On The Linear Structure of Symmetric Boolean Functions*

Ed Dawson and Chuan-Kun Wu

Information Security Research Centre,
Queensland University of Technology,
GPO Box 2434, Brisbane 4001, Australia.
{dawson, wu}@fit.qut.edu.au

Abstract

It is shown in this paper that nonlinear symmetric Boolean functions have no linear structures other than the all-zero and the all-one vectors. For such functions with n variables, it is shown that when n is odd, every such symmetric Boolean function is either a function with the all-one vector as an invariant linear structure or can be written as the product of two symmetric functions of which one has the all-one vector as an invariant linear structure and the other has the all-one vector as a complementary linear structure. In the case when n is even, it is shown that only $2^{\frac{n}{2}+1}$ of the symmetric Boolean functions have the all-one vector as an invariant linear structure and none has the all-one vector as a complementary linear structure.

1 Introduction

Symmetric Boolean functions are a class of Boolean functions with some interesting properties. The usefulness of symmetric functions in many cryptographic applications as well as other applications is still far from being clear. For example a potential application of these functions could be as the combining function for self-synchronizing stream ciphers when part of the input bits are used for seed key while the other bits are used for function alteration (see [1], [4]). Some research has been done in relation to the cryptographic properties of symmetric Boolean functions (see [2] [3] [5]). The linear structure feature of Boolean functions is an important criterion to measure the weakness of these functions in their cryptographic applications. In this paper the linear structures of symmetric Boolean functions are studied in detail.

Let $F_2 = \{0, 1\}$ be the binary field. A function $f : F_2^n \longrightarrow F_2$ is called a Boolean function of n variables. It is written as $f(x) = f(x_1, x_2, ..., x_n)$. A binary

*The content of this paper was presented at the CMSA conference in July 1996 in Sydney

vector of length 2^n generated by $f(x)$ is called the *truth table* of $f(x)$. The *Hamming weight* of $f(x)$, denoted by $W_H(f)$, is the number of ones in its truth table. The function $f(x)$ is called an *affine* function if there exist $a_0, a_1, ..., a_n \in \{0,1\}$ such that $f(x) = a_0 \oplus a_1x_1 \oplus \cdots \oplus a_nx_n$, where $\oplus$ means modulo 2 addition. If $a_0 = 0$, $f(x)$ is also called a *linear* function. We will denote by $\mathcal{F}_n$ the set of all Boolean functions of n variables and $\mathcal{L}_n$ the set of affine ones. By tradition we will call a function nonlinear if it is not in $\mathcal{L}_n$.

Let $f(x) \in \mathcal{F}_n$. Then $f(x)$ is called a symmetric function if for any permutation σ on $\{1, 2, ..., n\}$, we have

$$f(x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)}) = f(x_1, x_2, ..., x_n).$$

Clearly for any symmetric Boolean function $f(x)$, there is an integer function $I_f : \{0, 1, ..., n\} \longrightarrow \{0, 1\}$ such that

$$f(x) = I_f(k) \text{ if and only if } W_H(x) = k.$$

Let $\varphi_i(x)$, $i = 0, 1, ..., n$, be the symmetric function which is composed by all the terms of degree i, where $\varphi_0(x) = 1$. Let $\lambda_j(x)$, $j = 0, 1, ..., n$, be the symmetric function satisfying $\lambda_j(x) = 1$ if and only if $W_H(x) = j$. Then we have

Lemma 1 *The set of symmetric functions in $\mathcal{F}_n$ forms an $(n+1)$-dimensional vector space over F_2 where both $\{\varphi_i(x)\}_{i=0}^n$ and $\{\lambda_i(x)\}_{i=0}^n$ are bases.*

Furthermore, since the product of two symmetric functions is also a symmetric function, $\mathcal{S}_n$ is virtually a ring with an identity. For a symmetric function $f(x) \in \mathcal{F}_n$, it can be shown that

$$f(x) = \bigoplus_{k=0}^{n} I_f(k)\lambda_k(x). \tag{1}$$

We would like to note that $\lambda_i(x)\lambda_j(x) \equiv 0$ if and only if $i \neq j$.

2 Walsh transforms

Let $f(x) \in \mathcal{F}_n$. Then the Walsh transform of $f(x)$ is expressed as

$$S_f(\omega) = \sum_x f(x)(-1)^{\omega \cdot x}, \tag{2}$$

where $\omega \cdot x = \omega_1x_1 \oplus \cdots \oplus \omega_nx_n$ is the inner product of ω and x. The inverse transform is expressed as

$$f(x) = 2^{-n} \sum_\omega S_f(\omega)(-1)^{\omega \cdot x}. \tag{3}$$

Note that the summation in (2) as well as in (3) is over the real number field. Hence, the Walsh transform of a Boolean function is a real-valued function with the domain of definition still being on F_2^n. It should be noted that the value of $\omega \cdot x$ can be treated as a real value in the operations.

