# Nonlinearity and Propagation Characteristics of Balanced Boolean Functions [*]

Jennifer Seberry
Xian-Mo Zhang
Yuliang Zheng

Department of Computer Science
The University of Wollongong
Wollongong, NSW 2522, AUSTRALIA
E-mail: 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. The main contribution of this paper is to reveal a number of interesting properties of balancedness and nonlinearity, and to study systematic methods for constructing Boolean functions satisfying some or all of the three criteria. We show that concatenating, splitting, modifying and multiplying (in the sense of Kronecker) 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 balanced Boolean functions that are highly nonlinear and satisfy the strict avalanche criterion (SAC). Furthermore we 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.

[*] Submitted to *Information and Computation.*
Part of the results were presented in "J. Seberry and X-M. Zhang, *Highly nonlinear 0-1 balanced functions satisfying strict avalanche criterion*, AUSCRYPT'92", and "J. Seberry, X-M. Zhang and Y. Zheng, *Highly nonlinear balanced Boolean functions satisfying high degree propagation criterion*, Preprint 1/93, Department of Computer Science, University of Wollongong".

The first author was supported in part by the Australian Research Council under the reference numbers A49130102, A9030136, A49131885 and A49232172, the second author by A49130102, and the third author by A49232172.

## Key Words

Bent Functions, Boolean Function, Cryptography, Data Security, Hadamard Matrix, Nonlinearity, S-box, Sequences, Strict Avalanche Criterion.

# 1 Introduction

A Boolean function of $n$ input coordinates is said to satisfy *the propagation criterion with respect to a non-zero vector* if complementing input coordinates according to the vector results in the output of the function being complemented 50% of the time over all possible input vectors, and to satisfy *the propagation criterion of degree $k$* if complementing $k$ or less input coordinates results in the output of the function being complemented 50% of the time over all possible input vectors. Another important criterion, the strict avalanche criterion (SAC), coincides with the propagation criterion of degree 1. It is well known that bent functions possess the highest nonlinearity and satisfy the propagation criterion with respect to *all* non-zero vectors [Dil72]. However two drawbacks of bent functions prohibit their direct applications in practice. The first drawback is that they are not balanced, and the second drawback is that they exist only when the number of input coordinates is even. Cryptographic applications, such as the design of strong substitution boxes (S-boxes), often require that when input coordinates of a Boolean function are selected independently, at random, the output of the function must behave as a uniformly distributed random variable [KD79, AT90a]. In other words, the function has to be balanced. Some practical applications need Boolean functions with an odd number of input coordinates. On the other hand, the nonlinearity of Boolean functions measures the ability of a cryptographic system using the functions to resist against being expressed as a set of linear equations.

This paper is concerned properties and constructions of nonlinearly balanced functions. We present a number of methods for constructing highly nonlinear balanced functions. These include concatenating, splitting, modifying and multiplying (in the sense of Kronecker) sequences. It is interesting to note that balanced functions obtained by modifying and multiplying sequences achieve a nonlinearity higher than that attainable by any previously known construction method. We also initiate the research into the systematic construction of highly nonlinear balanced functions satisfying the SAC or the propagation criterion. We present simple methods for constructing balanced functions satisfying the SAC. When $n = 2k + 1$, where $n$ is the number of input coordinates, the nonlinearity of functions constructed is at least $2^{2k} - 2^k$, and when $n = 2k$, it is at least $2^{2k-1} - 2^k$.

Furthermore we present methods for constructing balanced functions satisfying the high degree propagation criterion. More precisely, when $n = 2k + 1$, we construct balanced functions that satisfy the propagation criterion with respect to *all but one* non-zero vectors, and when $n = 2k$, functions we construct are balanced and also satisfy the propagation criterion with respect to *all but three* non-zero vectors. We also show that the vectors where the propagation criterion is not satisfied can be transformed into other vectors. As a consequence, we obtain balanced functions satisfying the propagation criterion of degree $2k$ when $n = 2k+1$, and balanced functions satisfying the propagation criterion of degree $\frac{4k}{3}$ when $n = 2k$. The nonlinearity of functions constructed is at least $2^{2k} - 2^k$ when $n = 2k + 1$, and $2^{2k-1} - 2^k$ when $n = 2k$.

The organization of the rest part of the paper is as follows: in Section 2 we introduce notations and definitions used in this paper. In Section 3 we prove results on the nonlinearity and balancedness of functions including those obtained by concatenating or splitting bent sequences. In Section 4, we show methods for constructing highly nonlinear balanced functions by modifying and multiplying sequences. Our construction methods for highly nonlinear balanced functions satisfying the SAC are presented in Section 5, while methods for highly nonlinear balanced functions satisfying the high degree propagation criterion are presented in Section 6. Each method is illustrated by constructing a concrete function with the cryptographic properties. The paper is closed by a discussion of future work in Section 7.

# 2 Preliminaries

We consider functions from $V_n$ to $GF(2)$ (or simply functions on $V_n$), where $V_n$ is the vector space of $n$ tuples of elements from $GF(2)$. These functions are also called Boolean functions. Note that functions on $V_n$ can be represented by polynomials of $n$ coordinates. We are particularly interested in the *algebraic normal form* representation in which a function is viewed as the sum of products of coordinates. The *algebraic degree* of a function is the number of coordinates in the longest product when the function is represented in the algebraic normal form. To distinguish between a vector of coordinates and an individual coordinate, the former will be strictly denoted by $x$, $y$ or $z$, while the latter strictly by $x_i$, $y_i$, $z_i$, $u$ or $v$, where $i$ is an index.

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 $\alpha_i$, $0 \leqq i \leqq 2^n-1$, 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.

Obviously if $(a_0,\ldots,a_{2^n-1})$ and $(b_0,\ldots,b_{2^n-1})$ are the sequences of functions $f_1$ and $f_2$ on $V_n$ respectively, then $(a_0b_0,\ldots,a_{2^n-1}b_{2^n-1})$ is the sequence of $f(x)\oplus g(x)$, where $x=(x_1,x_2,\ldots,x_n)$. In particular, $-(a_0,\ldots,a_{2^n-1}) = (-a_0,\ldots,-a_{2^n-1})$ is the sequence of $1\oplus f_1(x)$.

An *affine* function $f$ on $V_n$ is a function that takes the form of $f(x) = a_1x_1\oplus\cdots\oplus a_nx_n\oplus c$, where $a_j, c\in GF(2)$, $j=1,2,\ldots,n$. Furthermore $f$ is called a *linear* function if $c=0$. The sequence of an affine (or linear) function is called an *affine (or linear) sequence*. The *Hamming weight* of a $(0,1)$-sequence (or vector) $\alpha$, denoted by $W(\alpha)$, is the number of ones in $\alpha$. The *Hamming distance* between two sequences $\alpha$ and $\beta$ 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 $\xi_f$ and $\xi_g$ 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 $\varphi_0$, $\varphi_1$, $\ldots$, $\varphi_{2^{n+1}-1}$ denote the affine functions on $V_n$.

The following notation will be used in this paper. Let $\alpha=(a_1,\cdots,a_n)$ and $\beta=(b_1,\cdots,b_n)$ be two sequences (or vectors), the *scalar product* of $\alpha$ and $\beta$, denoted by $\langle\alpha,\beta\rangle$, is defined as the sum of the component-wise multiplications. In particular, when $\alpha$ and $\beta$ are from $V_n$, $\langle\alpha,\beta\rangle = a_1b_1\oplus\cdots\oplus a_nb_n$, where the addition and the multiplication are over $GF(2)$, and when $\alpha$ and $\beta$ are $(1,-1)$-sequences, $\langle\alpha,\beta\rangle = a_1b_1+\cdots+a_nb_n$, where the addition and the multiplication are over the reals.

The *Kronecker product* of an $m\times n$ matrix $A$ and an $s\times t$ matrix $B$, denoted by $A\otimes B$, is an

$ms \times nt$ matrix defined by

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \cdots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{bmatrix}$$

where $a_{ij}$ is the element in the $i$th row and the $j$th column of $A$. In particular, the Kronecker product of a sequence $\alpha$ of length $m$ and a sequence $\beta$ of length $n$ is a sequence of length $mn$ defined by $\alpha \otimes \beta = (a_1 b, a_2 b, \cdots, a_m b)$, where $a_i$ is the $i$th element in $\alpha$.

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 [WSW72, SY92]. 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

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

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. For completeness, the proof of the lemma is also presented.

**Lemma 1** *Write* $H_n = \begin{bmatrix} \ell_0 \\ \ell_1 \\ \vdots \\ \ell_{2^n-1} \end{bmatrix}$ *where $\ell_i$ is a row of $H_n$. Then $\ell_i$ is the sequence of $h_i = \langle \alpha_i, x \rangle$, a linear function, where $\alpha_i$ 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 $H_n$.*

*Proof.* We prove the first half of the lemma by induction on $n$. Let $n = 1$. Then $H_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. The first row of $H_1$, $\ell_0 = (1, 1)$, is the sequence of $\langle \alpha_0, x \rangle$, while the second row of $H_1$, $\ell_1 = (1, -1)$, is the sequence of $h_1(x) = \langle \alpha_1, x \rangle$, where $x = (x_1, x_2)$, $\alpha_0 = (0, 0)$ and $\alpha_0 = (0, 1)$.

Now suppose the first half of the lemma is true for $n = 1, 2, \ldots, k-1$. Since $H_k = H_1 \otimes H_{k-1}$, each row of $H_k$ can be expressed as $\delta \otimes \ell$ where $\delta = (1, 1)$ or $(1, -1)$, and $\ell$ is a row of $H_{k-1}$. By the assumption $\ell$ is the sequence of a linear function $h_{k-1}(x) = \langle \alpha, x \rangle$ for some $\alpha \in V_{k-1}$, where $x = (x_1, \ldots, x_{k-1})$. Thus $\delta \otimes \ell$ is the sequence of a linear function on $V_k$ defined by $h_k(y) = \langle \beta, y \rangle$, where $y = (y_1, \ldots, y_k)$, $\beta = (0, \alpha)$ if $\delta = (1, 1)$ and $\beta = (1, \alpha)$ otherwise. Thus the first half is also true for $n = k$.

