On Distribution of Boolean Functions With Nonlinearity $\leq 2^{n-2}$

Chuan-Kun Wu*

Department of Computing
University of Western Sydney (Nepean)
PO Box 10, Kingswood NSW 2747
AUSTRALIA
E-mail: c.wu@uws.edu.au

Abstract

The nonlinearity of a Boolean function, which is defined as its distance from the set of affine functions, is an important measuring index in cryptographic applications. The distribution of nonlinearities over all the Boolean functions is equivalent to the weight distribution of first order Reed-Muller codes and is very difficult to determine. As the first step towards solving this problem, the distribution of Boolean functions with nonlinearity $\leq 2^{n-2}$ is presented in this paper. It is shown that the number of Boolean functions with nonlinearity t is exactly $\binom{2^n}{t} \cdot 2^{n+1}$ for $t < 2^{n-2}$ and $2^{n+1}\left[\binom{2^n}{2^{n-2}} - (2^n-1)\binom{2^{n-1}}{2^{n-2}} + \binom{2^n-1}{2}\right]$ for $t = 2^{n-2}$.

1 Introduction

It was indicated in [1] that any cryptosystem can be described by a nonlinear function. The nonlinearity of Boolean functions, which have largely been used in cryptology, is then an important index. There has been much study of the problems relating to the nonlinearity of Boolean functions. This paper aims to give an explicit expression for the number of Boolean functions with nonlinearity $\leq 2^{n-2}$.

2 Preliminaries

A function f: $\mathrm{GF}^n(2) \longrightarrow \mathrm{GF}(2)$ is called a *Boolean function* of n variables. $f(x)$ is called an *affine* function if there exist $a_0, a_1, \ldots, a_n \in \mathrm{GF}(2)$ such that $f(x) = a_0 \oplus a_1x_1 \oplus \cdots \oplus a_nx_n$, where $x = (x_1, \ldots, x_n) \in \mathrm{GF}^n(2)$ and $\oplus$ means modulo 2

addition. In particular, $f(x)$ is also called a *linear* function if $a_0 = 0$. We will call $f(x)$ a *nonsingular affine function* if $a_0 = 1$. The input $x = (x_1, ..., x_n)$ will be treated as *unbiased*, i.e., for every $(a_1, ..., a_n) \in GF^n(2)$, we have $Prob((x_1, ..., x_n) = (a_1, ..., a_n)) = \frac{1}{2^n}$. A Boolean function $f(x)$ can be expressed in three different ways: minterm expression, polynomial expression (in some papers this is also called the algebraic normal form) and truth-table expression. The latter two expressions will be adopted in this paper. We will treat a function $f \in \mathcal{F}_n$ as a vector of length 2^n and a polynomial of x_1, ..., x_n alternatively. The *Hamming weight* of a binary vector α, denoted by $W_H(\alpha)$, is the number of ones in α, and similarly the Hamming weight of a Boolean function $f(x)$, denoted by $W_H(f)$, is then the number of ones in its truth-table. $f(x)$ is called *balanced* if $W_H(f) = 2^{n-1}$. The *degree* of $f(x)$, denoted by $\deg(f)$, is the largest number of variables that appear in one product term of its polynomial expression. We will denote by $\mathcal{F}_n$ the set of all Boolean functions of n variables and by $\mathcal{L}_n$ the affine ones.

The *distance* between two Boolean functions f and g is defined as the number of different components in their truth tables and denoted by $d(f, g) = W_H(f \oplus g)$. The nonlinearity of f, denoted by N_f, is the least distance of f from the affine functions, i.e.,

$$N_f = \min_{l \in \mathcal{L}_n} d(f, l) = \min_{l \in \mathcal{L}_n} W_H(f \oplus l).$$

3 Nonlinearity distribution when less than 2^{n-2}

It is easy to see that $\mathcal{L}_n$ is a vector subspace of $\mathcal{F}_n$. We make a coset decomposition of $\mathcal{F}_n$ upon $\mathcal{L}_n$ as follows:

$$\mathcal{F}_n = \bigcup_{\alpha \in D} (\alpha \oplus \mathcal{L}_n) \tag{1}$$

where D is a set of nonlinear Boolean functions with cardinality 2^{2^n-n-1} and each coset leader $\alpha \in D$ is a Boolean function with least Hamming weight (it is not necessarily unique). By the definitions above we have

