Turkish Journal of Mathematics

Volume 36 | Number 4 Article 2

1-1-2012

Weight and nonlinearity of Boolean functions

LAVINIA CORINA CIUNGU

Turk J Math
36 (2012) , 520 – 529.

doi:10.3906/mat-1104-21

Weight and nonlinearity of Boolean functions

Lavinia Corina Ciungu

Abstract

In this paper we analyze the weight and the nonlinearity of various types of Boolean functions. We give some general results related to rotation symmetric Boolean functions, and in particular, we prove partially a conjecture stated by Cusick and Stănică in [3].

Key Words: Hamming weight, nonlinearity, balanced functions, affine equivalence, rotation symmetric

1. Introduction

Boolean functions have many applications in coding theory and cryptography. A detailed account of the latter applications can be found in the book [2]. If we define V_n to be the vector space of dimension n over the finite field $GF(2) = \{0, 1\}$, then an n variable Boolean function $f(x_1, x_2, ..., x_n) = f(x)$ is a map from V_n to $GF(2)$. Every Boolean function $f(x)$ has a unique polynomial representation (usually called the algebraic normal form [2, p. 6]), and the degree of f is the degree of this polynomial. A function of degree ≤ 1 is said to be *affine*, and if the constant term is 0 such a function is called *linear*. We let B_n denote the set of all Boolean functions in n variables, with addition and multiplication done modulo 2. If we list the 2^n elements of V_n as $v_0 = (0, ..., 0), v_1 = (0, ..., 0, 1), ...$ in lexicographic order, then the 2^n-vector $(f(v_0), f(v_1), ..., f(v_{2^n-1}))$ is called the *truth table* of f. The *weight* (also called *Hamming weight*) $wt(f)$ of f is defined to be the number of $1'$s in the truth table for f. In many cryptographic uses of Boolean functions, it is important that the truth table of each function f has an equal number of $0'$s and $1'$s; in that case, we say that the function f is *balanced*. The distance $d(f, g)$ between 2 Boolean functions f and g is defined by $d(f, g) = wt(f + g)$, where the polynomial addition is done modulo 2. An important concept in cryptography is the *nonlinearity* $N(f)$ defined by $N(f) = \min_{a \text{ affine}} wt(f + a)$. We say a Boolean function $f(x)$ in B_n is *rotation symmetric* if the algebraic normal form of the function is unchanged by any cyclic permutation of the variables $x_1, x_2, ..., x_n$. In recent years, rotation symmetric functions have proven to be very useful in several areas of cryptography [2, pp. 108–118]. This has led to many papers that study different aspects of the theory of rotation symmetric functions. We say that 2 Boolean functions $f(x)$ and $g(x)$ in B_n are *affine equivalent* (we shall use the notation $f \equiv g$) if $g(x) = f(Ax + b)$, where A is an n by n nonsingular matrix over the finite field $GF(2)$ and b is an n-vector over $GF(2)$. We say $f(Ax+b)$ is a *nonsingular affine transformation* of $f(x)$. It is easy to see that if f

2000 *AMS Mathematics Subject Classification:* 11F37, 11B50, 11B83.

and g are affine equivalent, then $wt(f) = wt(g)$ and $N(f) = N(g)$. We say that the weight and nonlinearity are *affine invariants*. In this paper we study various properties of the weight and nonlinearity of Boolean functions. Some of our results concern rotation symmetric Boolean functions, and in particular we prove some cases of a more general version of a conjecture of Cusick and Stănică [3, Conjecture 12, p. 300].

2. General algebraic properties of weight and nonlinearity

We will first recall the notion of "direct sum" for Boolean functions (notation $\oplus$) which is well known in the literature (see, for example, [1, p. 2880]).

Let $f = f(x_1, x_2, \ldots, x_n)$ and $g = g(x_1, x_2, \ldots, x_k)$ be 2 Boolean functions of n and respectively k variables. Denote by $f \oplus g$ the function

$$(f \oplus g)(x_1, \ldots, x_{n+k}) = f(x_1, \ldots, x_n) + g(x_{n+1}, \ldots, x_{n+k})$$

(this means that $f \oplus g$ is obtained from the tables of f and g by a kind of "expansion"). It is immediate from the definition that if f' and g' are other 2 such functions; then $(f + f') \oplus (g + g') = (f \oplus g) + (f' \oplus g')$.