By (2) and (3) it is obvious that

Lemma 2 *Let $f(x) \in \mathcal{F}_n$ with its Walsh transform $S_f(\omega)$. Then $f(x)$ is a symmetric Boolean function if and only if $S_f(\omega)$ is a symmetric real-valued function.*

3 Linear structures

Let $f(x) \in \mathcal{F}_n$. A vector $\alpha \in F_2^n$ is called a *linear structure* of $f(x)$ if $f(x \oplus \alpha) \oplus f(x) \equiv c$, where $c \in \{0, 1\}$. More precisely, α is called an *invariant linear structure* if $c = 0$ and a *complementary linear structure* if $c = 1$. The following lemma can easily be proved.

Lemma 3 *Let V be the set of invariant linear structures of $f(x)$. Then V forms a vector subspace of F_2^n. The set of all the linear structures of $f(x)$ is also a subspace V', of F_2^n containing V. The dimension of V' is dim(V)+1 if and only if $f(x)$ has a complementary linear structure.*

Denote by $\mathbf{0}$ and $\mathbf{1}$ the all-zero vector and the all-one vector of F_2^n respectively. We have

Lemma 4 *Let $f(x) \in \mathcal{F}_n$, $\alpha \in F_2^n - \{\mathbf{0}, \mathbf{1}\}$. Then $f(x \oplus \alpha)$ is a symmetric Boolean function if and only if $f(x) \in \mathcal{L}_n$.*

Proof: Sufficiency is obvious. So we need only to present a proof of the necessity. Assume $f(x) \in \mathcal{F}_n - \mathcal{L}_n$ and denote by $g(x) = f(x \oplus \alpha)$. Then we have

$$\begin{aligned} S_g(\omega) &= \textstyle\sum_x g(x)(-1)^{\omega \cdot x} \\ &= \textstyle\sum_x f(x \oplus \alpha)(-1)^{\omega \cdot x} \\ &= \textstyle\sum_x f(x)(-1)^{\omega \cdot x + \omega \cdot \alpha} \\ &= (-1)^{\omega \cdot \alpha} S_f(\omega). \end{aligned}$$

Since $f(x)$ is symmetric, without loss of generality we can assume that α is a vector with k $(0 < k < n)$ consecutive ones followed by $n - k$ consecutive zeros. By the assumption $f(x) \notin \mathcal{L}_n$ we know that there must exist an $\omega \in F_2^n - \{\mathbf{0}, \mathbf{1}\}$ such that $S_f(\omega) \neq 0$. By the same way we can assume that ω is a vector with t $(0 < t < n)$ consecutive ones followed by $n - t$ consecutive zeros. Let ω' be obtained from ω by exchanging the first and the last bits. Since $W_H(\omega') = W_H(\omega)$, by lemma 2 we know that $S_f(\omega') = S_f(\omega)$. By the restriction of both α and ω it is seen that $(-1)^{\omega' \cdot \alpha} + (-1)^{\omega \cdot \alpha} = 0$, i.e., $S_g(\omega') = -S_g(\omega) \neq S_g(\omega)$. Once again by lemma 2 we know that $g(x)$ is not symmetric. □

It is known that $\mathbf{0}$ is a trivial linear structure for any Boolean function. By lemma 4 we have

Theorem 1 *Let $f(x) \in \mathcal{F}_n$ be a symmetric Boolean function. Then*

- *$f(x)$ is constant if and only if every vector in F_2^n is an invariant linear structure of $f(x)$;*

- *$f(x) \in \mathcal{L}_n$ is not a constant if and only if every vector in F_2^n with even Hamming weight is an invariant linear structure and every vector in F_2^n with odd Hamming weight is a complementary linear structure;*

- *$f(x)$ is nonlinear if and only if it has no other linear structures except for the all-zero and the all-one vectors.*

Proof: The first two cases are trivial and we only need to prove the case when $f(x)$ is a nonlinear symmetric Boolean function. For any vector α other than $\mathbf{0}$ and $\mathbf{1}$, by lemma 4 we know that $f(x \oplus \alpha)$ is not symmetric and consequently $f(x \oplus \alpha) \oplus f(x)$ is not either. This means that $f(x \oplus \alpha) \oplus f(x)$ cannot be a constant and then α is not a linear structure of $f(x)$. □

Theorem 1 says that only the all-one vector can possibly be a linear structure of a nonlinear symmetric Boolean function. We now consider this case further. Denote by $I_f^{-1}(1) = \{k : I_f(k) = 1\}$. Then we have

Theorem 2 *Let $f(x) \in \mathcal{F}_n$ be a symmetric Boolean function corresponding to the integer function $I_f(t)$. Then $\mathbf{1}$ is an invariant linear structure of $f(x)$ if and only if $f(x)$ is such that $r \in I_f^{-1}(1)$ implies that $n - r \in I_f^{-1}(1)$.*

