Nonlinearity and Propagation Characteristics of Balanced Boolean Functions

JENNIFER SEBERRY, XIAN-MO ZHANG, AND YULIANG ZHENG*
Department of Computer Science, The University of Wollongong, Wollongong, New South Wales 2522, Australia
E-mail: {jennie,xianmo,yuliang}@cs.uow.edu.au

Three important criteria for cryptographically strong Boolean functions are balance, nonlinearity, and the propagation criterion. The main contributions of this paper are to reveal a number of interesting properties of balance and nonlinearity, and to study systematic methods for constructing Boolean functions that satisfy 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 balance and nonlinearity of the functions. The algebraic degrees of functions constructed are also discussed. © 1995 Academic Press, Inc.

I. INTRODUCTION

A Boolean function of $n$ input coordinates is said to satisfy the propagation criterion with respect to a nonzero 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 is the strict avalanche criterion (SAC) that coincides with the propagation criterion of degree 1. The SAC was first introduced by Webster (1985) and Webster and Tavares (1986) and was generalized in one direction by Forrè (1989) and in another direction by Adams and Tavares (1990a). A combination of the two generalizations was studied in (Preneel et al., 1991b, 1991a).

The nonlinearity of a Boolean function is defined as the minimum distance from the function to the affine functions. A cryptosystem that employs functions with a low nonlinearity is vulnerable to many cryptanalytic attacks, including the linear cryptanalysis discovered by Matsui (1993). It is well known that bent functions possess the highest nonlinearity and satisfy the propagation criterion with respect to all nonzero vectors (Dillon, 1972). However, two drawbacks of bent functions prohibit their direct application 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 (Kam and Davida, 1979; Adams and Tavares, 1990a; Seberry et al., 1993). In other words, the function has to be balanced. Some practical applications need Boolean functions with an odd number of input coordinates.

This paper studies properties and constructions of nonlinear, 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 present methods for systematically 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 high degree propagation criteria. More precisely, when $n = 2k + 1$, we construct nonlinearly balanced functions that satisfy the propagation criterion with respect to all but one nonzero vector, and when $n = 2k$, we construct functions that are balanced and also satisfy the propagation criterion with respect to all but three nonzero 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 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 remainder 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 balance 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 high degree propagation criterion are presented in Section 6. The paper is closed in Section 7 by a discussion of future work.

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 where 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 will be strictly denoted 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 \((-1)^{f(x_0)}, (-1)^{f(x_1)}, \ldots, (-1)^{f(x_{2^n - 1})}\) is called the sequence of \( f \), and the \( (0, 1) \)-sequence defined by \((f(x_0), f(x_1), \ldots, f(x_{2^n - 1}))\) is called the truth table of \( f \), where \( x_i, 0 \leq i \leq 2^n - 1 \), denotes the vector in \( V_n \), whose integer representation is \( i \). A \((0, 1)\)-sequence \((1, -1)\) sequence is said to be 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 \((a_0 b_0, \ldots, a_{2^n - 1} b_{2^n - 1})\) 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 \( f(x) = a_1 x_1 \oplus \cdots \oplus a_n x_n \oplus c \), 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) \( x \), denoted by \( W(x) \), is the number of ones in \( x \). The Hamming distance between two sequences \( x \) and \( \beta \) of the same length, denoted by \( d(x, \beta) \), 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., \( N_f = \min_{x \in GF(2)} d(f, \varphi_x) \), where \( \varphi_0, \varphi_1, \ldots, \varphi_{2^n - 1} \) denote the affine functions on \( V_n \).

The following notation will be used in this paper. Let \( \alpha = (a_1, \ldots, a_n) \) and \( \beta = (b_1, \ldots, b_n) \) 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 \( V_n \), \( \langle \alpha, \beta \rangle = a_1 b_1 + \cdots + a_n b_n \), where the addition and the multiplication are over \( GF(2) \), and when \( \alpha \) and \( \beta \) are \((1, -1)\)-sequences, \( \langle \alpha, \beta \rangle = a_1 b_1 + \cdots + a_n b_n \), 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

\[
A \otimes B = \begin{bmatrix}
a_{11} B & a_{12} B & \cdots & a_{1n} B \\
\vdots & \vdots & \ddots & \vdots \\
a_{m1} B & a_{m2} B & \cdots & a_{mn} B
\end{bmatrix},
\]

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 \( \alpha \otimes \beta = (a_1 \beta, a_2 \beta, \ldots, a_m \beta) \), 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 (Wallis et al., 1972). A special kind of Hadamard matrix, called the 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 recursive relation

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

Note that \( H_n \) can be represented as \( H_n = H_1 \otimes H_s \) for any \( s \) and \( t \) with \( s + t = n \). Such matrices are closely related to linear functions, as is shown in the following well-known lemma.
Lemma 1. Write

\[ H_n = \begin{bmatrix} l_0 \\ l_1 \\ \vdots \\ l_{2^n-1} \end{bmatrix}, \]

where \( l \) is a row of \( H_n \). Then \( l \) is the sequence of \( h = \langle x, x \rangle \), a linear function, where \( x \) 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 \( D_\delta \) 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 \( f_0, f_1, \ldots, f_{2^n-1} \) be functions on \( V_n \). Let \( \xi \) be the sequence of \( f_i \), \( i = 0, 1, \ldots, 2^n-1 \), and let \( \xi \) be the concatenation of \( \xi_0, \xi_1, \ldots, \xi_{2^n-1} \), namely, \( \xi = (\xi_0, \xi_1, \ldots, \xi_{2^n-1}) \). Then \( \xi \) is the sequence of the function on \( V_{n+q} \)

\[ f(y, x) = \bigoplus_{i=0}^{2^n-1} D_\xi(y) f_i(x), \]

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

For instance, 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 \( (1 \oplus u) f_1(x_1, \ldots, x_n) \oplus u f_2(x_1, \ldots, x_n) \), a function on \( V_{n+1} \).