Definition 2.1 *For $f = f(x_1, \ldots, x_n)$ of 2^n bits, we introduce the following notations:*
(a) $\overline{wt}(f) = \frac{1}{2^n} \cdot wt(f)$ *(the "relative" or "weighted" weight),*
(b) $\overline{N}(f) = \frac{1}{2^n} N(f)$,
(c) $w_0(f) = 1 - 2 \cdot \overline{wt}(f)$,
(d) $N_0(f) = 1 - 2 \cdot \overline{N}(f)$.

Note that then $\overline{N}(f) = \min\limits_{L \text{ affine}} \{\overline{wt}(f + L)\}$ and

$$\begin{aligned} N_0(f) &= 1 - \frac{1}{2} \min_{L \text{ affine}} \{\overline{wt}(f + L)\} = \max_{L \text{ affine}} \{1 - \frac{1}{2}\overline{wt}(f + L)\} \\ &= \max_{L \text{ affine}} \{w_0(f + L)\}. \end{aligned}$$

We also note that $wt(f) \in [0, 1] \cap \mathbb{Q}$ for all f and also $w_0(f) \in [-1, 1] \cap \mathbb{Q}$ for all f.

Lemma 2.2 *For any 2 functions f and g we have:*

$$\overline{wt}(f \oplus g) = \frac{1}{2} - \frac{1}{2}(1 - 2\overline{wt}(f))(1 - 2\overline{wt}(g)),$$

and

$$w_0(f \oplus g) = w_0(f) w_0(g).$$

Proof. For the first equation in the lemma, we use the identity: $wt(f\oplus g) = 2^k wt(f)+2^n wt(g)-2wt(f)wt(g)$ (well known in the literature; see, for example [1]). Dividing by 2^{n+k} we get

$$\begin{aligned}\overline{wt}(f\oplus g) &= \frac{wt(f)}{2^n}\cdot\frac{2^k-wt(g)}{2^k}+\frac{2^n-wt(f)}{2^n}\cdot\frac{wt(g)}{2^k}\\ &= \overline{wt}(f)(1-\overline{wt}(g))+\overline{wt}(g)(1-\overline{wt}(f))\\ &= \overline{wt}(f)+\overline{wt}(g)-2\overline{wt}(f)\cdot\overline{wt}(g)\\ &= \frac{1}{2}-\frac{1}{2}(1-2\overline{wt}(f))(1-2\overline{wt}(g)).\end{aligned}$$

To prove the second equation in the lemma, we observe that the work above implies

$$\begin{aligned}w_0(f\oplus g) &= 1-2\overline{wt}(f\oplus g) = 1-2(\frac{1}{2}-\frac{1}{2}(1-2\overline{wt}(f))(1-2\overline{wt}(g)))\\ &= 1-1+w_0(f)w_0(g) = w_0(f)w_0(g).\end{aligned}$$

□

In the same manner as above, we can prove the following result.

Lemma 2.3 *With the above notations we have*

$$N_0(f\oplus g) = N_0(f)N_0(g),$$

$$\overline{N}(f\oplus g) = \overline{N}(f)+\overline{N}(g)-2\overline{N}(f)\overline{N}(g),$$

and

$$N(f\oplus g) = 2^k N(f)+2^n N(g)-2N(f)N(g).$$

We note that the final assertion in Lemma 2.3 shows that an inequality proved by Seberry, Zhang, and Zheng in [6, Lemma 18, p. 196] in fact always holds with equality. This sharpens some results in that paper.

Thus, when one is interested in the weight and nonlinearity of a function, it is enough to consider the numbers $w_0(f)$ and $N_0(f)$ and work with these, since they have better algebraic properties.

From the above results, we obtain the following theorem, which is also well known in the literature (see, for example, [1]).

