus x_2) f(x_3, \ldots, x_{2k}) \oplus (1 \oplus x_1) x_2 (1 \oplus f(x_3, \ldots, x_{2k})) \\ & \quad x_1 (1 \oplus x_2)(1 \oplus f(x_3, \ldots, x_{2k})) \oplus x_1 x_2 f(x_3, \ldots, x_{2k}) \\ & = x_1 \oplus x_2 \oplus f(x_3, \ldots, x_{2k}). \end{aligned} \tag{5}$$

Lemma 19. *The function g defined in (5) satisfies the propagation criterion with respect to* all but three *non-zero vectors in V_{2k}. The three vectors where the propagation criterion is not satisfied are $\gamma_1 = (1, 0, 0, \ldots, 0)$, $\gamma_2 = (0, 1, 0, \ldots, 0)$, and $\gamma_3 = \gamma_1 \oplus \gamma_2 = (1, 1, 0, \ldots, 0)$.*

Proof. Let $\gamma = (a_1, a_2, \ldots, a_{2k})$ be a non-zero vector in V_{2k} differing from γ_1, γ_2 and γ_3. Also let $x = (x_1, \ldots, x_{2k})$. Then we have $g(x) \oplus g(x \oplus \gamma) = a_1 \oplus a_2 \oplus f(x_3, \ldots, x_{2k}) \oplus f(x_3 \oplus a_3, \ldots, x_{2k} \oplus a_{2k})$. Since f is a bent function on V_{2k-2} and $(a_3, \ldots, a_{2k}) \neq (0, \ldots, 0)$, $f(x_3, \ldots, x_{2k}) \oplus f(x_3 \oplus a_3, \ldots, x_{2k} \oplus a_{2k})$ is balanced, from which it follows that $g(x) \oplus g(x \oplus \gamma)$ is balanced for any non-zero vector γ in V_{2k} differing from γ_1, γ_2 and γ_3. This proves the lemma. □

Since $x_1 \oplus x_2$ is balanced on V_2, g is balanced on V_{2k}. On the other hand, by Lemma 8, we have $N_g \geq 2^{2k-1} - 2^k$. Thus we have the following result:

Corollary 20. *The function g defined by (5) is balanced and satisfies the propagation criterion with respect to all non-zero vectors $\gamma \in V_{2k}$ with $\gamma \neq (c_1, c_2, 0, \ldots, 0)$, where $c_1, c_2 \in GF(2)$. The nonlinearity of g satisfies $N_g \geq 2^{2k-1} - 2^k$.*

4.2 Moving Vectors Around

Though functions constructed according to (4) or (5) satisfy the propagation criterion with respect to all but one or three non-zero vectors, they are not interesting in practical applications. We show that through linear transformation of input coordinates, the vectors where the propagation criterion is not satisfied can be transformed while the balancedness and nonlinearity of the functions are preserved. In particular, the vectors can be transformed into vectors having a high Hamming weight. In this way we obtain highly nonlinear balanced functions satisfying the high degree propagation criterion.

Let f be a function on V_n, A a nondegenerate matrix of order n with entries from $GF(2)$, and b a vector in V_n. Then $f^*(x) = f(xA \oplus b)$ defines a new function on V_n, where $x = (x_1, x_2, \ldots, x_n)$. It can be proved that the algebraic degree and the nonlinearity of f^* is the same as those of f. In addition, f^* is balanced iff f is balanced.

On V_{2k+1}

Theorem 21. *For any non-zero vector $\gamma^* \in V_{2k+1}$ ($k \geq 1$), there exist balanced functions on V_{2k+1} satisfying the propagation criterion with respect to all non-zero vectors $\gamma \in V_{2k+1}$ with $\gamma \neq \gamma^*$. The nonlinearities of the functions are at least $2^{2k} - 2^k$.*

Proof. Let f be a bent function and let g be the function constructed by (4). From linear algebra we know that for any bases B_1 and B_2 of the vector space V_{2k+1}, where $B_1 = \{\alpha_j | j = 1, \ldots, 2k+1\}$ and $B_2 = \{\beta_j | j = 1, \ldots, 2k+1\}$, there exists a unique nondegenerate matrix A of order $2k+1$ with entries from $GF(2)$ such that $\alpha_j A = \beta_j$, $j = 1, \ldots, 2k+1$. In particular, this is true when $\alpha_1 = \gamma^*$ and $\beta_1 = (1, 0, \ldots, 0)$. Let $x = (x_1, x_2, \ldots, x_n)$ and let g^* be the function obtained from g by employing linear transformation on the input coordinates of g:

$$g^*(x) = g(xA).$$

Since A is nondegenerate, g^* is balanced and has the same nonlinearity as that of g. Now we show that g^* satisfies the propagation criterion with respect to all non-zero vectors except γ^*.