Theorem 1 *In coset decomposition (1), for any function $f \in (\alpha \oplus \mathcal{L}_n)$, we have $N_f = W_H(\alpha)$.*

By theorem 1 we know that the problem of determining the nonlinearity of Boolean functions can be transfered to the determination of the Hamming weight of coset leaders in equation (1). If there is more than one function having the same least Hamming weight, any one can act as the coset leader.

Theorem 2 *Let α_1 and α_2 be two coset leaders of $\mathcal{L}_n$ with $W_H(\alpha_1) = W_H(\alpha_2) < 2^{n-2}$. Then α_1 and α_2 belong to a same coset if and only if $\alpha_1 = \alpha_2$.*

Proof: Suppose that α_1 and α_2 belong to a same coset and $\alpha_1 \neq \alpha_2$. Then there must be a nonzero affine function $l \in \mathcal{L}_n$ such that $\alpha_2 = \alpha_1 \oplus l$, or $\alpha_1 \oplus \alpha_2 = l$. It is well known that for a nonzero affine function $l \in \mathcal{L}_n$ we have $W_H(l) = 2^{n-1}$ if and

only if $l \neq 1$. But $W_H(\alpha_1 \oplus \alpha_2) \leq W_H(\alpha_1) \oplus W_H(\alpha_2) < 2^{n-1}$, this is a contradiction. The conclusion of theorem 2 then follows. □

Denote by $\sigma_n(t)$ the number of Boolean functions in $\mathcal{F}_n$ with nonlinearity t. Then by theorem 2 it is known that for $0 \leq t < 2^{n-2}$, the number of Boolean functions with Hamming weight t is exactly $\binom{2^n}{t}$, and they all belong to different cosets where they can act as a coset leader. By theorem 1 we have

Theorem 3 *Let $t < 2^{n-2}$. Then the number of Boolean functions of $\mathcal{F}_n$ with nonlinearity t is*

$$\sigma_n(t) = \binom{2^n}{t} \cdot 2^{n+1} \tag{2}$$

4 Number of Boolean functions with nonlinearity 2^{n-2}

The following lemmas will be needed in determining the number of Boolean functions with nonlinearity 2^{n-2}.

Lemma 1 *Let $\alpha \in \mathcal{F}_n$. If there is a function β in the same coset with α such that $W_H(\beta) < W_H(\alpha)$, then we have $W_H(\alpha) > 2^{n-2}$.*

Proof: By the assumption it is known that there must exist a nonzero affine function $l \in \mathcal{L}_n$ such that $\beta = \alpha \oplus l$. Then $W_H(\beta) = W_H(\alpha \oplus l) = W_H(\alpha) + W_H(l) - 2W_H(\alpha \cdot l)$. So we have $W_H(\alpha \cdot l) > \frac{1}{2}W_H(l) \geq 2^{n-2}$ and hence $W_H(\alpha) \geq W_H(\alpha \cdot l) > 2^{n-2}$. □

Lemma 1 implies that a function of Hamming weight 2^{n-2} is guaranteed to have the least Hamming weight compared with the ones in the same coset and hence will be able to act as the coset leader. By theorem 1 and lemma 1 we have

Corollary 1 *Let $\alpha \in \mathcal{F}_n$ and $W_H(\alpha) = 2^{n-2}$. Then $N_\alpha = W_H(\alpha)$.*

Lemma 2 *Let $l_1, l_2, ..., l_k \in \mathcal{L}_n$. If $l_1, ..., l_k, 1$ are linearly independent, i.e., any linear combination $c_1 l_1 \oplus c_2 l_2 \oplus \cdots \oplus c_k l_k \oplus c_{k+1} = 0$ with $c_i \in \{0, 1\}$ will lead to a result $c_1 = c_2 = \cdots = c_{k+1} = 0$. Then we have $W_H(\prod_{i=1}^{k} l_i) = 2^{n-k}$.*