Theorem 2.4 *If $f_1,\dots,f_n$ are such that $N(f_i) = wt(f_i)$ then $N(f_1\oplus\cdots\oplus f_n) = wt(f_1\oplus\cdots\oplus f_n)$.*

3. Classes of Boolean functions with equal weight and nonlinearity

Theorem 3.1 *Let $f_k = x_1x_2\dots x_{s_k}$ for $k = 1,2,\dots,n$ and let $s_k\geq 2, s_0 = 0$.*
Let $S_{(s_1,s_2,\dots,s_N)} = f_1\oplus f_2\oplus\cdots\oplus f_n = \sum_{k=0}^{n-1} x_{s_1+\cdots+s_k+1}x_{s_1+\cdots+s_k+2}\dots x_{s_1+\cdots+s_k+s_{k+1}}$. Then $N(S_{(S_1,\dots,S_N)}) = wt(S_{(S_1,\dots,S_N)})$.

Proof. Obviously, $wt(f_k) = 1$, since the only value of 1 for this function is obtained for $x_1 = \cdots = x_{s_k} = 1$. Also, it is easy to see that f_k is not affine since it is neither balanced nor equal to 0 or 1 because $s_k\geq 2$ (a

linear function must necessarily have 1 of these 3 properties). Therefore, $wt(f_k + L) \geq 1$ for all L, L affine, $\#\{f_k = 1\} = wt(f_k + 0) = 1$, so

$$N(f_k) = \min_L\{wt(f_k + L)\} = 1.$$

Hence, $wt(f_k) = N(f_k)$ for all k. Using Theorem 2.4, we get the conclusion. □

This is a generalization of the fact that $wt(S_N) = N(S_N)$ and also of [4, Lemma 7]. Indeed, define $S_N = x_1x_{N+1}x_{2N+1} + x_2x_{N+2}x_{2N+2} + \cdots + x_Nx_{2N}x_{3N}$. It is obvious that $S_N = \underbrace{f \oplus f \oplus \cdots \oplus f}_{N}$, where $f = x_1x_2x_3$. Then the above theorem shows that

Corollary 3.2 *The function S_N has equal weight and nonlinearity.*

Corollary 3.3 *For functions $f_1, f_2, \ldots, f_n$ (of lengths in bits $2^{k_1}, 2^{k_2}, \ldots, 2^{k_n}$) we have*

$$\overline{wt}(f_1 \oplus f_2 \oplus \cdots \oplus f_n) = \frac{1}{2} - \frac{1}{2}\prod_{k=1}^{n}(1 - 2\overline{wt}(f_k)).$$

The following result on quadratic functions will be needed later (as in the Introduction, we use the notation $f \equiv g$ to mean that the Boolean functions f and g are affine equivalent). There are too many papers on quadratic Boolean functions to list here (see the book [2] for detailed references). The important reference here is the paper of Kim et al. [4]; we give simpler proofs and generalizations of several results in that paper. For example, Theorem 3.1 above extends [4, Lemma 7] from the degree 2 case to any degree > 2.

Theorem 3.4 *For a permutation σ of $\{1, 2, \ldots, n\}$, define $f_\sigma = \sum_{i=1}^{n} x_ix_{\sigma(i)}$. Assume the decomposition of σ into disjoint cycles is $\sigma = \tau_1\tau_2 \ldots \tau_t$, where each τ_i is a k_i-cycle (i.e. a cycle of length k_i.) Then*

$$f_\sigma \equiv f_{k_1,2} \oplus f_{k_2,2} \oplus \ldots \oplus f_{k_t,2} \oplus \sum_{i \geq k_1+\ldots+k_t+1} x_i.$$