The second half follows from the above discussion as well as the fact that $H_n$ has $2^n$ rows and that there are exactly $2^n$ linear functions on $V_n$. □

¿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 $D_\delta$ is a function on $V_p$ defined by

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

Using this notation one can readily prove

**Lemma 2** *Let $f_0$, $f_1$, …, $f_{2^p-1}$ be functions on $V_q$. Let $\xi_i$ the sequence of $f_i$, $i = 0, 1, \ldots, 2^p - 1$, and let $\xi$ be the concatenation of $\xi_0$, $\xi_1$, …, $\xi_{2^p-1}$, namely, $\xi = (\xi_0, \xi_1, \ldots, \xi_{2^p-1})$. Then $\xi$ is the sequence of the following function on $V_{p+q}$*

$$f(y, x) = \bigoplus_{i=0}^{2^p-1} D_{\alpha_i}(y) f_i(x)$$

*where $y = (y_1, \ldots, y_p)$, $x = (x_1, \ldots, x_q)$ and $\alpha_i$ is the vector in $V_p$ whose integer representation is $i$.*

As a special case, if $\xi_1$, $\xi_2$ are the sequences of functions $f_1$, $f_2$ on $V_n$, then $\eta = (\xi_1, \xi_2)$ is the sequence of the following function $g$ on $V_{n+1}$

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

We now introduce the concept of bent functions.

**Definition 1** *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 [Rot76]. Other issues related to bent functions, such as properties, constructions and counting, can be found in [AT90a, KS83, LC82, OSW82, YH89]. Kumar, Scholtz and Welch [KSW85] defined and studied bent functions from $Z_q^n$ to $Z_q$, where $q$ is a positive integer. Applications of bent functions to digital communications, coding theory and cryptography can be found in such as [AT90b, DT93, LC82, Los87, MS78, MS90, Nyb91, OSW82].

The following result can be found in an excellent survey of bent functions by Dillon [Dil72].

**Lemma 3** *Let $f$ be a function on $V_n$, and let $\xi$ 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 $\ell$ 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 Sections 5 and 6.

In [Web85, WT86], Webster and Tavares first introduced the notion of *strict avalanche criterion (SAC)*:

**Definition 2** *A function $f$ on $V_n$ is said to satisfy the SAC if complementing any single input coordinate results in the output of $f$ being complemented half the times over all input vectors, namely, $f(x) \oplus f(x \oplus \alpha)$ is a balanced function for any vector $\alpha \in V_n$ whose Hamming weight is 1.*

The SAC has been generalized in two different directions: the propagation criterion [AT90a, PLL$^{+}$91] and the high order SAC [For89]. (Note that in [AT90a] the former is called the high order SAC1, while the latter the high order SAC2.) A combination of the two generalizations has also been studied in [PLL$^{+}$91, PGV91]. In this paper we are concerned with the propagation criterion whose formal definition follows.

**Definition 3** *Let $f$ be a function on $V_n$. We say that $f$ satisfies*

1. *the* propagation criterion with respect to a non-zero vector $\alpha$ 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* $1 \leqq W(\alpha) \leqq k$*.*

Note that the SAC is equivalent to the propagation criterion of degree 1. Also note that the *perfect nonlinearity* studied by Meier and Staffelbach [MS90] is equivalent to the propagation criterion of degree $n$.

Now it becomes clear that when $n$ is even, only bent functions fulfill the propagation criterion of the maximal degree $n$. Another property of bent functions is that they possess the highest possible nonlinearity. This will be discussed in more detail in the next section. However, since bent functions are not balanced and exist only for even $n$, they can not be directly employed in many practical applications. Constructing highly nonlinear balanced functions is the main topic to be treated in the following sections. Methods for constructing functions with additional properties, such as the SAC or the high degree propagation criterion, will also be presented.

# 3 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.

## 3.1 Upper Bounds of Nonlinearity

First we prove a lemma that is very useful in calculating the nonlinearity of a function.

**Lemma 4** *Let $f$ and $g$ be functions on $V_n$ whose sequences are $\xi_f$ and $\xi_g$ respectively. Then the distance between $f$ and $g$ can be calculated by $d(f,g) = 2^{n-1} - \frac{1}{2}\langle \xi_f, \xi_g \rangle$.*

*Proof.* $\langle \xi_f, \xi_g \rangle = \sum_{f(x)=g(x)} 1 - \sum_{f(x)\neq g(x)} 1 = 2^n - 2\sum_{f(x)\neq g(x)} 1 = 2^n - 2d(f,g)$. This proves the lemma. □

Recall that $H_n$ is a $2^n \times 2^n$ matrix. Denote by $\ell_i$ the $i$th row of $H_n$, where $i = 0, 1, \ldots, 2^n - 1$. For each $\ell_i$, define $\ell_{i+2^n} = -\ell_i$. Since $\ell_0$, $\ell_1$, …, $\ell_{2^n-1}$ are linear sequences of length $2^n$, $\{\ell_0$, …, $\ell_{2^n-1}$, $\ell_{2^n}$, …, $\ell_{2^{n+1}-1}\}$ comprise all the affine sequences of length $2^n$. For convenience, the affine function corresponding to the sequence $\ell_i$ is denoted by $\varphi_i$. Now let $f$ be a function on $V_n$ whose sequence is $\xi$. We are interested in determining the upper bound of the distance between $f$ and all the affine functions on $V_n$.

Using Parseval's equation (Page 416, [MS78]), we have

$$\sum_{i=0}^{2^n-1} \langle \xi, \ell_i \rangle^2 = 2^{2n}. \tag{1}$$

Consequently there exists an integer $0 \leqq i_0 \leqq 2^n - 1$ such that $\langle \xi, \ell_{i_0} \rangle^2 = \langle \xi, \ell_{i_0+2^n} \rangle^2 \geqq 2^n$. By noting the fact that $\langle \xi, \ell_{i_0} \rangle = -\langle \xi, \ell_{i_0+2^n} \rangle$, we have either $\langle \xi, \ell_{i_0} \rangle \geqq 2^{\frac{1}{2}n}$ or $\langle \xi, \ell_{i_0+2^n} \rangle \geqq 2^{\frac{1}{2}n}$. Without loss of generality assume that $\langle \xi, \ell_{i_0} \rangle \geqq 2^{\frac{1}{2}n}$. Then by Lemma 4, $d(f, \varphi_{i_0}) = 2^{n-1} - \frac{1}{2}\langle \xi, \ell_{i_0} \rangle \leqq 2^{n-1} - 2^{\frac{1}{2}n-1}$. This proves the following lemma which gives the upper bound of the nonlinearity of a function on $V_n$.

**Lemma 5** *For any function $f$ on $V_n$, the nonlinearity $N_f$ of $f$ satisfies $N_f \leqq 2^{n-1} - 2^{\frac{1}{2}n-1}$.*

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 $2^n$ (see [CKHFMS85]). Many results on the covering radius of $R(1,n)$ have direct implications on the nonlinearity of functions. In particular, Lemma 5 can be viewed as a translation of the upper bound on the covering radius of $R(1,n)$ [CKHFMS85].

Let $n$ be even, $f$ be a bent function on $V_n$ and $\xi$ be the sequence of $f$. By Lemma 3, we have $\langle \xi, \ell_i \rangle = \pm 2^{\frac{1}{2}n}$ for any affine sequence $\ell_i$, $i = 0, 1, \ldots, 2^{n+1} - 1$. By Lemma 4, $d(f, \varphi_i) = 2^{n-1} \pm 2^{\frac{1}{2}n-1}$ for any $\varphi_i$, $i = 0, 1, \ldots, 2^{n+1} - 1$. Finally by the definition of nonlinearity we have $N_f = 2^{n-1} - 2^{\frac{1}{2}n-1}$. Thus bent functions attain the upper bound for the nonlinearities of functions on $V_n$ shown in Lemma 5.

Conversely, if the nonlinearity of a function $f$ on $V_n$ attains the upper bound $2^{n-1} - 2^{\frac{1}{2}n-1}$, we can show that $\langle \xi, \ell_i \rangle = \pm 2^{\frac{1}{2}n}$ for all $i = 0, 1, \ldots, 2^{n+1} - 1$, which implies that $f$ is bent. Suppose that it is not the case. Then $\langle \xi, \ell_i \rangle \neq \pm 2^{\frac{1}{2}n}$ for some $i$, $0 \leqq i \leqq 2^{n+1} - 1$. Note that for any $0 \leqq i \leqq 2^n - 1$, $\langle \xi, \ell_i \rangle = -\langle \xi, \ell_{i+2^n} \rangle$, and hence $\langle \xi, \ell_i \rangle^2 = \langle \xi, \ell_{i+2^n} \rangle^2$. Thus from the Parseval's equation (1), there exist $i_1$ and $i_2$, $0 \leqq i_1, i_2, \leqq 2^n - 1$, such that $\langle \xi, \ell_{i_1} \rangle^2 > 2^n$ and $\langle \xi, \ell_{i_2} \rangle^2 < 2^n$. This implies that either $\langle \xi, \ell_{i_1} \rangle > 2^{\frac{1}{2}n}$ or $\langle \xi, \ell_{i_1+2^n} \rangle > 2^{\frac{1}{2}n}$, and hence either $d(f, \varphi_{i_1}) < 2^{n-1} - 2^{\frac{1}{2}n-1}$ or $d(f, \varphi_{i_1+2^n}) < 2^{n-1} - 2^{\frac{1}{2}n-1}$ (see also Lemma 4.) As a consequence we have $N_f < 2^{n-1} - 2^{\frac{1}{2}n-1}$. This contradicts the assumption that $f$ attains the maximum nonlinearity $2^{n-1} - 2^{\frac{1}{2}n-1}$. Consequently we have the following result (see also [MS78]):

**Corollary 1** *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 1, 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.