Proof: It is known that $x_1, ..., x_n, 1$ form a basis of $\mathcal{L}_n$. Since $l_1, ..., l_k, 1$ are linearly independent, we can add $n - k$ functions $x_{i_1}, ..., x_{i_{n-k}}$ of $\{x_1, ..., x_n\}$ to form a basis of $\mathcal{L}_n$. The functions x_1, ..., x_n which can be treated as the variables or input of a Boolean function in $\mathcal{F}_n$ should be independent and with uniform probability distribution over $\{0, 1\}$, so $x_{i_1}, ..., x_{i_{n-k}}$ will randomly take values in $\{0, 1\}$ when every l_i is fixed with value 1. This implies that there are 2^{n-k} chances for $\prod_{i=1}^{k} l_i$ to take value 1, and the conclusion of lemma 2 then follows. □

Lemma 3 *Let $W_H(\alpha) = 2^{n-2}$. If there is a nonzero affine function $l \in \mathcal{L}_n$ such that $W_H(\alpha \oplus l) = W_H(\alpha)$, then we have $l \neq 1$ and consequently $W_H(l) = 2^{n-1}$.*

Proof: Assume that $l = 1$. Then by $W_H(\alpha \oplus 1) = 2^n - W_H(\alpha)$ we have $W_H(\alpha) = 2^{n-1}$. This violates the initial condition. □

Lemma 4 *Let $W_H(\alpha) = 2^{n-2}$. Then the sufficient and necessary condition for the existence of an affine function $l \in \mathcal{L}_n$ such that $W_H(\alpha \oplus l) = W_H(\alpha)$ is that $\alpha \cdot l = \alpha$.*

Proof: Suppose $W_H(\alpha \oplus l) = W_H(\alpha)$. Since $W_H(\alpha \oplus l) = W_H(\alpha) + W_H(l) - 2W_H(\alpha \cdot l)$, so by lemma 3 we have $W_H(\alpha \oplus l) = W_H(\alpha) \Longleftrightarrow W_H(\alpha \cdot l) = \frac{1}{2}W_H(l) = 2^{n-2} = W_H(\alpha) \Longleftrightarrow \alpha \cdot l = \alpha$. □

Lemma 5 *Let $W_H(\alpha) = 2^{n-2}$. Then there exist no affine functions $l_1, l_2, l_3 \in \mathcal{L}_n$ such that they together with 1 are linearly independent and satisfy the following equations:*

$$W_H(\alpha) = W_H(\alpha \oplus l_1) = W_H(\alpha \oplus l_2) = W_H(\alpha \oplus l_3)$$

Proof: Assume the contrary. Then by lemma 4 we have

$$\alpha = \alpha \cdot l_1 = \alpha \cdot l_2 = \alpha \cdot l_3$$

Moreover, by repeated use of lemma 4 we have $\alpha = \alpha \cdot l_1 \cdot l_2 \cdot l_3$. But by lemma 2 we have

$$W_H(\alpha) = W_H(\alpha \cdot l_1 \cdot l_2 \cdot l_3) \leq W_H(l_1 \cdot l_2 \cdot l_3) = 2^{n-3}.$$

This leads to a contradiction, and hence the conclusion of lemma 5 is true. □

By the discussion above we know that, there may be more than one function having the same minimum Hamming weight in the same coset where there is a vector with Hamming weight 2^{n-2}. The forthcoming discussion will be treated by the following three cases, and in each case α is a Boolean function having Hamming weight 2^{n-2}.