We now introduce the concept of bent functions.

Definition 1. A function \( f \) on \( V_n \) is called a bent function if

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

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 the 1960s, although his pioneering work was not published in the open literature until some ten years later (Rothaus, 1976). Other issues related to bent functions, such as properties, constructions, and counting, can be found in (Adams and Tavares, 1990a; Kumar and Scholtz, 1983; Lempel and Cohn, 1982; Olsen et al., 1982; Yarlagadda and Hershey, 1989). Kumar et al. (1985) defined and studied bent functions from \( Z_q^2 \) to \( Z_q \), where \( q \) is a positive integer. Applications of bent functions to digital communications, coding theory and cryptography can be found in (Adams and Tavares, 1990b; Detombe and Tavares, 1993; Lempel and Cohn, 1982; Losev, 1987; MacWilliams and Sloane, 1977; Meier and Staffelbach, 1990; Nyberg, 1991; Olsen et al., 1982; Seberry et al., 1993).

The following result can be found in an excellent survey of bent functions by Dillon (1972).

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) \( \langle \xi, l \rangle = \pm 2^{n/2} \) for any affine sequence \( l \) of length \( 2^n \).

(iii) \( f(x) \oplus f(x \oplus \alpha) \) is balanced for any nonzero vector \( \alpha \in V_n \).

(iv) \( f(x) \oplus \langle \alpha, x \rangle \) assumes the value one \( 2^n-1 \) \( \pm 2^{n+1} \) 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.

The notion of strict avalanche criterion (SAC) was first introduced by Webster (1985) and Webster and Tavares (1985; 1986).

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.

In this paper we are also concerned with the propagation criterion, which was introduced in (Adams and Tavares, 1990a; Preneel et al., 1991b) as a generalization of the SAC.

Definition 3. Let \( f \) be a function on \( V_n \). We say that \( f \) satisfies

1. the propagation criterion with respect to a nonzero 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 \( 1 \leq W(\alpha) \leq k \).

Note that the SAC is equivalent to the propagation criterion of degree 1, and that the perfect nonlinearity studied by Meier and Staffelbach (1990) 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.

3. PROPERTIES OF BALANCE AND NONLINEARITY

This section presents a number of results related to balance and nonlinearity. These include upper bounds for nonlinearity and properties of concatenated and split sequences.

3.1. Upper Bounds on Nonlinearity

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 $2^n$ (MacWilliams and Sloane, 1977). By translating an upper bound on the covering radius of $R(1,n)$ (Cohen et al., 1985), we have:

**Lemma 4.** For any function $f$ on $V_n$, the nonlinearity $N_f$ of $f$ satisfies $N_f \leq 2^{n-1} - 2^{n/2-1}$.

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

Recall that bent functions are not balanced. From Remark 1, balanced functions cannot attain the upper bound for nonlinearities, namely $2^{n-1} - 2^{n/2-1}$. 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 5.** Let $f$ be a balanced function on $V_n$ $(n \geq 3)$. Then the nonlinearity $N_f$ of $f$ is given by

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

where $\lfloor x \rfloor$ 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. Then $N_f = \min_{\varphi_0, \varphi_1, ..., \varphi_{2^n-1}} d(f, \varphi_i)$, where $\varphi_0, \varphi_1, ..., \varphi_{2^n-1}$ denote the affine functions on $V_n$, must be even. On the other hand, since $f$ is not bent, by Remark 1 we have $N_f < 2^{n-1} - 2^{n/2-1}$. This proves the lemma.

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

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

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

3.2. Concatenating Sequences

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

**Lemma 6.** 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.** $\langle \xi_f, \xi_g \rangle = \sum_{i=0}^{2^n-1} g_i x_i = \sum_{i=0}^{2^n-1} x_i = 2^n - 2 \sum_{i=0}^{2^n-1} g_i x_i = 2^n - 2d(f, g)$. This proves the lemma.

The following lemma gives a lower bound on 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

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

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

**Proof.** Note that $\xi = \langle \xi_1, \xi_2 \rangle$ 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 $L = (l, \pm l)$, where $l$ is an affine sequence of length $2^n$. Note that $\langle \xi, L \rangle = \langle \xi_1, l \rangle \pm \langle \xi_2, l \rangle$ and thus $|\langle \xi, L \rangle| \leq P_1 + P_2$. By Lemma 6, we have $\langle \psi, L \rangle = 2^n - \frac{1}{2} \langle \xi, L \rangle \geq 2^n - \frac{1}{2} (P_1 + P_2)$. Since $\psi$ is arbitrary, we have $N_g \geq 2^n - \frac{1}{2} (P_1 + P_2)$, 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 was discovered by Meier and Staffelbach in (1990).

**Corollary 1.** 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 the 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 $\langle \xi_i, l \rangle \leq P_i$, 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 $V_{n+3}$ defined by

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

where $D_{n}(y)$ is a function on $V_n$.
where \( y = (y_1, y_2), x = (x_1, \ldots, x_8) \), and \( x_i \) 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 \( V_n \), \( N_g \geq 2^{n+1} - 2^{n+2} + 1 \).

The proof for Lemma 8 is similar to that for Lemma 7, and hence is omitted. It is a simple exercise to further generalize the lemma to the case where the sequences of \( 2^i \), \( i \geq 1 \), functions are concatenated.

By selecting proper starting functions in (1) and (2), the resulting functions can be balanced. For instance, in (1), 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 \( f(x_1, x_2, \ldots, x_8) \) be a bent function on \( V_2^8 \), let \( \eta \) be the sequence of \( f(0, x_2, \ldots, x_8) \), and let \( \eta_1 \) be the sequence of \( f(1, x_2, \ldots, x_8) \). Then for any affine sequence \( l \) of length \( 2^{k-1} \), we have \( -2^k \leq \langle \eta, l \rangle \leq 2^k \) and \( -2^k \leq \langle \eta_1, l \rangle \leq 2^k \).