**Lemma 6** *Let $\xi$ and $\eta$ be $(0,1)$-sequences of length $2t$. If both $W(\xi)$ and $W(\eta)$ are even, then $d(\xi,\eta)$ is even.*

*Proof.* Write $\xi=(a_1,\ldots,a_{2t})$ and $\eta=(b_1,\ldots,b_{2t})$. Denote by $n_1$ the number of pairs $(a_i,b_i)=(0,0)$, by $n_2$ the number of pairs $(a_i,b_i)=(0,1)$, by $n_3$ the number of pairs $(a_i,b_i)=(1,0)$, and by $n_4$ the number of pairs $(a_i,b_i)=(1,1)$. Hence $n_1+n_2$, $n_3+n_4$, $n_1+n_3$ and $n_2+n_4$ are all even. Consequently, $2n_1+n_2+n_3=(n_1+n_2)+(n_1+n_3)$ is even. This proves that $d(\xi,\eta)=n_2+n_3$ is even. □

**Corollary 2** *Let $f$ be a balanced function on $V_n$ ($n\geqq 3$). Then the nonlinearity $N_f$ of $f$ is given by*

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

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

*Proof.* Note that the length of the sequence of a function is even. Also note that the truth table of $f$ contains an even number of ones and that all affine sequences contain an even number of ones. By Lemma 6, $N_f=\min_{i=0,1,\ldots,2^{n+1}-1} d(f,\varphi_i)$, where $\varphi_0$, $\varphi_1$, $\ldots$, $\varphi_{2^{n+1}-1}$ denote the affine functions on $V_n$, must be even. On the other hand, since $f$ is not bent, by corollary 1 we have $N_f<2^{n-1}-2^{\frac{1}{2}n-1}$. This proves the corollary. □

For $V_2$, there are six balanced sequences, namely

$$\pm(1,1,1,1), \pm(1,-1,1,-1), \pm(1,-1,-1,1)$$

all of which are linear. Therefore there are no nonlinearly balanced functions on $V_2$.

## 3.2 Concatenating Sequences

The following lemma gives the lower bound of the nonlinearity of a function obtained by concatenating the sequences of two functions.

**Lemma 7** *Let $f_1$ and $f_2$ be functions on $V_n$, and let $g$ be a function on $V_{n+1}$ defined by*

$$g(u,x_1,\ldots,x_n)=(1\oplus u)f_1(x_1,\ldots,x_n)\oplus uf_2(x_1,\ldots,x_n). \tag{2}$$

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

*Proof.* Note that $\xi = (\xi_1, \xi_2)$ is the sequence of $g$. Let $\psi$ be an arbitrary affine function on $V_{n+1}$ and let $L$ be the sequence of $\psi$. Then $L$ must take the form of $L = (\ell, \pm\ell)$ where $\ell$ is an affine sequence of length $2^n$. Note that $\langle \xi, L\rangle = \langle \xi_1, \ell\rangle \pm \langle \xi_2, \ell\rangle$ and thus $|\langle \xi, L\rangle| \leqq P_1 + P_2$. On the other hand, by Lemma 4 we have $d(g, \psi) = 2^n - \frac{1}{2}\langle \xi, L\rangle$. ¿From these discussions we have $d(g, \psi) \geqq 2^n - \frac{1}{2}(P_1 + P_2)$. Since $\psi$ is arbitrary we have $N_g \geqq 2^n - \frac{1}{2}(P_1 + P_2)$, and this completes the proof. □

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 7, shows that such functions can be obtained by concatenating bent sequences. This construction has also been discovered by Meier and Staffelbach in [MS90].

**Corollary 3** *In the construction (2), if both $f_1$ and $f_2$ are bent functions on $V_{2k}$, then $N_g \geqq 2^{2k} - 2^k$.*

*Proof.* In the proof of Lemma 7, let $P_1 = P_2 = 2^k$. □

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

**Lemma 8** *Let $f_0$, $f_1$, $f_2$ and $f_3$ be functions on $V_n$ whose sequences are $\xi_0$, $\xi_1$, $\xi_2$ and $\xi_3$ respectively. Assume that $\langle \xi_i, \ell\rangle \leqq P_i$ for each $0 \leqq i \leqq 3$ and for each affine sequence $\ell$ of length $2^n$, where each $P_i$ is a positive integer. Let $g$ be a function on $V_{n+2}$ defined by*

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

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

*Proof.* The proof is similar to that for Lemma 7, and hence is omitted. □

Lemma 8 can be further generalized. Let $f_0$, $f_1$, $\ldots$, $f_{2^t-1}$ be functions on $V_n$. Denote by $\xi_i$ the sequence of $f_i$. Assume that $\langle \xi_i, \ell\rangle \leqq P_i$ for each $0 \leqq i \leqq 2^t - 1$ and for each affine sequence $\ell$ of length $2^n$, where each $P_i$ is a positive integer. Let $g$ be a function on $V_{n+t}$ defined by

$$g(y, x) = \bigoplus_{i=0}^{2^t-1} D_{\alpha_i}(y) f_i(x) \tag{4}$$

where $y = (y_1, \ldots, y_t)$, $x = (x_1, \ldots, x_n)$ and $\alpha_i$ is a vector in $V_t$ whose integer representation is $i$. Then $N_g \geqq 2^{n+t-1} - \frac{1}{2}\sum_{i=0}^{2^t-1} P_i$. In particular, when $n$ is even and $f_i$, $i = 0, \ldots, 2^t - 1$, are all bent functions on $V_n$, $N_g \geqq 2^{n+t-1} - 2^{\frac{1}{2}n+t-1}$.

By selecting proper starting functions in (2), (3) and (4), the resulting functions can be balanced. For instance, in (2), if both $f_1$ and $f_2$ are balanced, or the number of times $f_1$ assumes the value one is equal to that $f_2$ assumes the value zero, the resulting function $g$ is balanced.

## 3.3 Splitting Sequences

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

*Proof.* We only give a proof for $-2^k \leqq \langle \eta_0, \ell \rangle \leqq 2^k$. The other half can be proved in the same way. Since $f(x_1, x_2, \ldots, x_{2k}) = (1 \oplus x_1) f(0, x_2, \ldots, x_{2k}) \oplus x_1 f(1, x_2, \ldots, x_{2k})$, $\eta = (\eta_0, \eta_1)$ is the sequence of $f(x_1, x_2, \ldots, x_{2k})$. Let $L = (\ell, \ell)$ and $L' = (\ell, -\ell)$. By Lemma 1, both $L$ and $L'$ are affine sequences of length $2^{2k}$.

Suppose that $-2^k \leqq \langle \eta_0, \ell \rangle \leqq 2^k$ is not true. Without loss of generality assume that $\langle \eta_0, \ell \rangle > 2^k$. There are two cases that have to be considered: $\langle \eta_1, \ell \rangle > 0$ and $\langle \eta_1, \ell \rangle < 0$. In the first case we have $\langle \eta, L \rangle \geqq \langle \eta_0, \ell \rangle + \langle \eta_1, \ell \rangle > 2^k$, and in the second case we have $\langle \eta, L' \rangle \geqq \langle \eta_0, \ell \rangle + \langle \eta_1, -\ell \rangle = \langle \eta_0, \ell \rangle + (-1) \langle \eta_1, \ell \rangle > 2^k$, both of which contradict the fact that $\langle \eta, L \rangle = \pm 2^k$ (see also (ii) of Lemma 3). This completes the proof. □

A consequence of Lemma 9 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 $\ell_i$ be the $i$th row of $H_k$ where $i = 0, 1, \ldots, 2^k - 1$. Note that $\ell_0$ is an all-one sequence while $\ell_1$, $\ell_2$, …, $\ell_{2^k-1}$ are all balanced sequences. The concatenation of the rows, $(\ell_0, \ell_1, \ldots, \ell_{2^k-1})$, is a bent sequence [AT90a]. Denote by $f(x_1, x_2, \ldots, x_{2k})$ the function corresponding to the bent sequence. Let $\xi$ 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 $\xi$ is the sequence of $f(1, x_2, \ldots, x_{2k})$. Since all $\ell_i$, $i = 2^{k-1}, 2^{k-1}+1, \ldots, 2^k - 1$, 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 $\xi$. 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 $\{1, -1\}$. $\xi''$ 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.

## 3.4 An Invariance Property

Next we examine properties of functions with respect to the affine transformation of coordinates. 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 is obvious that the algebraic degree of $f^*$ is the same as that of $f$.

On the other hand, since $A$ is nondegenerate, $xA \oplus b$ is an one-to-one mapping on $V_n$. Hence the truth table of $f^*$ contains exactly the same number of ones as that of $f$. This indicates that the balancedness of a function is preserved under the affine transformation of coordinates.

Now let $\varphi$ be an affine function on $V_n$ and let $\varphi^*(x) = \varphi(xA \oplus b)$. It is easy to verify that $d(f, \varphi) = d(f^*, \varphi^*)$. Since $A$ is nondegenerate, $\varphi^*$ will run through all affine functions on $V_n$ while

$\varphi$ runs through all affine functions on $V_n$. This proves that the nonlinearity of $f^*$ is the same as that of $f$.

Finally we consider the propagation characteristics under the affine transformation of coordinates. Let $\alpha$ be a nonzero vector in $V_n$. $f^*(x) \oplus f^*(x \oplus \alpha)$ is balanced if and only if

$$\begin{aligned} f(xA \oplus b) \oplus f((x \oplus \alpha)A \oplus b) &= f(xA \oplus b) \oplus f((xA \oplus b) \oplus \alpha A) \\ &= f(y) \oplus f(y \oplus \beta) \end{aligned}$$

is balanced, where $y = xA \oplus b$ and $\beta = \alpha A$. Since $A$ is nondegenerate and $\alpha$ is a nonzero vector, $\beta$ is a nonzero vector. In addition, $y = xA \oplus b$ will run through $V_n$ while $x$ runs through $V_n$. Therefore the number of vectors in $V_n$ where the propagation criterion is satisfied remains unchanged under the affine transformation. To summarize the discussions, we have

**Lemma 10** *The algebraic degree, the Hamming weight of the truth table, the nonlinearity, and the number of vectors with respect to which the propagation criterion is satisfied, of a function are invariant under the affine transformation of coordinates.*

# 4 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 [MS90], 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 8).