4.1 More than two functions with the same minimum Hamming weight in the same coset

Lemma 6 *Suppose we have $W_H(\alpha) = 2^{n-2}$. Then the sufficient and necessary condition for the existence of affine functions $l_1, l_2 \in \mathcal{L}_n$ such that $l_1 \oplus l_2$ is not a constant and satisfying $W_H(\alpha) = W_H(\alpha \oplus l_1) = W_H(\alpha \oplus l_2)$ is that $\alpha = l_1 \cdot l_2$.*

Proof: Let $W_H(\alpha) = W_H(\alpha \oplus l_1) = W_H(\alpha \oplus l_2)$. Then by lemma 4 we have $\alpha = \alpha \cdot l_1 \cdot l_2$. But by lemma 2, $W_H(\alpha) = W_H(\alpha \cdot l_1 \cdot l_2) = W_H(l_1 \cdot l_2) = 2^{n-2}$, so we have $\alpha = l_1 \cdot l_2$. Contrarily, if $\alpha = l_1 \cdot l_2$. Since $\alpha \oplus l_1 = l_1 \cdot (l_2 \oplus 1)$, $\alpha \oplus l_2 = l_2 \cdot (l_1 \oplus 1)$. By lemma 2 we have $W_H(\alpha) = W_H(\alpha \oplus l_1) = W_H(\alpha \oplus l_2) = 2^{n-2}$. □

Lemma 7 *Let $W_H(\alpha) = 2^{n-2}$. If there exist affine functions $l_1, l_2 \in \mathcal{L}_n$ such that $\alpha = l_1 \cdot l_2$, then there are exactly 4 functions in the same coset having the minimum Hamming weight, they are α, $\alpha \oplus l_1$, $\alpha \oplus l_2$ and $\alpha \oplus l_1 \oplus l_2 \oplus 1$.*

Proof: It is easy to see that both l_1 and l_2 are not constant. By lemma 2 we know that functions $\alpha \oplus l_1 = l_1 \cdot (l_2 \oplus 1)$, $\alpha \oplus l_2 = l_2 \cdot (l_1 \oplus 1)$ and $\alpha \oplus l_1 \oplus l_2 \oplus 1 = (l_1 \oplus 1) \cdot (l_2 \oplus 1)$ all have Hamming weight 2^{n-2} which is the minimum Hamming weight of functions in this coset. By lemma 5 we know that they are all the functions available with such Hamming weight. □

Lemma 8 *Let $l_1, l_2 \in \mathcal{L}_n$ such that $l_1 \oplus l_2$ is not a constant. Then $f = l_1 \cdot l_2$ is a function of degree 2, and there are three distinct forms for writing f as the product of two distinct affine functions, they are*

$$f = l_1 \cdot l_2 = l_1 \cdot (l_1 \oplus l_2 \oplus 1) = l_2 \cdot (l_1 \oplus l_2 \oplus 1)$$

Proof: See appendix. □

Corollary 2 *Let $l_1, l_2, l_3, l_4 \in \mathcal{L}_n$ such that $l_1 \oplus l_2$ is not a constant and $l_1 \cdot l_2 = l_3 \cdot l_4$. Then both sides of the above equation must have a same affine function.*

Proof: Directly from lemma 8. □

Lemma 9 *Let l_1 and l_2 be two distinct linear functions. If there exist linear functions $l_3, l_4 \in \mathcal{L}_n$ such that $l_1 \cdot l_2 = l_3 \cdot l_4$. Then we must have $l_1 = l_3$ and $l_2 = l_4$, or $l_1 = l_4$ and $l_2 = l_3$.*

Proof: From lemma 8 we know that only $l_1 \cdot l_2$ is the product of two linear functions, i.e., this expression is unique. □

It is known that there are totally $2^n - 1$ nonzero linear functions in $\mathcal{L}_n$. By lemma 9 we know that the number of functions of degree 2 which are the product of two linear functions is $\begin{pmatrix} 2^n - 1 \\ 2 \end{pmatrix}$.