**Proof.** We only give a proof for \( -2^k \leq \langle \eta, l \rangle \leq 2^k \). The other half can be proved in the same way. Since \( f(x_1, x_2, \ldots, x_8) = (1 \otimes x_1) f(0, x_2, \ldots, x_8) \oplus x_1 f(1, x_2, \ldots, x_8) \), \( \eta = (\eta_0, \eta_1) \) is the sequence of \( f(x_1, x_2, \ldots, x_8) \). Let \( L = (l, 1) \) and \( L' = (l, -1) \). By Lemma 1, both \( L \) and \( L' \) are affine sequences of length \( 2^k \).

Suppose that \( -2^k \leq \langle \eta, l \rangle \leq 2^k \) is not true. Without loss of generality assume that \( \langle \eta, l \rangle > 2^k \). There are two cases that have to be considered: \( \langle \eta, L \rangle > 0 \) and \( \langle \eta, L \rangle < 0 \). In the first case we have \( \langle \eta, L \rangle \geq \langle \eta_0, l \rangle + \langle \eta_1, l \rangle > 2^k \), and in the second case we have \( \langle \eta, L \rangle \geq \langle \eta_0, l \rangle + \langle \eta_1, l \rangle + (-1) \leq \langle \eta_0, l \rangle + (-1) \langle \eta_1, l \rangle > 2^k \), 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 split functions \( f(0, x_2, \ldots, x_8) \) and \( f(1, x_2, \ldots, x_8) \) 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.

### 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 a 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 balance 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 \( f \) (Meier and Staffelbach, 1990).

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

\[
\begin{align*}
&f(xA \oplus b) \oplus f((x \oplus \alpha) A \oplus b) \\
&= f(xA \oplus b) \oplus f((xA \oplus b) \oplus xA) \\
&= f(y) \oplus f(y \oplus \beta)
\end{align*}
\]

is balanced, where \( y = xA \oplus b \) and \( \beta = xA \). 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 discussion, 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

Recall that a bent sequence of length $2^k$ contains $2^{2^k-1} + 2^{k-1}$ ones and $2^{2^k-1} - 2^{k-1}$ zeros, or vice versa. As observed by Meier and Staffelbach (1990), complementing $2^k - 1$ positions in a bent sequence yields a balanced function on $V_{2^k}$ having a nonlinearity of at least $2^{2^k-1} - 2^k$. This nonlinearity is the same as that obtained by concatenating four bent sequences of length $2^{2^{k-2}}$ (see Lemma 8). We note, however, that concatenation is superior to complementation in that it is far easier to discuss cryptographic properties such as the propagation characteristics of functions obtained by concatenation than to discuss properties by complementation.

Now we consider the case of $V_{2^{k+1}}$. As the maximum nonlinearity of functions on $V_2$ coincides with the covering radius of the first order binary Reed–Muller code $R(1, n)$ of length $2^n$, using a result of (Patterson and Wiedemann, 1983), we can construct unbalanced functions on $V_{2^{k+1}}$, $k \geq 7$, whose nonlinearity is at least $2^{2^{k}} - (108/128) 2^{2^{k}}$, a higher value than $2^{2^{k}} - 2^{k}$ achieved by the construction in Corollary 1. One might be tempted to think that modifying the sequences in (Patterson and Wiedemann, 1983) 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 $V_4$ for an example. The Hamming weight of the sequences on $V_{15}$, which have the largest nonlinearity of 16,276, is 16,492. Changing 54 positions makes them balanced. The nonlinearity of the resulting functions is 16,222, smaller than 16,256 achieved by concatenating two bent sequences of length $2^{2^{k}}$ (see Corollary 1).

To summarize the above discussions, so far the best result on constructing nonlinearly balanced functions on $V_2$ is by concatenating four bent sequences of length $2^{2^{k-2}}$, while the best result on $V_{2^{k+1}}$ is by concatenating two bent sequences of length $2^{2^{k}}$, or by splitting a bent sequence of length $2^{2^{k+2}}$.

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 on $V_{2^k}$ are balanced and have a much higher nonlinearity than that attainable by concatenating four bent sequences. This result, in conjunction with sequences in (Patterson and Wiedemann, 1983), allows us to construct balanced functions on $V_{2^{k+1}}$, $k \geq 14$, that have a higher nonlinearity than that achieved by concatenating or splitting bent sequences. These results represent a significant improvement on the previously known construction methods.

4.1. On $V_{2^k}$

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

Lemma 11. For any integer $i \geq 1$ there exists

(i) a balanced function $f$ on $V_{4r}$ such that $N_f \geq 2^{4r-1} - 2^{2r-1} - 2^{r} - 1$.

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

Proof. (i) Let $l_i$ be the $i$th row of $H_{2^i}$, where $i = 0, 1, 2, ..., 2^r - 1$. Then $\xi = (l_0, l_1, ..., l_{2^r-1})$ is a bent sequence of length $2^{2r}$.

Note that except for $l_0 = (1, 1, ..., 1)$, all other $l_i$ ($i = 1, 2, ..., 2^r - 1$) are balanced sequences of length $2^{2r}$. Therefore replacing the all-one (or ‘flat’) leading sequence $l_0$ 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 $l_i^* = (e_1, e_1, e_2, ..., e_{2^r-1})$, where $e_i$ is the $i$th row of $H_{2^r}$. Note that the leading sequence in $l_i^*$ is $e_1$ but not $e_0 = (1, 1, ..., 1)$. $l_i^*$ is a balanced sequence of length $2^{2r}$, since all $e_i$, $i = 1, 2, ..., 2^r - 1$, are balanced sequences of length $2^i$. Replacing $l_0$ by $l_i^*$, we get a balanced sequence $\xi^* = (l_0^*, l_1, ..., l_{2^r-1})$.