As 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 $2^n$ [CKHFMS85], using a result of [PW83], we can construct *unbalanced* functions on $V_{2k+1}$, $k \geqq 7$, 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 3. One might tempt to think that modifying the sequences in [PW83] 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 3).

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 [PW83], allows us to construct balanced functions on $V_{2k+15}$, $k \geqq 7$, that have a higher nonlinearity than that achieved by concatenating or splitting bent sequences.

## 4.1 On $V_{2k}$

Note that an even number $n \geqq 4$ can be expressed as $n = 4t$ or $n = 4t + 2$, where $t \geqq 1$. As the first step towards our goal, we prove

**Lemma 11** *For any integer $t \geqq 1$ there exists* *(i) a balanced function $f$ on $V_{4t}$ such that $N_f \geqq 2^{4t-1} - 2^{2t-1} - 2^t$,*

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

*Proof.* (i) Let $\ell_i$ be the $i$th row of $H_{2t}$ where $i = 0, 1, \dots, 2^{2t} - 1$. Then $\xi = (\ell_0, \ell_1, \dots, \ell_{2^{2t}-1})$ is a bent sequence of length $2^{4t}$.

Note that except for $\ell_0 = (1, 1, \dots, 1)$, all other $\ell_i$ $(i = 1, \dots, 2^{2t} - 1)$ are balanced sequences of length $2^{2t}$. Therefore replacing the all-one (or "flat") leading sequence $\ell_0$ with a balanced sequence renders $\xi$ balanced. The crucial idea here is to select a replacement with a high nonlinearity, since the nonlinearity of the resulting function depends largely on that of the replacement.

The replacement we select is $\ell_0^* = (e_1, e_1, e_2, \dots, e_{2^t-1})$, where $e_i$ is the $i$th row of $H_t$. Note that the leading sequence in $\ell_0^*$ is $e_1$ but not $e_0 = (1, 1, \dots, 1)$. $\ell_0^*$ is a balanced sequence of length $2^{2t}$, since all $e_i$, $i = 1, \dots, 2^t - 1$, are balanced sequences of length $2^t$. Replacing $\ell_0$ by $\ell_0^*$, we get a balanced sequence $\xi^* = (\ell_0^*, \ell_1, \dots, \ell_{2^{2t}-1})$.

Denote by $f^*$ the function corresponding to the sequence $\xi^*$, and consider the nonlinearity of $f^*$. Let $\varphi$ be an arbitrary affine function on $V_{4t}$, and let $L$ be the sequence of $\varphi$. By Lemma 1, $L$ is a row of $\pm H_{4t}$. Since $H_{4t} = H_{2t} \otimes H_{2t}$, $L$ can be expressed as $L = \pm \ell_i \otimes \ell_j$, where $\ell_i$ and $\ell_j$ are two row of $H_{2t}$. Assume that $\ell_i = (a_0, a_1, \dots, a_{2^{2t}-1})$. Then $L = \pm(a_0\ell_j, a_1\ell_j, \dots, a_{2^{2t}-1}\ell_j)$. A property of a Hadamard matrix is that its rows are mutually orthogonal. Hence $\langle \ell_p, \ell_q \rangle = 0$ for $p \neq q$. Thus

$$|\langle \xi^*, L \rangle| \leqq |\langle \ell_0^*, \ell_j \rangle| + |\langle \ell_j, \ell_j \rangle| \leqq |\langle \ell_0^*, \ell_j \rangle| + 2^{2t}.$$

We proceed to estimate $|\langle \ell_0^*, \ell_j \rangle|$. Note that $H_{2t} = H_t \otimes H_t$, $\ell_j$ can be expressed as $\ell_j = e_u \otimes e_v$, where $e_u$ and $e_v$ are rows of $H_t$. Write $e_u = (b_0, \dots, b_{2^t-1})$. Then $\ell_j = (b_0 e_v, \dots, b_{2^t-1} e_v)$. Similarly to the discussion for $|\langle \xi^*, L \rangle|$, we have

$$|\langle \ell_0^*, \ell_j \rangle| \leqq \begin{cases} 2|\langle e_2, e_2 \rangle| = 2^{t+1}, & \text{if } v = 2, \\ |\langle e_v, e_v \rangle| = 2^t, & \text{if } v = 3, \dots, 2^t, \\ 0, & \text{if } v = 1 \end{cases}$$

Thus $\langle \ell_0^*, \ell_j \rangle| \leqq 2^{t+1}$ and hence $|\langle \xi^*, L \rangle| \leqq 2^{t+1} + 2^{2t}$.

By Lemma 4, $d(f^*, \varphi) \geqq 2^{4t-1} - \frac{1}{2}\langle \xi^*, L \rangle \geqq 2^{4t-1} - 2^{2t-1} - 2^t$. Since $\varphi$ is arbitrary, $N_{f^*} \geqq 2^{4t-1} - 2^{2t-1} - 2^t$.

(ii) Now consider the case of $V_{4t+2}$. Let $\ell_i$, $i = 0, 1, \dots, 2^{2t+1} - 1$, be the $i$th row of $H_{2t+1}$. Then $\xi = (\ell_0, \ell_1, \dots, \ell_{2^{2t+1}-1})$ is a bent sequence of length $2^{4t+2}$.

The replacement for the all-one leading sequence $\ell_0 = (1, 1, \dots, 1) \in V_{2t+1}$ is the following balanced sequence $\ell_0^* = (e_{2^t}, e_{2^t+1}, \dots, e_{2^{t+1}-1})$, the concatenation of the $2^t$th, the $(2^t + 1)$th, ..., and the $(2^{t+1}-1)$th rows of $H_{t+1}$. Let $\xi^* = (\ell_0^*, \ell_1, \dots, \ell_{2^{2t+1}-1})$, and let $f^*$ the function corresponding to the balanced sequence.

Similarly to the case of $V_{4t}$, let $\varphi$ be a affine function on $V_{4t+2}$ and let $L$ be its sequence. $L$ can be expressed as $L = \pm \ell_i \otimes \ell_j$ where $\ell_i$ and $\ell_j$ are rows of $H_{2t+1}$. Hence

$$|\langle \xi^*, L \rangle| \leqq |\langle \ell_0^*, \ell_j \rangle| + |\langle \ell_j, \ell_j \rangle| \leqq |\langle \ell_0^*, \ell_j \rangle| + 2^{2t+1}$$

Since $\ell_0^*$ is obtained by splitting the bent sequence $(e_0, e_1, \dots, e_{2^{t+1}-1})$, where $e_i$ is a row of $H_{t+1}$, by Lemma 9, we have $|\langle \ell_0^*, \ell_j \rangle| \leqq 2^{t+1}$. ¿From this it follows that $|\langle \xi^*, L \rangle| \leqq 2^{t+1} + 2^{2t+1}$ and $N_{f^*} \geqq 2^{4t+1} - 2^{2t} - 2^t$. □

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 $n \geqq 4$ can be expressed as $n = 2^m$, $m \geqq 2$, or $n = 2^s(2t+1)$, $s \geqq 1$ and $t \geqq 1$.

Consider the case when $n = 2^m$, $m \geqq 2$. 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 $n = 2^s(2t+1)$, $s \geqq 1$ and $t \geqq 1$, is the same as that for the case of $n = 2^m$, $m \geqq 2$, 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 1** *For any even number $n \geqq 4$, there exists a balanced function $f^*$ on $V_n$ whose nonlinearity is*

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

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 3.3 can also be applied to $\zeta$. 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 $\zeta_0$ has exactly the same structure as the large sequence $\zeta$, and hence permuting and changing signs can also be applied to $\zeta_0$.

The nonlinearities of balanced functions on $V_4$, $V_6$, $V_8$, $V_{10}$, $V_{12}$ and $V_{14}$ constructed by the method shown in the proof of Theorem 1 are calculated in Table 1. For comparison, the nonlinearities of balanced functions constructed by concatenating four bent sequences (see Lemma 8) as well as the upper bounds for the nonlinearities of balanced functions (see Corollary 2) are also presented.

## 4.2 On $V_{2k+1}$

**Lemma 12** *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.*

| Vector Space | $V_4$ | $V_6$ | $V_8$ | $V_{10}$ | $V_{12}$ | $V_{14}$ |
|---|---|---|---|---|---|---|
| Upper Bound | 4 | 26 | 118 | 494 | 2014 | 8126 |
| By Modification | 4 | 26 | 116 | 492 | 2010 | 8120 |
| By Concatenation | 4 | 24 | 112 | 480 | 1984 | 8064 |

Table 1: Nonlinearities of Balanced Functions

*Proof.* Let $g(x_1,\dots,x_s,y_1,\dots,y_t) = f_1(x_1,\dots,x_s) \oplus f_2(y_1,\dots,y_t)$. Without loss of generality, suppose that $f_1$ is balanced. Then for any vector $(a_1,\dots,a_t) \in V_t$,

$$g(x_1,\dots,x_s,a_1,\dots,a_t) = f_1(x_1,\dots,x_s) \oplus f_2(a_1,\dots,a_t)$$

is a balanced function on $V_s$. ¿From this it immediately follows that $g$ is a balanced function on $V_{s+t}$. □

Let $\xi_1$ be the sequence of $f_1$ on $V_s$ and $\xi_2$ 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 $f_1(x_1,\dots,x_s) \oplus f_2(y_1,\dots,y_t)$.