Lemma 10 *Let $l_1 \in \mathcal{L}_n$ be a linear function, $l_2 \in \mathcal{L}_n$ be a nonsingular affine function, and $l_1 \oplus l_2 \neq 1$. Then there must exist a linear function $l_3 \in \mathcal{L}_n$ such that $l_1 \cdot l_2 = l_1 \cdot l_3$.*

Proof: The conclusion follows by setting $l_3 = l_1 \oplus l_2 \oplus 1$. □

Lemma 11 *Let $l_1, l_2 \in \mathcal{L}_n$ be two different nonsingular affine functions. Then their product is a function of degree 2 which can be written in three distinct forms: $l_1 \cdot l_2$, $l_1 \cdot (l_1 \oplus l_2 \oplus 1)$, and $l_2 \cdot (l_1 \oplus l_2 \oplus 1)$.*

Proof: Directly from lemma 8. □

Lemma 10 implies that the product of a linear function and a nonsingular affine function can be equivalently expressed by the product of two nonsingular affine functions, and lemma 11 implies that the number of products of two different nonsingular affine functions is $\begin{pmatrix} 2^n - 1 \\ 2 \end{pmatrix}/3$. To sum up the discussion above we have

Theorem 4 *The number of functions of degree 2 in $\mathcal{F}_n$ which can be written as the product of two different affine functions in $\mathcal{L}_n$ is*

$$\binom{2^n-1}{2}+\binom{2^n-1}{2}/3=\frac{4}{3}\binom{2^n-1}{2} \tag{3}$$

and they are distributed in $\frac{1}{3}\binom{2^n-1}{2}$ cosets.

4.2 Only two functions with the same minimum Hamming weight in the same coset

In this case there should be an affine function $l \in \mathcal{L}_n$ such that $W_H(\alpha \oplus l) = W_H(\alpha.)$ By lemma 4 we have $\alpha = \alpha \cdot l$. This implies that whenever $\alpha(x) = 1$, we must have $l(x) = 1$. Note that there are $\binom{2^{n-1}}{2^{n-2}}$ such functions for a fixed l because $W_H(l) = 2^{n-1}$ and $W_H(\alpha) = 2^{n-2}$, discarding the functions in the form $l \cdot l'$, where l' is another affine function, the desired functions (they have the minimum Hamming weight and any one of their cosets has only two such functions) will remain.

Lemma 12 *For a fixed non-constant affine function $l \in \mathcal{L}_n$, the number of functions of degree 2 which can be written as $l \cdot l'$ is $2^n - 2$, where $l' \in \mathcal{L}_n$ is another affine function.*

Proof: Any function in this form can be expressed in two ways: $l \cdot l'$ and $l \cdot (1 \oplus l' \oplus l)$. Since the multiplicative function is of degree two, the set where l' can be chosen from is $\mathcal{L}_n - \{0, 1, l, 1 \oplus l\}$. So the number of possible l', or equivalently the number of functions in the form $l \cdot l'$ is $(2^{n+1} - 4)/2 = 2^n - 2$. □

Now we are considering functions α such that there is only one nonzero affine function l such that $\alpha \oplus l$ and α are in the same coset and $W_H(\alpha \oplus l) = W_H(\alpha)$. Then by lemma 12 it is known that the number of such functions is

$$\binom{2^{n-1}}{2^{n-2}} - (2^n - 2) = \binom{2^{n-1}}{2^{n-2}} - 2^n + 2$$

Since l can be an arbitrary non-constant affine function of $\mathcal{L}_n$, the number of such cosets where there are exactly two functions with minimum Hamming weight 2^{n-2} in each coset is

$$(2^{n+1} - 2)[\binom{2^{n-1}}{2^{n-2}} - 2^n + 2]/2 \tag{4}$$

4.3 Only one function can be the coset leader

As a coset leader, since α can be any function with Hamming weight 2^{n-2}, the total number of valid such functions then is $\binom{2^n}{2^{n-2}}$. By theorem 3 and equation (4) we

know that, among these functions there are $\frac{4}{3}\binom{2^n-1}{2}$ are of the form $l \cdot l'$ and there are $(2^{n+1}-2)\left[\binom{2^{n-1}}{2^{n-2}} - 2^n + 2\right]$ functions in the cosets which have two valid coset leaders. What remains are the functions which are the only valid coset leaders of their coset, and the number of such functions is

$$\binom{2^n}{2^{n-2}} - (2^{n+1}-2)\left[\binom{2^{n-1}}{2^{n-2}} - 2^n + 2\right] - \frac{4}{3}\binom{2^n-1}{2} \tag{5}$$