Proof. Let τ_i be $(a_{i1}, a_{i2}, \ldots, a_{i,k_i})$, that is, $\tau_i(a_{i1}) = a_{i2}, \tau_i(a_{i2}) = a_{i3}, \ldots, \tau_i(a_{i,k_{i-1}}) = a_{i,k_i}, \tau_i(a_{i,k_i}) = a_{i1}$ and $\tau_i(j) = j$ for all $j \notin \{a_{i1}, \ldots, a_{i,k_i}\}$. Let $A_i = \{a_{i1}, a_{i2}, \ldots, a_{i,k_i}\}$, and let $F = \{i : \sigma(i) = i\}$. Then

$$f_\sigma = \sum_{i=1}^{n} x_ix_{\sigma(i)} = \sum_{i=1}^{t}\sum_{j\in A_i} x_jx_{\sigma(j)} + \sum_{j\in F} x_jx_{\sigma(j)} = \sum_{i=1}^{t}\sum_{j\in A_i} x_ix_{\sigma_i(j)} + \sum_{i\in F} x_ix_i$$

$$= \sum_{i=1}^{k}(x_{a_{i1}}x_{a_{i2}} + x_{a_{i2}}x_{a_{i3}} + \ldots + x_{a_{i,k_i-1}}x_{a_{i,k_i}} + x_{a_{i,k_i}}x_{a_{i1}}) + \sum_{i\in F} x_i$$

After a suitable change of variables, namely the permutation of the variables given by

$$x_{a_{11}} \leftrightarrow x_1; x_{a_{12}} \leftrightarrow x_2; \ldots; x_{a_{1,k_1}} \leftrightarrow x_{k_1};$$

$$x_{a_{21}} \leftrightarrow x_{k_1+1}; \ldots; x_{a_{2,k_2}} \leftrightarrow x_{k_1+k_2}; \ldots\ldots\ldots;$$

$$x_{a_{t,1}} \leftrightarrow x_{k_1+\ldots+k_{t-1}+1}; \ldots; x_{a_{t,k_t}} \leftrightarrow x_{k_1+\ldots+k_{t-1}+k_t},$$

with the rest of the variables that correspond to indices in F being changed to the variables $x_{k_1+\ldots+k_t+1}, \ldots, x_n$, we obtain

$$\begin{aligned} f_\sigma &\equiv \sum_{i=1}^{t} f_{k_i,2}(x_{k_1+\ldots+k_{i-1}+1}, \ldots, x_{k_1+\ldots+k_i}) + \sum_{i \geq k_1+\ldots+k_t+1} x_i \\ &\equiv f_{k_1,2} \oplus f_{k_2,2} \oplus \ldots \oplus f_{k_t,2} \oplus \sum_{i \geq k_1+\ldots+k_t+1} x_i \end{aligned}$$

□

We next show that, using the result above, we can exactly compute the weight and nonlinearity of $S_{(s_1,s_2,\ldots,s_N)}$ from Theorem 3.1. We obtain

Theorem 3.5 *With the notations of Theorem 3.1, we have*

$$wt(S_{(s_1,s_2,\ldots,s_N)}) = N(S_{(s_1,s_2,\ldots,s_N)}) = 2^{s_1+s_2+\ldots s_N-1}(1 - \prod_{k=1}^{N}\left(1 - \frac{1}{2^{s_k-1}}\right)).$$

Proof. Again, let $f_k = x_1x_2\ldots x_{s_k}$ whose weight is $wt(f_k) = 1$. Therefore, $\overline{wt}(f_k) = \frac{1}{2^{s_k}}$ and $w_0(f_k) = 1 - \frac{1}{2^{s_k-1}}$. Thus by Theorems 3.1 and 3.4, $w_0(S_{(s_1,s_2,\ldots,s_N)}) = N_0(S_{(s_1,s_2,\ldots,s_N)}) = \prod_{k=1}^{N} w_0(f_k) = \prod_{k=1}^{N}\left(1 - \frac{1}{2^{s_k-1}}\right)$. Since $wt(S_{(s_1,s_2,\ldots,s_N)}) = 2^{s_1+s_2+\cdots+s_N} \cdot \frac{1}{2}(1 - w_0(S_{(s_1,s_2,\ldots,s_N)}))$, using also Theorem 3.1, the conclusion follows. □

Theorems 3.1 and 3.4 generalize [4, Theorem 8] on homogeneous quadratic functions. We also get the following result on homogeneous cubic functions.