**Lemma 13** *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*

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

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

*Proof.* Note that $\xi = \xi_1 \otimes \xi_2$ is the sequence of $g$. Let $\varphi$ be an arbitrary affine function on $V_{s+t}$ and let $\ell$ be the sequence of $\varphi$. Then $\ell$ can be expressed as $\ell = \pm\ell_1 \otimes \ell_2$ where $\ell_1$ is a row of $H_s$ and $\ell_2$ is a row of $H_t$. Since

$$\langle\xi,\ell\rangle = \langle\xi_1 \otimes \xi_2, \pm\ell_1 \otimes \ell_2\rangle = \pm\langle\xi_1,\ell_1\rangle\langle\xi_2,\ell_2\rangle$$

we have

$$|\langle\xi,\ell\rangle| = |\langle\xi_1,\ell_1\rangle| \cdot |\langle\xi_2,\ell_2\rangle| \leqq P_1 \cdot P_2$$

and by Lemma 4

$$d(g,\varphi) \geqq 2^{s+t-1} - \frac{1}{2}P_1 \cdot P_2$$

By the arbitrariness of $\varphi$, $N_g \geqq 2^{s+t-1} - \frac{1}{2}P_1 \cdot P_2$. □

Let $\xi_1$ be a balanced sequence of length $2^{2k}$ that is constructed using the method in the proof of Theorem 1, where $k \geqq 2$, Let $\xi_2$ be a sequence of length $2^{15}$ obtained by the method of [PW83]. Note that the nonlinearity of $\xi_2$ is 16276, and there are 13021 such sequences. Denote by $f_1$ the function corresponding to $\xi_1$ and by $f_2$ the function corresponding to $\xi_2$. Let

$$f(x_1,\dots,x_{2k},x_{2k+1},\dots,x_{2k+15}) = f_1(x_1,\dots,x_{2k}) \oplus f_2(x_{2k+1},\dots,x_{2k+15}) \quad (5)$$

Then

**Theorem 2** *The function $f$ defined by (5) is a balanced function on $V_{2k+15}$, $k \geqq 2$, whose nonlinearity is at least*

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

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

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

and

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

By Lemma 13, 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 $k \geqq 7$.

# 5 Constructing Highly Nonlinear balanced Functions Satisfying SAC

This section presents methods for constructing balanced functions with a high nonlinearity and satisfying the SAC. The algebraic degrees of the functions are discussed.

## 5.1 On $V_{2k+1}$

Let $k \geqq 1$, $f$ a bent function and $h$ a non-constant affine function, both on $V_{2k}$. Note that $f(x) \oplus h(x)$ is also bent. Without loss of generality we suppose that the number of times that $f(x)$ assumes the value zero differs from that of $f(x) \oplus h(x)$. (Otherwise we can replace $h(x)$ by $h(x) \oplus 1$ and hence $f(x) \oplus h(x)$ by $f(x) \oplus h(x) \oplus 1$.) Let $g$ be a function on $V_{2k+1}$ defined by

$$\begin{aligned} & g(u, x_1, \ldots, x_{2k}) \\ = \ & (1 \oplus u) f(x_1, \ldots, x_{2k}) \oplus u(f(x_1, \ldots, x_{2k}) \oplus h(x_1, \ldots, x_{2k})) \\ = \ & f(x_1, \ldots, x_{2k}) \oplus u h(x_1, \ldots, x_{2k}). \end{aligned} \tag{6}$$

**Lemma 14** *The function $g$ defined by (6) is a balanced function on $V_{2k+1}$.*

*Proof.* By Lemma 2 the sequence of $g$ is the concatenation of the sequences of $f(x)$ and $f(x) \oplus h(x)$. Recall that a bent function on $V_{2k}$ assumes the value one $2^{2k-1} \pm 2^{k-1}$ times. Therefore the number of times that $g$ assumes the value one is $(2^{2k-1} + 2^{k-1}) + (2^{2k-1} - 2^{k-1}) = 2^{2k}$. □

The following lemma is a direct consequence of Corollary 3.

**Lemma 15** *$N_g \geqq 2^{2k} - 2^k$ where $g$ is defined by (6).*

**Lemma 16** *The function $g$ defined by (6) satisfies the SAC.*

*Proof.* Let $\gamma = (b, a_1, \cdots, a_{2k})$ be an arbitrary vector in $V_{2k+1}$ with $W(\gamma) = 1$. Also let $\alpha = (a_1, \cdots, a_{2k})$, $z = (u, x_1, \ldots, x_{2k})$ and $x = (x_1, \ldots, x_{2k})$. We show that $g(z) \oplus g(z \oplus \gamma) = f(x) \oplus f(x \oplus \alpha) \oplus u(h(x) \oplus h(x \oplus \alpha)) \oplus bh(x \oplus \alpha)$ is balanced by considering the following two cases.

Case 1: $b = 0$ and hence $W(\alpha) = 1$. Then $g(z) \oplus g(z \oplus \gamma) = f(x) \oplus f(x \oplus \alpha) \oplus u(h(x) \oplus h(x \oplus \alpha))$. Since $h$ is an affine function, $h(x) \oplus h(x \oplus \alpha) = c$ where $c$ is a constant from $GF(2)$. Thus $g(z) \oplus g(z \oplus \gamma) = f(x) \oplus f(x \oplus \alpha) \oplus cu$. By (iii) of Lemma 3, $f(x) \oplus f(x \oplus \alpha)$ is a balanced function on $V_{2k}$ and hence by Lemma 12, $g(z) \oplus g(z \oplus \gamma)$ is a balanced function on $V_{2k+1}$.

Case 2: $b = 1$ and hence $W(\alpha) = 0$, i.e. $\alpha = (0, 0, \cdots, 0)$. Then $g(z) \oplus g(z \oplus \gamma) = h(x)$. Since $h(x)$ is a non-constant affine function on $V_{2k}$, $h(x)$ and hence $g(z) \oplus g(z \oplus \gamma)$ are balanced. □

Summarizing Lemmas 14, 15 and 16 we have

**Theorem 3** *For $k \geqq 1$, $g$ defined by (6) is a balanced function on $V_{2k+1}$ having $N_g \geqq 2^{2k} - 2^k$ and satisfying the SAC.*

## 5.2 On $V_{2k}$

Let $k \geqq 2$ and $f$ a bent function on $V_{2k-2}$. And let $h_1$, $h_2$ and $h_3$ be non-constant affine functions on $V_{2k-2}$ such that $h_i(x) \oplus h_j(x)$ is non-constant for any $i \neq j$. Such affine functions exist for all $k \geqq 2$. Let $x = (x_1, \cdots, x_{2k-2})$. Note that each $f(x) \oplus h_j(x)$ is also bent.

Without loss of generality we suppose both $f(x)$ and $f(x) \oplus h_1(x)$ assume the value one $2^{2k-3} + 2^{k-2}$ times while both $f(x) \oplus h_2(x)$ and $f(x) \oplus h_3(x)$ assume the value one $2^{2k-3} - 2^{k-2}$ times. This assumption is reasonable because $f(x) \oplus h_j(x)$ assumes the value one $2^{2k-3} + 2^{k-2}$ times if and only if $f(x) \oplus h_j(x) \oplus 1$ assumes the value one $2^{2k-3} - 2^{k-2}$ times. In addition $h_j(x) \oplus 1$ is also a non-constant affine function. This allows us to choose either $f(x) \oplus h_j(x)$ or $f(x) \oplus h_j(x) \oplus 1$ so that the assumption is satisfied. Let $g$ be a function on $V_{2k}$ defined by

$$\begin{aligned} & g(u, v, x_1, \ldots, x_{2k-2}) \\ &= (1 \oplus u)(1 \oplus v)f(x) \oplus (1 \oplus u)v(f(x) \oplus h_1(x)) \oplus \\ &\quad u(1 \oplus v)(f(x) \oplus h_2(x)) \oplus uv(f(x) \oplus h_3(x)) \\ &= f(x) \oplus vh_1(x) \oplus uh_2(x) \oplus uv(h_1(x) \oplus h_2(x) \oplus h_3(x)). \end{aligned} \tag{7}$$

**Lemma 17** *$g$ defined by (7) is a balanced function on $V_{2k}$.*

*Proof.* Note that the sequence of $g$ is the concatenation of the sequences of $f(x)$, $f(x) \oplus h_1(x)$, $f(x) \oplus h_2(x)$ and $f(x) \oplus h_3(x)$, and that $f(x)$ and $f(x) \oplus h_1(x)$ assume the value one $2^{2k-3} + 2^{k-2}$ times while $f(x) \oplus h_2(x)$ and $f(x) \oplus h_3(x)$ assume the value one $2^{2k-3} - 2^{k-2}$ times. Thus $g$ assumes the value one $2^{2k-1}$ times and hence is a balanced function on $V_{2k}$. □

**Lemma 18** *$N_g \geqq 2^{2k-1} - 2^k$ where $g$ is defined by (7).*

*Proof.* It follows from Corollary 3. □

**Lemma 19** *The function $g$ defined by (7) satisfies the SAC.*

*Proof.* Let $\gamma = (b, c, a_1, \cdots, a_{2k-2})$ be any vector in $V_{2k}$ with $W(\gamma) = 1$. Write $\alpha = (a_1, \cdots, a_{2k-2})$, $z = (u, v, x_1, \ldots, x_{2k-2})$ and $x = (x_1, \ldots, x_{2k-2})$. Note that $g(z \oplus \gamma) = f(x \oplus \alpha) \oplus (v \oplus c)h_1(x \oplus \alpha) \oplus (u \oplus b)h_2(x \oplus \alpha) \oplus (u \oplus b)(v \oplus c)(h_1(x \oplus \alpha) \oplus h_2(x \oplus \alpha) \oplus h_3(x \oplus \alpha))$. Consider the balancedness of $g(z) \oplus g(z \oplus \gamma)$ in the following three cases.

Case 1: $b = 1$, $c = 0$ and hence $W(\alpha) = 0$, i.e. $\alpha = (0, 0, \cdots, 0)$. In this case, $g(z) \oplus g(z \oplus \gamma) = h_2(x) \oplus v(h_1(x) \oplus h_2(x) \oplus h_3(x))$ will be $h_2(x)$ when $v = 0$ and $h_1(x) \oplus h_3(x)$ when $v = 1$. Both $h_2(x)$ and $h_1(x) \oplus h_3(x)$ are non-constant affine functions on $V_{2k-2}$ and hence $g(z) \oplus g(z \oplus \gamma)$ is a balanced function on $V_{2k}$.