Sum up the discussion above, the number of cosets in equation (1) which contain a coset leader of Hamming weight 2^{n-2} is

$$\begin{aligned}
&\binom{2^n}{2^{n-2}} - (2^{n+1}-2)\left[\binom{2^{n-1}}{2^{n-2}} - 2^n + 2\right] - \frac{4}{3}\binom{2^n-1}{2} \\
&\quad +(2^n-1)\left[\binom{2^{n-1}}{2^{n-2}} - 2^n + 2\right] + \frac{1}{3}\binom{2^n-1}{2} \\
&= \binom{2^n}{2^{n-2}} - (2^n-1)\binom{2^{n-1}}{2^{n-2}} + \binom{2^n-1}{2}
\end{aligned} \tag{6}$$

Since there are 2^{n+1} functions in each coset, by theorem 1 we have

Theorem 5

$$\sigma_n(2^{n-2}) = 2^{n+1}\left[\binom{2^n}{2^{n-2}} - (2^n-1)\binom{2^{n-1}}{2^{n-2}} + \binom{2^n-1}{2}\right] \tag{7}$$

5 Conclusion

We have studied in this paper the problem of the distribution of Boolean functions in $\mathcal{F}_n$ with nonlinearity no larger than 2^{n-2}. This result is the first step towards finding the distribution of nonlinearities of Boolean functions, or equivalently the weight distribution of first order Reed-Muller codes. It seems much more difficult for the case when the nonlinearity is larger than 2^{n-2} since there will be a great variety in the number of coset leaders. This problem is harder and more challenging.

References

[1] W.Diffie and M.E.Hellman, Privacy and authentication : an introduction of cryptography, *Proc. IEEE,* 1979, 67(3): 397-427.

[2] C.Ding, G.Xiao, and W.Shan, *The Stability Theory of Stream Ciphers,* Springer-Verlag, 1991.

[3] M.G.Karpovsky, *Finite Orthogonal Series in the Design of Digital Devices,* John Wiely & Sons, New York, 1976.

[4] C.Mitchell, Enumerating boolean functions of cryptographic significance, *J. of Cryptology,* 1990, 2(3):155- 170.

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

Appendix: Proof of lemma 8

In order to prove lemma 8, we have to introduce the concept of Walsh-Hadamard transformation.

Let $f(x) \in \mathcal{F}_n$, then

$$S_f(\omega) = \sum_x f(x)(-1)^{\omega \cdot x}$$

is called the *Walsh-Hadamard transformation* or briefly W-H transformation of $f(x)$ which is a real valued function, where $\omega \cdot x = \omega_1 x_1 \oplus \cdots \oplus \omega_n x_n$ is the *inner product* of ω and x. Accordingly, the inverse transformation can be expressed as

$$f(x) = 2^{-n} \sum_\omega S_f(\omega)(-1)^{\omega \cdot x}$$

With this concept the proof of lemma 8 is derived as follows. Let $l_1(x) = \alpha \cdot x \oplus a$, $l_2(x) = \beta \cdot x \oplus b$ be two affine functions and neither is a constant and so does $l_1 \oplus l_2$, where $\alpha, \beta \in GF^n(2)$, $a, b \in GF(2)$. Let $f(x) = l_1(x) \cdot l_2(x)$. Then we have

$$S_f(\omega) = \sum_x f(x)(-1)^{\omega \cdot x} = \sum_{l_1 \cdot l_2 = 1} (-1)^{\omega \cdot x}$$

The following discussions will be considered:

(1) Let ω=0. Then by lemma 2 we have $S_f(0) = W_H(l_1 \cdot l_2) = 2^{n-2}$.

(2) Let $\omega = \alpha$. Then we have $\omega \cdot x = 1 \oplus a$ whenever $l_1(x) = 1$. So

$$S_f(\omega) = \sum_{l_1 \cdot l_2 = 1} (-1)^{1 \oplus a} W_H(l_1 \cdot l_2) = (-1)^{1 \oplus a} \cdot 2^{n-2}.$$

(3) Let $\omega = \beta$. By the same way as in case (2) we have $S_f(\omega) = (-1)^{1 \oplus b} \cdot 2^{n-2}$.