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

$$|\langle \xi^*, L \rangle| \leq |\langle l_0^*, l_i \rangle| + |\langle l_i, l_j \rangle| \leq |\langle l_0^*, l_i \rangle| + 2^{2^{r}}.$$

We proceed to estimate $|\langle l_0^*, l_i \rangle|$. Note that $H_{2r} = H_{2r} \otimes H_{2r}$, $l_i$ can be expressed as $l_i = e_i \otimes e_i$, where $e_i$ and $e_j$ are rows of $H_{2r}$. Write $e_i = (b_0, b_1, ..., b_{2^r-1})$. Then $l_i = (b_0 e_i, ..., b_{2^r-1} e_i)$. Similarly to the discussion for $|\langle \xi^*, L \rangle|$, we have

$$|\langle l_0^*, l_i \rangle| \leq |\langle e_i, e_i \rangle| = 2^{2^{r}-1}, \quad \text{if} \quad v = 1,$$

$$|\langle l_0^*, l_i \rangle| \leq |\langle e_i, e_i \rangle| = 2^{2^{r}-1}, \quad \text{if} \quad v = 2, ..., 2^{r}-1,$$

$$|\langle l_0^*, l_i \rangle| \leq 0, \quad \text{if} \quad v = 0.$$

Thus $|\langle l_0^*, l_i \rangle| \leq 2^{2^{r}-1} + 1$ and hence $|\langle \xi^*, L \rangle| \leq 2^{2^{r}+1} + 2^{2^{r}}$.

By Lemma 6, $d(f^*, \varphi) \geq 2^{4r-1} - 1 - |\langle \xi^*, L \rangle| \geq 2^{4r-1} - 2^{2^{r}-1} - 2^{r} - 1$. Since $\varphi$ is arbitrary, $N_f \geq 2^{4r-1} - 2^{2^{r}-1} - 2^{r} - 1$. 


(ii) Now consider the case of \( V_{2r+2} \). Let \( l_i, i = 0, 1, \ldots, 2^{2r+1} - 1 \), be the \( i \)th row of \( H_{2r+1} \). Then \( \xi = (l_0, l_1, \ldots, l_{2^{2r+1} - 1}) \) is a bent sequence of length \( 2^{2r+2} \).

The replacement for the all-one leading sequence \( l_0 = (1, 1, \ldots, 1) \in V_{2^{2r+1}} \) is the following balanced sequence \( l_0^* = (e_0, e_1, \ldots, e_{2^{2r+1} - 1}) \), the concatenation of the 2\(^{th}\), the \( (2^{r+1})\)th, \ldots, and the \( (2^{r+1} - 1)\)th rows of \( H_{2r+1} \). Let \( \xi^* = (l_0^*, l_1, l_2, \ldots, l_{2^{2r+1} - 1}) \), and let \( f^* \) be the function corresponding to the balanced sequence.

Similarly, to the case of \( V_{2^r} \), let \( \phi \) be a affine function on \( V_{2^{2r+2}} \) and let \( L \) be its sequence. \( L \) can be expressed as \( L = \pm l_i \otimes l_j \), where \( l_i, l_j \) are rows of \( H_{2^{2r+1}} \). Hence

\[
|\langle \xi^*, L \rangle| \leq |\langle l_0^*, l_j \rangle| + |\langle l_i, l_j \rangle| \leq |\langle l_0^*, l_j \rangle| + 2^{2r+1}.
\]

Since \( l_0^* \) is obtained by splitting the bent sequence \( (e_0, e_1, \ldots, e_{2^{2r+1} - 1}) \), where \( e_i \) is a row of \( H_{2r+1} \), by Lemma 9, we have \( |\langle l_0^*, l_j \rangle| \leq 2^{2r+1} \). From this it follows that \( |\langle \xi^*, L \rangle| \leq 2^{2r+1} + 2^{2r+1} = 2^{2r+2} \) and \( N_f \geq 2^{2r+2} - 2^{2r+1} \).

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

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

The modifying procedure for the case of \( n = 2^r(2t+1), s \geq 1 \) 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 \( 2^{2r+1} \). The last leading sequence is replaced by \( l_0^* = (e_0, e_1, \ldots, e_{2^{2r+1} - 1}) \), the second half of the bent sequence \( (e_0, e_1, \ldots, e_{2^{2r+1} - 1}) \), where each \( e_i \) is a row of \( H_{2r+1} \). Again by induction on \( s = 1, 2, 3, \ldots \), it can be proved that the nonlinearity of the resulting function is at least

\[
2^{2^{r+1}} + \frac{1}{2}(2^{2^{r-1}2r+1} + 2^{2^{r-2}2r+1} + \cdots + 2^{2+1} + 2^{r+1}).
\]

We have completed the proof for

**Theorem 1.** For any even number \( n \geq 4 \), there exists a balanced function \( f^* \) on \( V_n \) whose nonlinearity is

\[
\begin{align*}
N_f &\geq \begin{cases}
2^{2^{r+1}} - \frac{1}{2}(2^{2^{r-1}2r+1} + 2^{2^{r-2}2r+1} + \cdots + 2^2 + 2 \cdot 2^2), & n = 2^m,
2^{2^{r+1} + 1} - \frac{1}{2}(2^{2^{r-1}(2r+1)} + 2^{2^{r-2}(2r+1)} + \cdots + 2^{2+1} + 2^{r+1}), & n = 2^r(2t+1).
\end{cases}
\end{align*}
\]

Let \( \xi = (\xi_0, \xi_1, \ldots, \xi_{2^r-1}) \) 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 \( \xi \). In this way we obtain in total \( 2^{2^r} \cdot 2^k \) different balanced functions, all of which have the same nonlinearity. Even more functions can be obtained by observing the fact that the leading sequence \( \xi_0 \) has exactly the same structure as the large sequence \( \xi \), and hence permuting and changing signs can also be applied to \( \xi_0 \).