Case 2: $b = 0$, $c = 1$ and hence $W(\alpha) = 0$, i.e. $\alpha = (0, 0, \cdots, 0)$. The proof of the balancedness of $g(z) \oplus g(z \oplus \gamma)$ is similar to Case 1.

Case 3: $b = 0$, $c = 0$ and hence $W(\alpha) = 1$. Since $h_j$ is an affine function, $h_j(x) \oplus h_j(x \oplus \alpha) = a_j$ where $a_j$ is a constant from $GF(2)$. Hence $g(z) \oplus g(z \oplus \gamma) = f(x) \oplus f(x \oplus \alpha) \oplus va_1 \oplus ua_2 \oplus uv(a_1 \oplus a_2 \oplus a_3)$. By (iii) of Lemma 3, $f(x) \oplus f(x \oplus \alpha)$ is a balanced function on $V_{2k-2}$ and hence by Lemma 12, $g(z) \oplus g(z \oplus \gamma)$ is a balanced function on $V_{2k}$. This proves that $g$ satisfies the SAC. □

Summarizing Lemmas 17, 18 and 19 we have

**Theorem 4** *For $k \geqq 2$, $g$ defined by (7) is a balanced function on $V_{2k}$ having $N_g \geqq 2^{2k-1} - 2^k$ and satisfying the SAC.*

## 5.3 Remarks

We have shown that a function on $V_n$ constructed according to (6) and (7) satisfy the propagation criterion with respect to all the $n$ vectors whose Hamming weight is 1. In fact there are many more vectors where the propagation criterion is satisfied.

Let $x = (x_1, \ldots, x_{2k})$, $z = (u, x)$, and let $g$ be a function constructed according to (6). Let $\gamma = (b, \alpha)$ where $b \in GF(2)$ and $\alpha \in V_{2k}$. Then $g(z) \oplus g(z \oplus \gamma) = f(x) \oplus f(x \oplus \alpha) \oplus bh(x \oplus \alpha) \oplus uh(\alpha)$. Consider the following three cases.

Case 1: $b = 0$ and $W(\alpha) \neq 0$. In this case, $g(z) \oplus g(z \oplus \gamma)$ is balanced for all $2^{2k} - 1$ non-zero vectors $\alpha \in V_{2k}$.

Case 2: $b = 1$ and $W(\alpha) = 0$. $g(z) \oplus g(z \oplus \gamma)$ is balanced for $\gamma = (1, 0, 0, \ldots, 0)$.

Case 3: $b = 1$ and $W(\alpha) \neq 0$. $g(z) \oplus g(z \oplus \gamma)$ is balanced if $h(\alpha) \neq 0$. The number of vectors $\alpha \in V_{2k}$ such that $h(\alpha) \neq 0$ is $2^{2k-1}$. $g(z) \oplus g(z \oplus \gamma)$ can not be balanced for any $\alpha \in V_{2k}$ such that $h(\alpha) = 0$. (Otherwise it would imply that $g$ is bent.)

Consequently, the total number of vectors such that $g$ constructed by (6) satisfies the propagation criterion is $2^{2k} + 2^{2k-1}$.

For a function $g$ on $V_{2k}$ constructed according to (7), a similar discussion reveals that the total number of vectors in $V_{2k}$ where the propagation criterion is satisfied is at least $2^{2k-2} + 1$.

The algebraic degree is also a nonlinearity criterion and it becomes important in certain practical applications where linear approximation of a nonlinear function needs to be avoided. In our constructions (6) and (7), the algebraic degree of a resulting function $g$ is the same as that of the starting bent function $f$.

The simplest bent function on $V_{2k}$ is the following quadratic function:

$$f(x_1, x_2, \ldots, x_{2k}) = x_1 x_{k+1} \oplus x_2 x_{k+2} \oplus \cdots \oplus x_k x_{2k}.$$

Bent functions with higher algebraic degrees exist and there are many methods for constructing such functions [Dil72]. The following is a method discovered by Dillon and Maiorana [Dil72, KSW85] for constructing a bent function $f$ on $V_{2k}$:

$$f(x) = \langle x', \pi(x'') \rangle \oplus r(x'')$$

where $x = (x', x'')$, $x' = (x_1, \ldots, x_k)$, $x'' = (x_{k+1}, \ldots, x_{2k})$, $r$ is an arbitrary function on $V_k$ and $\pi = (\pi_1(x''), \pi_2(x''), \ldots, \pi_k(x''))$ is a permutation on the vector space $V_k$. Due to the arbitrariness of $r$, the algebraic degree of $f$ can be any integer between 2 and $k$. ¿From these discussions it becomes clear that functions obtained by (6) and (7) can achieve a wide range of algebraic degrees, namely $2, \ldots, k$ and $2, \ldots, k-1$ respectively.

## 5.4 Examples

**Example 1** Consider $V_5$. As we know, $f(x_1, x_2, x_3, x_4) = x_1 x_2 \oplus x_3 x_4$ is a bent function in $V_4$. Choose the non-constant affine function $h(x_1, x_2, x_3, x_4) = 1 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4$. Note that $f(x_1, x_2, x_3, x_4)$ assumes the value one $2^{4-1} - 2^{2-1} = 6$ times and $f(x_1, x_2, x_3, x_4) \oplus h(x_1, x_2, x_3, x_4)$ assumes the value one $2^{4-1} + 2^{2-1} = 10$ times. Set $g(u, x_1, x_2, x_3, x_4) = f(x_1, x_2, x_3, x_4) \oplus u h(x_1, x_2, x_3, x_4) = x_1 x_2 \oplus x_3 x_4 \oplus u(1 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4)$. By Theorem 3, $g$ is a balanced function with $N_g \geqq 2^4 - 2^2 = 12$ and satisfying the SAC. On the other hand, by Corollary 2 the nonlinearity of balanced functions on $V_5$ is bounded from the above by $\lfloor\lfloor 2^4 - 2^{2-\frac{1}{2}} \rfloor\rfloor = \lfloor\lfloor 13.1818 \cdots \rfloor\rfloor = 12$. Therefore the nonlinearity of $g$ attains the upper bound for balanced functions on $V_5$.

**Example 2** Consider $V_6$. Choose $f(x_1, x_2, x_3, x_4) = x_1 x_2 \oplus x_3 x_4$, a bent function in $V_6$. Also choose affine functions $h_1(x_1, x_2, x_3, x_4) = x_1$, $h_2(x_1, x_2, x_3, x_4) = 1 \oplus x_2$, $h_3(x_1, x_2, x_3, x_4) = 1 \oplus x_3$. Note both $f(x_1, x_2, x_3, x_4)$ and $f(x_1, x_2, x_3, x_4) \oplus h_1(x_1, x_2, x_3, x_4)$ assume the value one $2^{4-1} - 2^{2-1} = 6$ times while both $f(x_1, x_2, x_3, x_4) \oplus h_3(x_1, x_2, x_3, x_4)$ and $f(x_1, x_2, x_3, x_4) \oplus h_4(x_1, x_2, x_3, x_4)$ assume the value one $2^{4-1} + 2^{2-1} = 10$ times. Set $g(u, v, x_1, x_2, x_3, x_4) = f(x_1, x_2, x_3, x_4) \oplus v h_1(x_1, x_2, x_3, x_4) \oplus u h_2(x_1, x_2, x_3, x_4) \oplus uv(h_1(x_1, x_2, x_3, x_4) \oplus h_2(x_1, x_2, x_3, x_4) \oplus h_3(x_1, x_2, x_3, x_4))$. By Theorem 4, $g$ is a balanced function with $N_g \geqq 2^5 - 2^3 = 24$ and satisfying the SAC. The nonlinearity of $g$ is comparable to $2^5 - 2^2 - 2 = 26$, the upper bound for the nonlinearities of balanced functions on $V_6$ (see Corollary 2).

Recently Zheng, Pieprzyk and Seberry [ZPS93] constructed a very efficient one way hashing algorithm using boolean functions constructed by the method given in Theorem 3. These functions have further cryptographically useful properties.

# 6 Constructing Highly Nonlinear balanced Functions Satisfying High Degree Propagation Criterion

Another interesting topic is to study methods for constructing functions that are balanced and possess good propagation characteristics. In [PGV91], it was suggested that a function $f$ on $V_n$

which has a zero point in its Walsh spectrum be modified into a balanced function by adding a suitable linear function $h$ on $V_n$. As $h$ has to be found by exhaustive search over all the linear functions on $V_n$, the method is infeasible when $n$ is large. In addition, the method is not applicable to the functions which do not have zero points in their Walsh spectra. These functions include (1) bent functions, and (2) highly nonlinear functions obtained by complementing a single position in bent sequences.

This section presents two methods for systematically constructing highly nonlinear balanced functions satisfying the propagation criterion. For odd $n$, we construct balanced functions that satisfy the propagation criterion with respect to all non-zero vectors except $\gamma=(1,0,\ldots,0)$. And for even $n$, we construct balanced functions that satisfy the propagation criterion with respect to *all but three* non-zero vectors. 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 $\gamma_3=\gamma_1\oplus\gamma_2=(1,1,0,\ldots,0)$. The two methods both start with bent functions, and hence are similar from a technical point of view. We also show how $\gamma$, $\gamma_1$ and $\gamma_2$, can be transformed into any other non-zero vectors.