(4) Let $\omega = \alpha \oplus \beta$. Then we have $\omega \cdot x = a \oplus b$ whenever $l_1(x) \cdot l_2(x) = 1$. So

$$S_f(\omega) = \sum_{l_1 \cdot l_2 = 1} (-1)^{a \oplus b} = (-1)^{a \oplus b} \cdot 2^{n-2}.$$

(5) Let $\omega \notin \{0, \alpha, \beta, \alpha \oplus \beta\}$. It is easy to check in this case that $\omega \cdot x$, $l_1(x)$, $l_2(x)$ and 1 are linearly independent. By lemma 2 we have $W_H(l_1 \cdot l_2 \cdot (\omega \cdot x)) = 2^{n-3}$. But

$W_H(l_1 \cdot l_2) = 2^{n-2}$. This means that in the set $\{x \in GF^n(2) : l_1(x) \cdot l_2(x) = 1\}$, the number of x satisfying $\omega \cdot x = 1$ is equal to the number of x satisfying $\omega \cdot x = 0$. Therefore we have

$$S_f(\omega) = \begin{cases} 2^{n-2} & if\ \omega = 0 \\ (-1)^{1 \oplus a} \cdot 2^{n-2} & if\ \omega = \alpha \\ (-1)^{1 \oplus b} \cdot 2^{n-2} & if\ \omega = \beta \\ (-1)^{a \oplus b} \cdot 2^{n-2} & if\ \omega = \alpha \oplus \beta \\ 0 & otherwise \end{cases} \tag{8}$$

Suppose that there exist affine functions $l_3(x) = \lambda \cdot x \oplus s$ and $l_4(x) = \mu \cdot x \oplus t$ such that $f(x) = l_3(x) \cdot l_4(x)$, where λ, $\mu \in GF^n(2)$ and s, $t \in GF(2)$. Similar to the procedure above we have

$$S_f(\omega) = \begin{cases} 2^{n-2} & if\ \omega = 0 \\ (-1)^{1 \oplus s} \cdot 2^{n-2} & if\ \omega = \lambda \\ (-1)^{1 \oplus t} \cdot 2^{n-2} & if\ \omega = \mu \\ (-1)^{s \oplus t} \cdot 2^{n-2} & if\ \omega = \lambda \oplus \mu \\ 0 & otherwise \end{cases} \tag{9}$$

Since there is a one-to-one relationship between $f(x)$ and its W-H transformation, equation (8) and equation (9) must be an identity, i.e., $\{0, \alpha, \beta, \alpha \oplus \beta\} = \{0, \lambda, \mu, \lambda \oplus \mu\}$, and we have simultaneously

- If $\lambda = \alpha$, then $s = a$ and hence $l_3(x) = l_1(x)$. In this case we must have $\mu = \beta$ or $\mu = \alpha \oplus \beta$, i.e., $l_4(x) = l_2$ or $l_4(x) = l_1(x) \oplus l_2(x) \oplus 1$.
- If $\mu = \alpha$, then $t = a$ and hence $l_4(x) = l_1(x)$. In this case we must have $\lambda = \beta$ or $\lambda = \alpha \oplus \beta$, i.e., $l_3(x) = l_2$ or $l_3(x) = l_1(x) \oplus l_2(x) \oplus 1$.
- If $\lambda = \beta$, then $s = b$ and hence $l_3(x) = l_2(x)$. In this case we must have $\mu = \alpha$ or $\mu = \alpha \oplus \beta$, i.c., $l_4(x) = l_1$ or $l_4(x) = l_1(x) \oplus l_2(x) \oplus 1$.
- If $\mu = \beta$, then $t = b$ and hence $l_4(x) = l_2(x)$. In this case we must have $\lambda = \alpha$ or $\lambda = \alpha \oplus \beta$, i.e., $l_3(x) = l_1$ or $l_3(x) = l_1(x) \oplus l_2(x) \oplus 1$.

To sum up the discussion above, the conclusion of lemma 8 then follows.

(Received 10/7/96)