Let γ be a non-zero vector in V_{2k+1} with $\gamma \neq \gamma^*$. Consider the following function $g^*(x) \oplus g^*(x \oplus \gamma) = g(xA) \oplus g(xA \oplus \gamma A) = g(y) \oplus g(y \oplus \gamma A)$ where $y = xA$. Note that A is nondegenerate and thus y runs through V_{2k+1} while x runs through V_{2k+1}. Since $\gamma \neq \gamma^*$ we have $\gamma A \neq (1, 0, \ldots, 0)$. From (iii) of Lemma 3, $g(y) \oplus g(y \oplus \gamma A)$ is balanced and hence $g^*(x) \oplus g^*(x \oplus \gamma)$ is balanced. Consequently, g^* satisfies the propagation criterion with respect to all non-zero vectors in V_{2k+1} but γ^*. This completes the proof. □

As a consequence of Theorem 21, we obtain, by letting $\gamma^* = (1, 1, \ldots, 1)$, highly nonlinear balanced functions on V_{2k+1} satisfying the propagation criterion of degree $2k$. This is described in the following:

Corollary 22. *Let f be a bent function on V_{2k} and let $g^*(x_1, \ldots, x_{2k+1}) = x_1 \oplus f(x_1 \oplus x_2, x_1 \oplus x_3, \ldots, x_1 \oplus x_{2k+1})$. Then g^* is a balanced function on V_{2k+1} and satisfies the propagation criterion of degree $2k$. The nonlinearity of g^* satisfies $N_{g^*} \geq 2^{2k} - 2^k$.*

On V_{2k}

Theorem 23. *For any non-zero vectors $\gamma_1^*, \gamma_2^* \in V_{2k}$ ($k \geq 2$) with $\gamma_1^* \neq \gamma_2^*$, there exist balanced functions on V_{2k} satisfying the propagation criterion with respect to* all but three *non-zero vectors in V_{2k}. The three vectors where the propagation criterion is not satisfied are γ_1^*, γ_2^* and $\gamma_1^* \oplus \gamma_2^*$. The nonlinearities of the functions are at least $2^{2k-1} - 2^k$.*

Proof. The proof is essentially the same as that for Theorem 21. The major difference lies in the selection of bases $B_1 = \{\alpha_j | j = 1, \ldots, 2k\}$ and $B_2 = \{\beta_j | j =$

$1,\ldots,2k\}$. By linear algebra, we can let $\alpha_1 = \gamma_1^*$, $\alpha_2 = \gamma_2^*$, $\beta_1 = (1,0,0,\ldots,0)$, and $\beta_2 = (0,1,0,\ldots,0)$. By the same reasoning as in the proof of Theorem 21, we can see that g^* defined by $g^*(x) = g(xA)$ satisfies the propagation criterion with respect to all but the following three non-zero vectors in V_{2k}: γ_1^*, γ_2^* and $\gamma_1^* \oplus \gamma_2^*$. Here $x = (x_1, x_2, \ldots, x_{2k})$, $g(x) = x_1 \oplus x_2 \oplus f(x_3, \ldots, x_{2k})$, and f, a bent function on V_{2k-2}, are all the same as in (5), and A is the unique nondegenerate matrix such that $\alpha_j A = \beta_j$, $j = 1,\ldots,2k$. □

Similarly to the case on V_{2k+1}, we can obtain highly nonlinear balanced functions satisfying the high degree propagation criterion, by properly selecting vectors γ_1^* and γ_2^*. Unlike the case on V_{2k+1}, however, the degree of propagation criterion the functions can achieve is $\frac{4}{3}k$, but not $2k-1$. The construction method is described in the following corollary.

Corollary 24. *Suppose that $2k = 3t + c$ where $c = 0, 1$ or 2. Then there exist balanced functions on V_{2k} that satisfy the propagation criterion of degree $2t - 1$ (when $c = 0$ or 1), or $2t$ (when $c = 2$). The nonlinearities of the functions are at least $2^{2k-1} - 2^k$.*

Proof. Set $c_1 = 0$, $c_2 = 1$ if $c = 1$ and set $c_1 = c_2 = \frac{1}{2}c$ otherwise. Let $\gamma_1^* = (a_1,\ldots,a_{3t+c})$ and $\gamma_2^* = (b_1,\ldots,b_{3t+c})$, where

$$a_j = \begin{cases} 1 & \text{for } j = 1,\ldots,2t+c_1, \\ 0 & \text{for } j = 2t+c_1+1,\ldots,3t+c. \end{cases}$$

$$b_j = \begin{cases} 0 & \text{for } j = 1,\ldots,t+c_1, \\ 1 & \text{for } j = t+c_1+1,\ldots,3t+c. \end{cases}$$

By Theorem 23 there exists a balanced function g^* on V_{2k} satisfying the propagation criterion with respect to all but three non-zero vectors in V_{2k}. The three vectors are γ_1^*, γ_2^* and $\gamma_1^* \oplus \gamma_2^*$. The nonlinearity of g^* satisfies $N_{g^*} \geq 2^{2k-1} - 2^k$.