Corollary 3.6 $wt(S_N) = N(S_N) = 2^{3N-1}(1 - \left(\frac{3}{4}\right)^N) = \frac{1}{2}(8^N - 6^N)$ *where* $S_N = x_1x_{N+1}x_{2N+1} + x_2x_{N+2}x_{2N+2} + \cdots + x_Nx_{2N}x_{3N}$ *as before.*

Definition 3.7 *For a function f of 2^n bits (n variables) and a function g of 2^k bits (k variables), define* $(f \odot g)(x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n+k}) = f(x_1, \ldots, x_n)g(x_{n+1}, \ldots, x_{n+k})$.

Lemma 3.8 *For f of n variables, we have*

$$N(x_1 \odot f) = \min\{wt(f), wt(f+1)\}.$$

Proof. For affine functions $L = a_1x_1 + a_2x_2 + \cdots + a_{n+1}x_{n+1} + a_0$, we have
$wt(x_1 \odot f + L) = wt(x_1(f(x_2, \ldots, x_{n+1}) + a_1) + l)$, where $l = a_2x_2 + \cdots + a_{n+1}x_{n+1} + a_0$.
To compute the weight, we note that

$$\begin{aligned} \{x_1 \odot (f + a_1) + l = 1\} &= \{x_1 = 0\} \cap \{x_1 \odot (f + a_1) + l = 1\} \sqcup \{x_1 = 1\} \cap \{x_1 \odot (f + a_1) + l = 1\} \\ &= \{0\} \oplus \{l = 1\} \sqcup \{1\} \oplus \{(f + a_1) + l = 1\}, \end{aligned}$$

where by $A \sqcup B$ we mean a disjoint union. So

$$wt\{x_1 \odot (f + a_1) + l \ = \ 1\} = \begin{cases} \#\{f + a_1 = 1\} = wt(f + a_1) & \text{when } l = 0 \\ 2^n + wt(f + a_1 + 1) & \text{when } l = 1 \\ 2^{n-1} + wt(f + a_1 + l) & \text{otherwise.} \end{cases} \tag{3}$$

These alternatives come from the fact that when l is affine, then we have

$$\#\{l = 1\} = wt(l) = \begin{cases} 0 & \text{if } l = 0 \\ 1 & \text{if } l = 1 \\ 2^{n-1} & \text{otherwise (in this case, the affine function } l \text{ is balanced).} \end{cases}$$

We are interested in the minimum of all possible values in equation (3). So

$$N(x_1 \odot f) = \min_{a_1 \in \{0,1\}; l \text{ affine of } 2^n \text{ bits}} \{wt(f + a_1); 2^n + wt(f + a_1 + 1); 2^{n-1} + wt(f + l)\}.$$

But $\min\{wt(f + 0), wt(f + 1)\} \leq 2^{n-1}$ and therefore,

$$\min\{wt(f), wt(f + 1)\} \leq \min\{2^n + wt(f + a_1 + 1); 2^{n-1} + wt(f + l)\}$$

for any $a_1 \in \{0, 1\}, l$ affine of 2^n bits. Thus $N(x_1 \odot f) = \min\{wt(f), wt(f + 1)\}$. □

Lemma 3.9 *The following hold:*
(1) $wt(f \odot g) = wt(f) \cdot wt(g)$.
(2) *Given* $f(x_2, \ldots, x_{n+1})$ *and* $g(x_2, \ldots, x_{k+1})$, *we have*

$$wt(x_1 \odot f \oplus g) = 2^{n+1} wt(g) + 2^k wt(f) - 2wt(f)wt(g).$$

(3) *Given* $f(x_2, \ldots, x_{n+1})$ *and* $g(x_2, \ldots, x_{k+1})$, *we have*

$$wt(x_1 \odot f + g) = wt(g) + wt(f + g).$$

Also,

$$wt(\overline{x_1} \odot f + g) = wt(g) + wt(f + g),$$

where $\overline{x_1} = x_1 + 1$.