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 Lemma 5), are also presented.

### Table 1

<table>
<thead>
<tr>
<th>Vector Space</th>
<th>( V_4 )</th>
<th>( V_6 )</th>
<th>( V_8 )</th>
<th>( V_{10} )</th>
<th>( V_{12} )</th>
<th>( V_{14} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upper bound (( \leq ))</td>
<td>4</td>
<td>26</td>
<td>118</td>
<td>494</td>
<td>2014</td>
<td>8126</td>
</tr>
<tr>
<td>By modification (( \geq ))</td>
<td>4</td>
<td>26</td>
<td>116</td>
<td>492</td>
<td>2010</td>
<td>8120</td>
</tr>
<tr>
<td>By concatenation (( \geq ))</td>
<td>4</td>
<td>24</td>
<td>112</td>
<td>480</td>
<td>1984</td>
<td>8064</td>
</tr>
</tbody>
</table>

4.2. On \( V_{2^k+1} \)

The following lemma can be confirmed easily and is very useful in obtaining balanced functions.

**Lemma 12.** 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

1. \( f_1(x_1, \ldots, x_s) \oplus f_2(y_1, \ldots, y_t) \) is a balanced function on \( V_{s+t} \), if \( f_1 \) or \( f_2 \) is balanced.
2. 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 13.** Let \( \xi \) be the sequence of \( f_1 \) on \( V_s \) and \( \xi_2 \) be the sequence of \( f_2 \) on \( V_t \). Also let

\[
g(x_1, \ldots, x_s, y_1, \ldots, y_t) = f_1(x_1, \ldots, x_s) \oplus f_2(y_1, \ldots, y_t).
\]
Assume that \( \langle \xi_1, l_1 \rangle \leq P_1 \) and \( \langle \xi_2, l_2 \rangle \leq P_2 \), where \( l_1 \) is an arbitrary affine sequence of length \( 2^l \), \( l_2 \) is an arbitrary affine sequence of length \( 2^l \), and \( P_1 \) and \( P_2 \) are positive integers. Then the nonlinearity of \( g \) satisfies \( N_g \geq 2^{2^l+1} - \frac{1}{2} P_1 \cdot P_2 \).

**Proof.** Note that \( \xi = \xi_2 \otimes \xi_2 \) is the sequence of \( g \). Let \( \varphi \) be an arbitrary affine function on \( V_{x_1} \), and let \( l \) be the sequence of \( \varphi \). Then \( l \) can be expressed as \( l = l_1 \otimes l_2 \), where \( l_1 \) is a row of \( H_l \) and \( l_2 \) is a row of \( H_2 \). Since

\[
\langle \xi, l \rangle = \langle \xi_1 \otimes \xi_2, l_1 \otimes l_2 \rangle = \langle \xi_1, l_1 \rangle \cdot \langle \xi_2, l_2 \rangle,
\]

we have

\[
|\langle \xi, l \rangle| = |\langle \xi_1, l_1 \rangle| \cdot |\langle \xi_2, l_2 \rangle| \leq P_1 \cdot P_2,
\]

and by Lemma 6,

\[
d(g, \varphi) \geq 2^{2^l+1} - \frac{1}{2} P_1 \cdot P_2.
\]

Due to the arbitrariness of \( \varphi \), we have \( N_g \geq 2^{2^l+1} - \frac{1}{2} P_1 \cdot P_2 \).

Let \( \xi_1 \) be a balanced sequence of length \( 2^{2k} \) that is constructed using the method in the proof of Theorem 1, where \( k \geq 2 \). Let \( \xi_2 \) be a sequence of length \( 2^{15} \) obtained by the method of Patterson and Wiedemann (1983). Note that the nonlinearity of \( \xi_2 \) is 16,276, and there are 13,021 such sequences. Denote by \( f_1 \) the function corresponding to \( \xi_1 \) and by \( f_2 \) the function corresponding to \( \xi_2 \). Let

\[
f(x_1, ..., x_{2k}, x_{2k+1}, ..., x_{2k+15}) = f_1(x_1, ..., x_{2k}) \oplus f_2(x_{2k+1}, ..., x_{2k+15}).
\]

Note that

\[
\langle \xi_1, l_1 \rangle \leq \begin{cases} 2^{2^l+1} + 2^{2^l-1} + \cdots + 2^2 + 2 \cdot 2^2, \\ 2k = 2^m, \\ 2^{2^l-2m} + 2^{2^l-2m+1} + \cdots + 2^{2i+1} + 2^{2i+1} + 2^{2j+1}, \\ 2k = 2^l(2t + 1), \end{cases}
\]

and

\[
\langle \xi_2, l_2 \rangle \leq 2 \cdot (2^{14} - 16,276) = 216,
\]

where \( l_2 \) is a linear sequence of length \( 2^{2k} \), and \( l_2 \) is a linear sequence of length \( 2^{15} \). Then by Lemma 13, we have

**Theorem 2.** The function \( f \) defined by (3) is a balanced function on \( V_{2k+15} \), \( k \geq 2 \), whose nonlinearity is at least \( 2^{2^l+14} - 108(2^{2^l-1} + 2^{2^l-2} + \cdots + 2^2 + 2 \cdot 2^2), \)

\[
k_2 = 2^m,
\]

\[
N_g \geq 2^{2^l(2t+1)+1} - 108(2^{2^l-2m+1} + 2^{2^l-2m+1} + \cdots + 2^{2^l-2m+1} + 2^{2i+1} + 2^{2i+1}),
\]

\[
k_2 = 2^l(2t+1).
\]

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 \( k \geq 7 \).