## 6.1 Basic Construction

### 6.1.1 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

$$\begin{aligned} & g(x_1,x_2,\ldots,x_{2k+1}) \\ &= (1\oplus x_1)f(x_2,\ldots,x_{2k+1})\oplus x_1(1\oplus f(x_2,\ldots,x_{2k+1})) \\ &= x_1\oplus f(x_2,\ldots,x_{2k+1}). \end{aligned} \quad (8)$$

**Lemma 20** *The function $g$ defined in (8) 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 3, the nonlinearity of the function $g$ defined by (8) satisfies $N_g\geqq 2^{2k}-2^k$. Furthermore, by Lemma 12, $g$ is balanced. Thus we have

**Corollary 4** *The function $g$ defined by (8) 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 $N_g\geqq 2^{2k}-2^k$.*

### 6.1.2 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:

$$g(x_1,x_2,x_3,\ldots,x_{2k})$$

$$\begin{aligned} &= (1\oplus x_1)(1\oplus x_2)f(x_3,\ldots,x_{2k})\oplus(1\oplus x_1)x_2(1\oplus f(x_3,\ldots,x_{2k})) \\ &\quad x_1(1\oplus x_2)(1\oplus f(x_3,\ldots,x_{2k}))\oplus x_1x_2f(x_3,\ldots,x_{2k}) \\ &= x_1\oplus x_2\oplus f(x_3,\ldots,x_{2k}). \end{aligned} \tag{9}$$

**Lemma 21** *The function $g$ defined in (9) 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 $\gamma_1$, $\gamma_2$ and $\gamma_3$. 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 $\gamma$ in $V_{2k}$ differing from $\gamma_1$, $\gamma_2$ and $\gamma_3$. 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 7, we have $N_g\geqq 2^{2k-1}-2^k$. Thus we have the following result:

**Corollary 5** *The function $g$ defined by (9) 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 $N_g\geqq 2^{2k-1}-2^k$.*

## 6.2 Moving Vectors Around

Though functions constructed according to (8) or (9) satisfy the propagation criterion with respect to all but one or three non-zero vectors, they only fulfill the propagation criterion of degree zero. Therefore these functions are not interesting in practical applications. Recall that the balancedness, the nonlinearity and the number of vectors where the propagation criterion is satisfied are all invariant under an affine transformation of coordinates. This indicates that the degree for the propagation criterion might be improved through a suitable affine transformation of coordinates. Identifying such an affine transformation, however, is not an easy exercise, especially when the dimension of the underlying vector space is large and the number of vectors where the propagation criterion is satisfied is small.

In this section, we show that for functions constructed according to (8) or (9), the vectors where the propagation criterion is not satisfied 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.

### 6.2.1 On $V_{2k+1}$

**Theorem 5** *For any non-zero vector $\gamma^*\in V_{2k+1}$ ($k\geqq 1$), 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 (8). ¿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, by Lemma 10, $g^*$ 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 $\gamma^*$.

Let $\gamma$ 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 $\gamma A \neq (1, 0, \ldots, 0)$. By Lemma 20, $g(y) \oplus g(y \oplus \gamma A)$ runs through the values zero and one an equal number of times. 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 $\gamma^*$. This completes the proof. □

As a consequence of Theorem 5, 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 6** *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 $N_{g^*} \geqq 2^{2k} - 2^k$.*

*Proof.* Let $e_j$, $j = 1, 2, \ldots, 2k+1$, be a vector in $V_{2k+1}$ whose $j$th coordinate is 1 and all other coordinates are 0. In the proof of Theorem 5, we let $\alpha_1 = \gamma_0 = (1, \ldots, 1)$, $\alpha_j = e_j$, $j = 2, \ldots, 2k+1$ and $\beta_j = e_j$, $j = 1, \ldots, 2k+1$. Then there is a unique nondegenerate matrix $A$ of order $2k+1$ such that $\alpha_j A = \beta_j$, $j = 1, \ldots, 2k+1$. It is easy to verify that $A$ has the following form:

$$A = \begin{bmatrix} \gamma_0 \\ e_2 \\ \vdots \\ e_{2k+1} \end{bmatrix}.$$

Thus we have $g^*(x) = g(xA) = g(x_1, x_1 \oplus x_2, \ldots, x_1 \oplus x_{2k+1}) = x_1 \oplus f(x_1 \oplus x_2, x_1 \oplus x_3, \ldots, x_1 \oplus x_{2k+1})$, where $g(x) = x_1 \oplus f(x_2, \ldots, x_{2k+1})$, and $x = (x_1, x_2, \ldots, x_{2k+1})$. By Theorem 5 $g^*$ satisfies the propagation criterion with respect to all non-zero vectors in $V_{2k+1}$ except the all-one vector $\gamma^* = (1, 1, \ldots, 1)$. Consequently $g^*$ satisfies the propagation criterion of degree $2k$. □

### 6.2.2 On $V_{2k}$

**Theorem 6** *For any non-zero vectors $\gamma_1^*, \gamma_2^* \in V_{2k}$ ($k \geqq 2$) 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 $\gamma_1^*$, $\gamma_2^*$ 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 5. The major difference lies in the selection of bases $B_1 = \{\alpha_j | j = 1, \dots, 2k\}$ and $B_2 = \{\beta_j | j = 1, \dots, 2k\}$. By linear algebra, we can let $\alpha_1 = \gamma_1^*$, $\alpha_2 = \gamma_2^*$, $\beta_1 = (1, 0, 0, \dots, 0)$, and $\beta_2 = (0, 1, 0, \dots, 0)$. By the same reasoning as in the proof of Theorem 5, 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 $V_{2k}$: $\gamma_1^*$, $\gamma_2^*$ and $\gamma_1^* \oplus \gamma_2^*$. Here $x = (x_1, x_2, \dots, x_{2k})$, $g(x) = x_1 \oplus x_2 \oplus f(x_3, \dots, x_{2k})$, and $f$, a bent function on $V_{2k-2}$, are all the same as in (9), and $A$ is the unique nondegenerate matrix such that $\alpha_j A = \beta_j$, $j = 1, \dots, 2k$. □

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 $\gamma_1^*$ and $\gamma_2^*$. 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 7** *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 $\gamma_1^* = (a_1, \dots, a_{3t+c})$ and $\gamma_2^* = (b_1, \dots, b_{3t+c})$, where

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

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

By Theorem 6 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 $\gamma_1^*$, $\gamma_2^*$ and $\gamma_1^* \oplus \gamma_2^*$. The nonlinearity of $g^*$ satisfies $N_{g^*} \geqq 2^{2k-1} - 2^k$.

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 $W(\gamma) \leqq 2t + c_1 - 1$, we have $\gamma \neq \gamma_1^*, \gamma_2^*$ or $\gamma_1^* \oplus \gamma_2^*$. By Theorem 6, $g^*(x) \oplus g^*(x \oplus \gamma)$ 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 $c = 2$. □

## 6.3 Discussions and Examples

Comparing (6) with (8), one can see that the difference between the two constructions lies in the selection of the affine functions. In (6) a *non-constant* affine function $h$ is selected, while in (8) a constant 1 is employed. In a sense, the two constructions complement one another. This is also true in the case of (7) and (9).

Functions obtained by (8) and (9) can achieve a wide range of algebraic degrees, namely $2, \dots, k$ and $2, \dots, k - 1$ respectively. (See also the discussions in Section 5.3.) Recently, Detombe and Tavares obtained, while studying the design of S-boxes, balanced *quadratic* functions on $V_{2k+1}$ that satisfy the propagation criterion with respect to all but one vectors in $V_{2k+1}$. (They called these functions *near bent* functions.) They obtained the functions by the use of the *cubing* technique suggested by Pieprzyk [Pie91]. Propagation characteristics of quadratic functions were also studied extensively in [PGV91]. However, applicability of these quadratic functions in practice is limited by the following two facts:

1. Their algebraic degree is only 2.
2. They are all equivalent in structure in the sense that they can be transformed into one another by linear transformation of input coordinates.

In the following we provide two concrete examples to illustrate our methods for constructing highly nonlinear balanced functions that satisfy the high degree propagation criterion.

**Example 3** We consider balanced functions on $V_7$. Note that $f(x_1, x_2, x_3, x_4, x_5, x_6) = x_1x_2 \oplus x_3x_4 \oplus x_5x_6 \oplus x_2x_4x_6$ is a bent function on $V_6$. It is obtained by the use of Dillon and Maiorana's construction [Dil72, KSW85]. Now let

$$\begin{aligned} & g(x_1, x_2, x_3, x_4, x_5, x_6, x_7) \\ & \quad = x_1 \oplus f(x_2, x_3, x_4, x_5, x_6, x_7) \\ & \quad = x_1 \oplus x_2x_3 \oplus x_4x_5 \oplus x_6x_7 \oplus x_3x_5x_7. \end{aligned}$$

By Corollary 6, the following function

$$\begin{aligned} g^*(x_1, x_2, x_3, x_4, x_5, x_6, x_7) &= x_1 \oplus f(x_1 \oplus x_2, x_1 \oplus x_3, x_1 \oplus x_4, x_1 \oplus x_5, x_1 \oplus x_6, x_1 \oplus x_7) \\ &= x_1 \oplus (x_1 \oplus x_2)(x_1 \oplus x_3) \oplus (x_1 \oplus x_4)(x_1 \oplus x_5) \oplus \\ & \quad (x_1 \oplus x_6)(x_1 \oplus x_7) \oplus (x_1 \oplus x_3)(x_1 \oplus x_5)(x_1 \oplus x_7) \end{aligned}$$

satisfies the propagation criterion of degree 6. The propagation criterion is not satisfied only by the all-one vector $(1, 1, 1, 1, 1, 1, 1)$.