Proof: For any x, $W_H(x \oplus \mathbf{1}) = n - W_H(x)$. So $f(x \oplus \mathbf{1}) = f(x) \Longleftrightarrow \{x, x \oplus \mathbf{1}\} \subset f^{-1}(1)$ or $\{x, x \oplus \mathbf{1}\} \subset f^{-1}(0) \Longleftrightarrow \{W_H(x), n - W_H(x)\} \subset I_f^{-1}(1)$ or $\{W_H(x), n - W_H(x)\} \subset I_f^{-1}(0) \Longleftrightarrow r \in I_f^{-1}(1)$ implies that $n - r \in I_f^{-1}(1)$. □

By theorem 2 it can be easily derived that the number of symmetric functions with $\mathbf{1}$ as an invariant linear structure is

$$\sum_{i=0}^{\lceil \frac{n+1}{2} \rceil} \binom{\lceil \frac{n+1}{2} \rceil}{i} = 2^{\lceil \frac{n+1}{2} \rceil},$$

where $\lceil a \rceil$ is meant the smallest integer $\geq a$. Likewise we have

Theorem 3 *Let $f(x) \in \mathcal{F}_n$ be a symmetric Boolean function corresponding to the integer function $I_f(t)$. Then $\mathbf{1}$ is a complementary linear structure of $f(x)$ if and only if n is odd and for any integer r, only one of $\{r, n - r\}$ is contained in $I_f^{-1}(1)$.*

Proof: If n is even, for any x with $W_H(x) = \frac{n}{2}$, since $W_H(x \oplus \mathbf{1}) = \frac{n}{2}$, we must have $f(x \oplus \mathbf{1}) = f(x)$. So $f(x \oplus \mathbf{1}) \equiv f(x) \oplus 1$ is impossible for even n. The proof of the rest of the theorem is similar to that of theorem 2. □

Therefore we have from theorem 3 that the number of symmetric functions with $\mathbf{1}$ as a complementary linear structure is

$$\sum_{i=0}^{\frac{n+1}{2}} \binom{\frac{n+1}{2}}{i} = 2^{\frac{n+1}{2}}.$$

Lemma 5 *Denote by* $A = \{f(x) : f(x \oplus \mathbf{1}) = f(x)\}$, $B = \{f(x) : f(x \oplus \mathbf{1}) = f(x) \oplus 1\}$. *Then for any* $g(x) \in B$,

$$\gamma : f(x) \xrightarrow{\gamma} f(x) \oplus g(x)$$

is a one-to-one mapping from A *to* B.

Proof: Easily verified. □

By lemma 5 we know that the two classes of functions with $\mathbf{1}$ as a variant-permanently linear structure are closely related. It is interesting to notice that

Lemma 6 *As defined in lemma 5, the set* A *forms a vector space over* F_2 *of dimension* $\lceil \frac{n+1}{2} \rceil$. *Moreover, for any symmetric function* $g(x) \in B$ *and for any symmetric function function* $f(x) \in A$, $f(x) \cdot g(x) \equiv 0$ *if and only if* $f(x) \equiv 0$.

Proof: By theorem 3 and its deduction the former part can be verified easily. The proof of the later part is as follows: Let $F(x) = f(x)g(x)$. Then $F(x \oplus \mathbf{1}) = f(x \oplus \mathbf{1}) \cdot g(x \oplus \mathbf{1}) = f(x)(g(x) \oplus 1) = F(x) \oplus f(x)$. So, $F(x) \equiv 0$ if and only if $F(x \oplus \mathbf{1}) \equiv 0$ if and only if $f(x) \equiv 0$. □

Theorem 4 *Let* n *be an odd integer. Then for any symmetric function* $f(x) \in \mathcal{F}_n$, *we have either* $f(x) \in A$ *or* $f(x)$ *can be written as* $f(x) = f_1(x)f_2(x)$ *with* $f_1(x) \in A$ *and* $f_2(x) \in B$.

Proof: By lemma 6, the product of one nonzero function from A and one (nonzero) function from B results in $(2^{\frac{n+1}{2}} - 1) \cdot 2^{\frac{n+1}{2}} = 2^{n+1} - 2^{\frac{n+1}{2}}$ different symmetric functions. These different symmetric functions, and the ones in A, cover exactly all the symmetric functions of n variables (refer to lemma 1). Consequently, the conclusion follows. □

References

[1] J.Daemen, R.Govaerts, and J.Vandewalle, On the design of high speed self-synchronizing stream ciphers, *Proceedings of ISCC/ISITA'92,* Singapore 1992, 279-283.

[2] K.Gopalakrishnan, D.G.Hoffman, and D.R.Stinson, A note on a conjecture concerning symmetric resilient functions, *Information Processing Letters*, 47 (1993), 139-143.

[3] N.Jefferies, Sporadic Partitions of Binomial Coefficients, *Electronics Letters,* Vol.27, No.15, 1991, 1334-1336.

[4] U.M.Maurer, New approaches to the design of self-synchronizing stream ciphers, *Proceedings of Eurocrypt'91,* Springer 1991, 458-471.

[5] C.Mitchell, Enumerating Boolean functions of cryptographic significance, *Journal of Cryptology,* No.2, 1990, 155-170.

(Received 20/11/96)