**5. CONSTRUCTING HIGHLY NONLINEAR BALANCED FUNCTIONS SATISFYING THE 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 \( k \geq 1 \), \( f \) a bent function, and \( h \) a nonconstant 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 for \( f(x) \oplus h(x) \). Let \( g \) be a function on \( V_{2k+1} \) defined by

\[
g(u, x_1, ..., x_{2k}) = (1 \oplus u) f(x_1, ..., x_{2k})
\]

\[
\oplus u(h(x_1, ..., x_{2k}) \oplus h(x_1, ..., x_{2k}))
\]

\[
f(x_1, ..., x_{2k}) \oplus uh(x_1, ..., x_{2k}).
\]

By Lemma 2 the sequence of \( g \) is the concatenation of the sequences of \( f(x) \) and \( f(x) \oplus h(x) \). Thus we have

**Lemma 14.** The function \( g \) defined by (4) is a balanced function on \( V_{2k+1} \).

The following lemma is a direct consequence of Corollary 1.

**Lemma 15.** \( N_g \geq 2^{2k} - 2^k \) where \( g \) is defined by (4).

**Lemma 16.** The function \( g \) defined by (4) satisfies the SAC.

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

**Case 1.** \( b = 0 \) and hence \( W(\alpha) = 1 \). Then \( g(z) \oplus g(z \oplus \gamma) = f(x) \oplus f(x \oplus \alpha) \oplus uh(x) \oplus h(x \oplus \alpha) \). Since \( h \) is an affine function, \( h(x) \oplus h(x \oplus \alpha) = c \), where \( c \) is a constant from \( GF(2) \). Thus \( g(z) \oplus g(z \oplus \gamma) = f(x) \oplus f(x \oplus \alpha) \oplus c \). By (3) 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 \( V_{2k+1} \).

**Theorem 2.** The function \( f \) defined by (3) is a balanced function on \( V_{2k+15} \), \( k \geq 2 \), whose nonlinearity is at least \( 2^{2^l+14} - 108(2^{2^l-1} + 2^{2^l-2} + \cdots + 2^2 + 2 \cdot 2^2), \)

\[
k_2 = 2^m,
\]

\[
N_g \geq 2^{2^l(2t+1)+1} - 108(2^{2^l-2m+1} + 2^{2^l-2m+1} + \cdots + 2^{2^l-2m+1} + 2^{2i+1} + 2^{2i+1}),
\]

\[
k_2 = 2^l(2t+1).
\]
Case 2. \( b = 1 \) and hence \( W(\alpha) = 0 \), i.e., \( \alpha = (0, 0, ..., 0) \). Then \( g(z) \oplus g(z \oplus \gamma) = h(x) \). Since \( h(x) \) is a nonconstant 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 \( k \geq 1 \), \( g \) defined by (4) is a balanced function on \( V_{2k-1} \) having \( N_x \geq 2^{2k} - 2^k \) and satisfying the SAC.

Recently Zheng et al. (1993) 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.

### 5.2. On \( V_{2k} \)

Let \( k \geq 2 \) and \( f \) a bent function on \( V_{2k-2} \). Let \( h_1, h_2, \) and \( h_3 \) be nonconstant affine functions on \( V_{2k-2} \) such that \( h_i(x) \oplus h_j(x) \) is nonconstant for any \( i \neq j \). Such affine functions exist for all \( k \geq 2 \). Let \( x = (x_1, ..., x_{2k-2}) \). 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. Let \( g \) be a function on \( V_{2k} \) defined by

\[
g(u, v, x_1, ..., x_{2k-2}) = (1 \oplus u)(1 \oplus v) f(x) = (1 \oplus u)(1 \oplus v) f(x) \oplus h_1(x))
\]

\[
\oplus u(1 \oplus v)(f(x) \oplus h_2(x)) \oplus v(1 \oplus u)(f(x) \oplus h_3(x))
\]

\[
= f(x) \oplus v h_1(x) \oplus u h_2(x) \oplus u h_3(x).
\]

(5)

**Lemma 17.** \( g \) defined by (5) 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.** \( N_x \geq 2^{2k-1} - 2^k \), where \( g \) is defined by (5).

**Proof.** This follows from Corollary 1.

**Lemma 19.** The function \( g \) defined by (5) satisfies the SAC.

**Proof.** Let \( \gamma = (b, c, a_1, ..., a_{2k-2}) \) be any vector in \( V_{2k} \) with \( W(\gamma) = 1 \). Write \( \alpha = (a_1, ..., a_{2k-2}), \) \( z = (u, v, x_1, ..., x_{2k-2}) \), and \( x = (x_1, ..., x_{2k-2}) \). Note that \( g(z \oplus \gamma) = f(x \oplus \alpha) \oplus (v \oplus c) h_1(x \oplus \alpha) \oplus (u \oplus b) h_2(x \oplus \alpha) \oplus (u \oplus b) h_3(x \oplus \alpha) \). Consider the balance 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., \( \alpha = (0, 0, ..., 0) \). In this case, \( g(z) \oplus g(z \oplus \gamma) = h_3(x) \oplus (h_1(x) \oplus h_2(x) \oplus h_3(x)) \) will be \( h_3(x) \) when \( v = 0 \) and \( h_1(x) \oplus h_2(x) \) when \( v = 1 \). Both \( h_3(x) \) and \( h_1(x) \oplus h_2(x) \) are nonconstant affine functions on \( V_{2k-1} \) 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., \( \alpha = (0, 0, ..., 0) \). The proof of the balance 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 \( h_3 \) is an affine function, \( h_3(x) \oplus h_3(x \oplus \alpha) = a_j \), where \( a_j \) is a constant from \( GF(2) \). Hence \( g(z) \oplus g(z \oplus \gamma) = f(x) \oplus f(x \oplus \alpha) \oplus v a_1 \oplus u a_2 \oplus u v a_3 \). 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 \( V_{2k} \). This proves that \( g \) satisfies the SAC.