Note that $W(\gamma_1^*) = 2t + c_1$, $W(\gamma_2^*) = 2t + c_2$, and $W(\gamma_1^* \oplus \gamma_2^*) = 2t + 2c_1 = 2t + c$. The minimum among the three weights is $2t + c_1$. Therefore, for any nonzero vector $\gamma \in V_{2k}$ with $W(\gamma) \leq 2t + c_1 - 1$, we have $\gamma \neq \gamma_1^*, \gamma_2^*$ or $\gamma_1^* \oplus \gamma_2^*$. By Theorem 23, $g^*(x) \oplus g^*(x \oplus \gamma)$ is balanced. From this we conclude that g^* satisfies the propagation criterion of order $2t + c_1 - 1$. The proof is completed by noting that $c_1 = 0$ if $c = 0$ or 1 and $c_1 = 1$ if $c = 2$. □

In the full paper [13] we shall show that functions obtained by (4) and (5) can achieve a wide range of algebraic degrees, namely $2, \ldots, k$ and $2, \ldots, k-1$ respectively. We shall also provide two concrete examples to illustrate our construction methods.

References

1. ADAMS, C. M., AND TAVARES, S. E. Generating and counting binary bent sequences. *IEEE Transactions on Information Theory IT-36 No. 5* (1990), 1170–1173.
2. ADAMS, C. M., AND TAVARES, S. E. 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.
3. COHEN, G. D., KARPOVSKY, M. G., H. F. MATTSON, J., AND SCHATZ, J. R. Covering radius — survey and recent results. *IEEE Transactions on Information Theory IT-31*, 3 (1985), 328–343.
4. DETOMBE, J., AND TAVARES, S. Constructing large cryptographically strong S-boxes. In *Advances in Cryptology - AUSCRYPT'92* (1993), Springer-Verlag, Berlin, Heidelberg, New York. to appear.
5. DILLON, J. F. A survey of bent functions. *The NSA Technical Journal* (1972), 191–215. (unclassified).
6. MEIER., W., AND STAFFELBACH, O. Nonlinearity criteria for cryptographic functions. In *Advances in Cryptology - EUROCRYPT'89* (1990), vol. 434, Lecture Notes in Computer Science, Springer-Verlag, Berlin, Heidelberg, New York, pp. 549–562.
7. NYBERG, K. Perfect nonlinear S-boxes. In *Advances in Cryptology - EUROCRYPT'91* (1991), vol. 547, Lecture Notes in Computer Science, Springer-Verlag, Berlin, Heidelberg, New York, pp. 378–386.
8. PATTERSON, N. J., AND WIEDEMANN, D. H. The covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16276. *IEEE Transactions on Information Theory IT-29*, 3 (1983), 354–356.
9. PRENEEL, B., LEEKWICK, W. V., LINDEN, L. V., GOVAERTS, R., AND VANDEWALLE, J. Propagation characteristics of boolean functions. In *Advances in Cryptology - EUROCRYPT'90* (1991), vol. 437, Lecture Notes in Computer Science, Springer-Verlag, Berlin, Heidelberg, New York, pp. 155–165.
10. ROTHAUS, O. S. On "bent" functions. *Journal of Combinatorial Theory Ser. A, 20* (1976), 300–305.
11. SEBERRY, J., AND YAMADA, M. Hadamard matrices, sequences, and block designs. In *Contemporary Design Theory: A Collection of Surveys*, J. H. Dinitz and D. R. Stinson, Eds. John Wiley & Sons, Inc, 1992, ch. 11, pp. 431–559.
12. SEBERRY, J., AND ZHANG, X. M. Highly nonlinear 0-1 balanced functions satisfying strict avalanche criterion. In *Advances in Cryptology - AUSCRYPT'92* (1993), Springer-Verlag, Berlin, Heidelberg, New York. to appear.
13. SEBERRY, J., ZHANG, X. M., AND ZHENG, Y. Nonlinearity and propagation characteristics of balanced boolean functions. Submitted for Publication, 1993.