On the other hand, assume that $\gamma^* = (0, 0, 1, 0, 1, 1, 0)$. Let $e_j$ be a vector on $V_7$ whose $j$th coordinate is 1 and other coordinates are 0, where $j = 1, 2, \ldots, 7$. Let $\alpha_1 = \gamma_0 = (1, 1, 1, 1, 1, 1, 1)$, $\alpha_2 = e_2$, $\alpha_3 = e_1$ and $\alpha_j = e_j$, $j = 4, 5, 6, 7$. And let $\beta_j = e_j$, $j = 1, \ldots 7$. Thus $\{\alpha_1, \ldots, \alpha_7\}$ and $\{\beta_1, \ldots, \beta_7\}$ are two bases of $V_7$. By matrix manipulation we can find the following matrix

$$A = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

that satisfies $\alpha_j A = \beta_j$, $j = 1, \ldots, 7$. By Theorem 5

$$\begin{aligned} & h^*(x_1, x_2, x_3, x_4, x_5, x_6, x_7) \\ & \quad = g((x_1, x_2, x_3, x_4, x_5, x_6, x_7)A) \\ & \quad = g(x_3, x_2, x_1, x_4, x_3 \oplus x_5, x_3 \oplus x_6, x_7) \\ & \quad = x_3 \oplus x_2x_1 \oplus x_4(x_3 \oplus x_5) \oplus (x_3 \oplus x_6)x_7 \oplus x_1(x_3 \oplus x_5)x_7 \end{aligned}$$

is a balanced function on $V_7$ satisfying the propagation criterion with respect to all $\gamma \in V_7$ with $\gamma \neq (0,0,1,0,1,1,0)$.

Note that $N_{g^*} = N_{h^*} \geqq 2^6 - 2^3 = 56$, which in fact is the maximum nonlinearity of functions on $V_7$ [CKHFMS85].

**Example 4** Consider balanced functions on $V_{12}$. Note that $n$ can be written as $n = 2k = 3t + c$, where $k = 6$, $t = 4$ and $c = 0$. Again by using Dillon and Maiorana's construction we have the following bent function on $V_{10}$:

$$\begin{aligned} & f(x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}) \\ = \;& x_3x_4 \oplus x_5x_6 \oplus x_7x_8 \oplus x_9x_{10} \oplus x_{11}x_{12} \oplus x_4x_6x_8x_{10}x_{12}. \end{aligned}$$

By Corollary 5

$$\begin{aligned} & g(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}) \\ = \;& x_1 \oplus x_2 \oplus f(x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}) \\ = \;& x_1 \oplus x_2 \oplus x_3x_4 \oplus x_5x_6 \oplus x_7x_8 \oplus x_9x_{10} \oplus x_{11}x_{12} \oplus x_4x_6x_8x_{10}x_{12} \end{aligned}$$

is balanced and satisfies the propagation criterion with respect all non-zero vectors $\gamma \in V_{12}$ with $\gamma \neq (c_1, c_2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$, where $c_1, c_2 \in GF(2)$. The nonlinearity of $g$ satisfies $N_g \geqq 2^{11} - 2^6 = 1984$, which is comparable to $2^{11} - 2^5 - 2 = 2014$, the upper bound of the nonlinearity of a balanced function on $V_{12}$ (see Corollary 2).

Let $e_j$ be the vector in $V_{12}$, whose the $j$th coordinate is 1 and other coordinates are all 0, where $j = 1, \ldots, 12$.

Let $\gamma_1^* = (1,1,1,1,1,1,1,1,1,0,0,0,0)$, $\gamma_2^* = (0,0,0,0,1,1,1,1,1,1,1,1)$ and set

$$\begin{aligned} B_1 &= \{\gamma_1^*, \gamma_2^*, e_2, e_3, e_4, e_5, e_6, e_7, e_8, e_{10}, e_{11}, e_{12}\}, \\ B_2 &= \{e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8, e_9, e_{10}, e_{11}, e_{12}\}. \end{aligned}$$

Now let $A$ be a matrix defined by

$$A = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

It is not hard to check that $\gamma_1^*A = e_1$, $\gamma_2^*A = e_2$, $e_2A = e_3$, $e_3A = e_4$, $e_4A = e_5$, $e_5A = e_6$, $e_6A = e_7$, $e_7A = e_8$, $e_8A = e_9$, $e_{10}A = e_{10}$, $e_{11}A = e_{11}$, $e_{12}A = e_{12}$. Let

$$g^*(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12})$$

$$\begin{aligned} &= g((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12})A) \\ &= g(x_1,\ x_9,\ x_1 \oplus x_2,\ x_1 \oplus x_3,\ x_1 \oplus x_4,\ x_1 \oplus x_5 \oplus x_9,\ x_1 \oplus x_6 \oplus x_9, \\ &\quad x_1 \oplus x_7 \oplus x_9,\ x_1 \oplus x_8 \oplus x_9,\ x_9 \oplus x_{10},\ x_9 \oplus x_{11},\ x_9 \oplus x_{12}). \end{aligned}$$

By Theorem 6 the function $g^*$ is balanced and its nonlinearity satisfies $N_g \geqq 2^{11} - 2^6 = 1984$. In addition, $g^*$ satisfies the propagation criterion with respect all but three non-zero vectors in $V_{12}$. The three non-zero vectors are $\gamma_1^* = (1,1,1,1,1,1,1,1,0,0,0,0)$, $\gamma_2^* = (0,0,0,0,1,1,1,1,1,1,1,1)$ and $\gamma_3^* = \gamma_1^* \oplus \gamma_2^* = (1,1,1,1,0,0,0,0,1,1,1,1)$. By Corollary 7, $g^*$ satisfies the propagation criterion of degree $2t-1=7$.

# 7 Concluding Remarks

We have studied properties of balancedness and nonlinearity of Boolean functions including concatenating, splitting, modifying and multiplying sequences. Systematic methods have been presented for constructing highly nonlinear balanced functions satisfying the SAC or the high degree propagation criterion. A technique has been developed that allows us to transform vectors where the propagation criterion is not satisfied into other vectors, while preserving the nonlinearity and balancedness of the functions. This paper has also introduced a number of interesting problems which remain to be solved. We discuss one of them before closing the paper. For $V_{2k+1}$, functions constructed according to (8) are optimal in the sense that they fulfill the propagation criterion with respect to $2^{2k+1}-2$ non-zero vectors, and after the affine transformation of coordinates, they satisfy the propagation criterion of degree $2k$. For $V_{2k}$, the number of non-zero vectors given by (9) is $2^{2k}-4$ and the degree after the transformation is $\frac{4k}{3}$. It is left as future work to examine whether there are highly nonlinear balanced functions on $V_{2k}$ satisfying the propagation criterion of degree $2k-1$, and if there are, to find methods for constructing such functions.

# References

[AT90a] 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.

[AT90b] 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.

[CKHFMS85] G. D. Cohen, M. G. Karpovsky, Jr. H. F. Mattson, and J. R. Schatz. Covering radius — survey and recent results. *IEEE Transactions on Information Theory*, IT-31(3):328–343, 1985.

[Dil72] J. F. Dillon. A survey of bent functions. *The NSA Technical Journal*, pages 191–215, 1972. (unclassified).

[DT93] J. Detombe and S. Tavares. Constructing large cryptographically strong S-boxes. In *Advances in Cryptology - AUSCRYPT'92*, volume 718, Lecture Notes in Computer Science, pages 165–181. Springer-Verlag, Berlin, Heidelberg, New York, 1993.

[For89] R. Forré. The strict avalanche criterion: Special properties of boolean functions and extended definition. In *Advances in Cryptology - CRYPTO'88*, volume 403, Lecture Notes in Computer Science, pages 450–468. Springer-Verlag, Berlin, Heidelberg, New York, 1989.

[KD79] J. B. Kam and G. I. Davida. Structured design of substitution-permutation encryption networks. *IEEE Transactions on Computers*, 28:747–753, 1979.

[KS83] 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.

[KSW85] 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.

[LC82] A. Lempel and M. Cohn. Maximal families of bent sequences. *IEEE Transactions on Information Theory*, IT-28 No. 6:865–868, 1982.

[Los87] V. V. Losev. Decoding of sequences of bent functions by means of a fast Hadamard transform. *Radiotechnika i elektronika*, 7:1479–1492, 1987.

[MS78] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, New York, Oxford, 1978.

[MS90] W. Meier 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.

[Nyb91] 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.

[OSW82] 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.

[PGV91] B. Preneel, R. Govaerts, and J. Vandewalle. Boolean functions satisfying higher order propagation criteria. In *Advances in Cryptology - EUROCRYPT'91*, volume 547, Lecture Notes in Computer Science, pages 141–152. Springer-Verlag, Berlin, Heidelberg, New York, 1991.

[Pie91] J. Pieprzyk. Bent permutations. In *Proceeding of the International Conference on Finite Fields, Coding Theory, and Advances in Communications and Computing*, Las Vegas, 1991.

[PLL+91] B. Preneel, W. V. Leekwijck, L. V. Linden, R. Govaerts, and J. Vandewalle. Propagation characteristics of boolean functions. In *Advances in Cryptology - EUROCRYPT'90*, volume 437, Lecture Notes in Computer Science, pages 155–165. Springer-Verlag, Berlin, Heidelberg, New York, 1991.

[PW83] N. J. Patterson and D. H. Wiedemann. The covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16276. *IEEE Transactions on Information Theory*, IT-29(3):354–356, 1983.

[Rot76] O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory*, Ser. A, 20:300–305, 1976.

[SY92] J. Seberry and M. Yamada. Hadamard matrices, sequences, and block designs. In J. H. Dinitz and D. R. Stinson, editors, *Contemporary Design Theory: A Collection of Surveys*, chapter 11, pages 431–559. John Wiley & Sons, Inc, 1992.

[Web85] A. F. Webster. Plaintext/ciphertext bit dependencies in cryptographic system. Master's Thesis, Department of Electrical Engineering, Queen's University, Ontario, 1985.

[WSW72] 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.

[WT86] A. F. Webster and S. E. Tavares. On the design of S-boxes. In *Advances in Cryptology - CRYPTO'85*, volume 219, Lecture Notes in Computer Science, pages 523–534. Springer-Verlag, Berlin, Heidelberg, New York, 1986.

[YH89] R. Yarlagadda and J. E. Hershey. Analysis and synthesis of bent sequences. *IEE Proceedings (Part E)*, 136:112–123, 1989.

[ZPS93] Y. Zheng, J. Pieprzyk, and J. Seberry. HAVAL - one-way hashing algorithm with variable length of output. In *Advances in Cryptology - AUSCRYPT'92*, volume 718, Lecture Notes in Computer Science, pages 83–104. Springer-Verlag, Berlin, Heidelberg, New York, 1993.