Summarizing Lemmas 17, 18, and 19, we have

**Theorem 4.** For \( k \geq 2 \), \( g \) defined by (5) is a balanced function on \( V_{2k} \) having \( N_x \geq 2^{2k-1} - 2^k \) and satisfying the SAC.

### 5.3. Remarks

We have shown that a function on \( V_n \) constructed according to (4) and (5) satisfies 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, and it is not hard to show that the total number of vectors in \( V_{2k+1} \) such that a function constructed by (4) satisfies the propagation criterion is \( 2^{2k+2} - 2^{k+1} \), while the total number of vectors in \( V_{2k} \) such that a function constructed by (5) satisfies the propagation criterion 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 (4) and (5), 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:

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

Bent functions with higher algebraic degrees exist and there are many methods for constructing such functions (Dillon, 1972). The following is a method discovered by Dillon and Maiorana (1972, 1985) 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 (4) and (5) can achieve a wide range of algebraic degrees, namely 2, ..., $k$ and 2, ..., $k - 1$, respectively.

6. CONSTRUCTING HIGHLY NONLINEAR BALANCED FUNCTIONS SATISFYING HIGH DEGREE PROPAGATION CRITERION

Another interesting topic is methods for constructing balanced and possess good propagation characteristics. In (Preneel et al., 1991a), it was suggested that a function $f$ on $V_n$ which has a zero point in its Walsh spectrum could 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. Two types of such functions are (1) bent functions and (2) highly nonlinear functions obtained by complementing a single position in a bent sequence. In the following we describe two methods for systematically constructing highly nonlinear balanced functions satisfying high degree propagation criterion.

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

$$g(x_1, x_2, \ldots, x_{2k+1}) = (1 \oplus x_1)f(x_2, \ldots, x_{2k+1})$$
$$\oplus x_1(1 \oplus f(x_2, \ldots, x_{2k+1}))$$
$$= x_1 \oplus f(x_2, \ldots, x_{2k+1}). \quad (6)$$

**LEMMA 20.** The function $g$ defined in (6) satisfies the propagation criterion with respect to all nonzero vectors $y \in V_{2k+1}$ with $y \neq (1, 0, \ldots, 0)$.

**Proof.** Let $y = (a_1, a_2, \ldots, a_{2k+1}) \neq (1, 0, \ldots, 0)$ and let $x = (x_1, x_2, \ldots, x_{2k+1})$. Then $g(x) \oplus g(x \oplus y) = a_1 \oplus f(x_2, \ldots, x_{2k+1}) \oplus f(x_2 \oplus a_2, \ldots, x_{2k+1} \oplus a_{2k+1})$. 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, $g(x) \oplus g(x \oplus y)$ is balanced for all $y = (a_1, a_2, \ldots, a_{2k+1}) \neq (1, 0, \ldots, 0)$. |}

From Corollary 1, the nonlinearity of the function $g$ defined by (6) satisfies $N_g \geq 2^{2k} - 2^k$. Furthermore, by Lemma 12, $g$ is balanced. Thus we have

**COROLLARY 2.** The function $g$ defined by (6) is balanced and satisfies the propagation criterion with respect to all nonzero vectors $y \in V_{2k+1}$ with $y \neq (1, 0, \ldots, 0)$. The nonlinearity of $g$ satisfies $N_g \geq 2^{2k} - 2^k$.

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:

$$g(x_1, x_2, x_3, \ldots, x_{2k}) = (1 \oplus x_1)(1 \oplus x_2)f(x_3, \ldots, x_{2k})$$
$$\oplus (1 \oplus x_1)x_2(1 \oplus f(x_3, \ldots, x_{2k}))$$
$$\oplus x_1x_2f(x_3, \ldots, x_{2k})$$
$$= x_1 \oplus x_2 \oplus f(x_3, \ldots, x_{2k}). \quad (7)$$

**LEMMA 21.** The function $g$ defined in (7) satisfies the propagation criterion with respect to all but three nonzero vectors in $V_{2k}$. The three vectors where the propagation criterion is not satisfied are $y_1 = (1, 0, 0, \ldots, 0)$, $y_2 = (0, 1, 0, \ldots, 0)$, and $y_3 = y_1 \oplus y_2 = (1, 1, 0, \ldots, 0)$.

**Proof.** Let $y = (a_1, a_2, \ldots, a_{2k})$ be a nonzero vector in $V_{2k}$ differing from $y_1, y_2, y_3$. Also let $x = (x_1, \ldots, x_{2k})$. Then we have $g(x) \oplus g(x \oplus y) = a_1 \oplus a_2 \oplus f(x_3, \ldots, x_{2k}) \oplus f(x_3 \oplus a_3, \ldots, x_{2k} \oplus a_{2k})$. 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 $g(x) \oplus g(x \oplus y)$ is balanced for any nonzero vector $y$ in $V_{2k}$ differing from $y_1, y_2, y_3$, thus proving the lemma.

Since $x_1 \oplus x_2$ is balanced on $V_{2k}$, $g$ is balanced on $V_{2k}$. On the other hand, by Lemma 7, we have $N_g \geq 2^{2k-1} - 2^k$. Thus we have the following result:

**COROLLARY 3.** The function $g$ defined by (7) is balanced and satisfies the propagation criterion with respect to all nonzero vectors $y \in V_{2k}$ with $y \neq (c_1, c_2, 0, \ldots, 0)$, where $c_1, c_2 \in GF(2)$. The nonlinearity of $g$ satisfies $N_g \geq 2^{2k-1} - 2^k$.

6.2. Moving Vectors Around

Though functions constructed according to (6) or (7) satisfy the propagation criterion with respect to all but one or three nonzero vectors, they only fulfill the propagation criterion of degree zero. Therefore these functions are not interesting in practical applications. Recall that the balance, 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 (6) or (7), 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 high degree propagation criterion.

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

**Theorem 5.** For any nonzero 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 nonzero 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 (6). From linear algebra we know that for any bases $B_1$ and $B_2$ of the vector space $V_{2k+1}$, where $B_1 = \{x_j \mid j = 1, \ldots, 2k+1\}$ and $B_2 = \{\beta_j \mid j = 1, \ldots, 2k+1\}$, there exists a unique nondegenerate matrix $A$ of order $2k+1$ with entries from $GF(2)$ such that $\gamma, A = \beta, j = 1, \ldots, 2k+1$. In particular, this is true when $x_j = \gamma^*$ and $\beta_j = (1, 0, \ldots, 0)$. 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 nonzero vectors except $\gamma^*$.

Let $\gamma$ be a nonzero vector in $V_{2k+1}$ with $\gamma \neq \gamma^*$. Consider the function $g^*(x) \oplus g^*(x \oplus \gamma) = g(xA) \oplus g(xA \oplus \gamma A) = g(\gamma) \oplus g(\gamma \oplus \gamma A)$, where $\gamma = xA$. Note that $A$ is nondegenerate and thus $\gamma$ 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, $g(\gamma) \oplus g(\gamma \oplus \gamma A)$ 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 nonzero 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 4.** 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 $N_{g^*} \geq 2^{2k} - 2^k$.

6.2.2. On $V_{2k}$

**Theorem 6.** For any nonzero 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 nonzero 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 $B_1 = \{x_j \mid j = 1, \ldots, 2k\}$ and $B_2 = \{\beta_j \mid j = 1, \ldots, 2k\}$. By linear algebra, we can let $x_1 = \gamma_1^*$, $x_2 = \gamma_2^*$, $\beta_1 = (1, 0, \ldots, 0)$, and $\beta_2 = (0, 1, 0, \ldots, 0)$. 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 nonzero vectors in $V_{2k}$: $\gamma_1^*$, $\gamma_2^*$, 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 (7), and $A$ is the unique nondegenerate matrix such that $x_j = \beta_j = (1, \ldots, 1)$. 2k.

Similarly to the case on $V_{2k+1}$, we can obtain highly nonlinear balanced functions satisfying high degree propagation criteria by properly selecting vectors $\gamma_1^*$ and $\gamma_2^*$. In contrast to the case on $V_{2k+1}$, however, the degree of propagation criterion the functions can achieve is $\frac{1}{2}k$, but not $2k-1$. The construction method is described in the following corollary.

**Corollary 5.** 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 $\gamma^+_1 = (a_1, ..., a_{3t+c})$ and $\gamma^+_2 = (b_1, ..., b_{3t+c})$, where

\[
\begin{align*}
a_j &= \begin{cases} 
1 & \text{for } j = 1, ..., 2t + c_1, \\
0 & \text{for } j = 2t + c_1 + 1, ..., 3t + c,
\end{cases} \\
b_j &= \begin{cases} 
0 & \text{for } j = 1, ..., t + c_1, \\
1 & \text{for } j = t + c_1 + 1, ..., 3t + c.
\end{cases}
\end{align*}
\]

By Theorem 6 there exists a balanced function $g^*$ on $V_{2k}$ satisfying the propagation criterion with respect to all but three nonzero vectors in $V_{2k}$. The three vectors are $\gamma^+_1$, $\gamma^+_2$, and $\gamma^+_1 \oplus \gamma^+_2$. The nonlinearity of $g^*$ satisfies $N_{g^*} \leq 2^{2k-1} - 2^k$.

Note that $W(\gamma^+_1) = 2t + c_1$, $W(\gamma^+_2) = 2t + c_2$, and $W(\gamma^+_1 \oplus \gamma^+_2) = 2t + c_1 + c_2 = 2t + c$. 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 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

Comparing (4) with (6), one can see that the difference between the two constructions lies in the selection of the affine functions. In (4) a nonconstant affine function $h$ is selected, while in (6) a constant 1 is employed. In a sense, the two constructions complement one another. A similar observation applies to the case of (5) and (7).

Functions obtained by (6) and (7) can achieve a wide range of algebraic degrees, namely 2, ..., $k$ and 2, ..., $k - 1$, 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 $V_5$ that satisfy the propagation criterion with respect to all but one vector in $V_5$. (They called these functions near bent functions.) They obtained the functions by the use of the cubing technique suggested by Pieprzyk (1991). Propagation characteristics of quadratic functions were also studied extensively in (Preneel et al., 1991a). 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.

7. CONCLUDING REMARKS

We have studied properties of balance and nonlinearity of Boolean functions including concatenating, splitting, modifying, and multiplying sequences. A novel method has been presented for constructing balanced functions whose nonlinearity is much higher than that attained by any previously known construction. In addition, systematic methods have been presented for constructing highly nonlinear balanced functions satisfying the SAC or 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 balance 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 (6) are optimal in the sense that they fulfill the propagation criterion with respect to $2^{2k+1} - 2$ nonzero vectors, and after the affine transformation of coordinates, they satisfy the propagation criterion of degree $2k$. For $V_{2k}$, the number of nonzero vectors given by (7) is $2^{2k-4}$ and the degree after the transformation is $4k/3$. 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.

ACKNOWLEDGMENTS

This work was supported by Telecom Australia under Contract 7027 and by the Australian Research Council under Reference Numbers A4830241, A49130102, A9030136, A49131885, and A49232172. The authors thank the anonymous referees for their helpful comments.

Received May 17, 1993; final manuscript received November 30, 1993

REFERENCES

HIGHLY NONLINEAR BALANCED BOOLEAN FUNCTIONS