Proof. (1) Obviously, $f(x_1, \ldots, x_n)g(x_{n+1}, \ldots, x_{n+k}) = 1$ is equivalent to $f(x_1, \ldots, x_n) = 1$ and $g(x_{n+1}, \ldots, x_{n+k}) = 1$ so

$$|\{(x_1, \ldots, x_{n+k}) | (f \odot g)(x_1, \ldots, x_{n+k}) = 1\}| =$$
$$|\{(x_1, \ldots, x_n) | f(x_1, \ldots, x_n) = 1\}| \cdot |\{(x_{n+1}, \ldots, x_{n+k}) | g(x_{n+1}, \ldots, x_{n+k}) = 1\}|.$$

This implies the conclusion.

(2) We have

$$\begin{aligned} wt(x_1 \odot f \oplus g) &= 2^{n+1}wt(g) + 2^k wt(x_1 \odot f) - 2wt(x_1 \odot f)wt(g) \\ &= 2^{n+1}wt(g) + 2^k wt(x_1)wt(f) - 2wt(x_1)wt(f)wt(g), \end{aligned}$$

and therefore $wt(x_1 \odot f \oplus g) = 2^{n+1}wt(g) + 2^k wt(f) - 2wt(f)wt(g)$.

(3) We have

$$\begin{aligned} wt(x_1 \odot f + g) &= \#\{(x_1 \odot f + g) = 1\} = \#(\{x_1 \odot f + g = 1\} \wedge \{x_1 = 0\}) \\ &+ \#(\{x_1 \odot f + g = 1\} \wedge \{x_1 = 1\}) = \#\{g = 1\}) + \#\{f + g = 1\}) \\ &= wt(g) + wt(f + g). \end{aligned}$$

The proof of the second statement is similar. □

Example 3.10 *Consider $f = x_1x_2 + x_3, g = x_3$ as functions of 3 variables.*
We have $wt(f) = wt(g) = 4$, so $wt(f + 1) = 4$ and $wt(g + 1) = 4$.
From the above theorems we have:
$wt(x_1 \odot f) = wt(x_1) \cdot wt(f) = 1 \cdot 4 = 4$
$wt(x_1 \odot g) = wt(x_1) \cdot wt(g) = 1 \cdot 4 = 4$
$N(x_1 \odot f) = \min\{wt(f), wt(f + 1)\} = \min\{4, 4\} = 4$
$N(x_1 \odot g) = \min\{wt(g), wt(g + 1)\} = \min\{4, 4\} = 4$
Thus, we have that the functions $x_1 \odot f = x_1(x_2x_3 + x_4) = x_1x_2x_3 + x_1x_4$ and $x_1 \odot g = x_1x_4$ have the same weight and the same nonlinearity. However, they cannot be affine equivalent, because the degree is an affine invariant.

Nevertheless, we have the following theorem.

Theorem 3.11 *Two functions of degree 2 are affine equivalent if and only if they have the same weight and the same nonlinearity.*

Proof. According to Theorem 4 in [4] (as stated there, this is an old result due to Dickson), every function of degree 2 and n bits is affine equivalent to one of the following:
- $x_1x_2 + x_3x_4 + \cdots + x_{2k-1}x_{2k} + x_{2k+1}$
- $x_1x_2 + x_3x_4 + \cdots + x_{2k-1}x_{2k}$
- $x_1x_2 + x_3x_4 + \cdots + x_{2k-1}x_{2k} + 1$

Note that $wt(x_1x_2) = 1$, $N(x_1x_2) = 1$, $wt(x_1) = 1$, $N(x_{2k+1}) = 0 = N(0) = N(1)$. Thus, $w_0(x_1x_2) = 1 - 2 \cdot \frac{1}{2^2}wt(x_1x_2) = \frac{1}{2}$ and similarly $N_0(x_1x_2) = \frac{1}{2}$, $w_0(x_{2k+1}) = 0$, $w_0(0) = w_0(1) = -1$; $N_0(x_{2k+1}) = 1 = N_0(0) = N_0(1)$. Now, using Theorems 3.4, 2.4, and Lemma 2.3 we have the following table showing the possible values for the invariants w_0 and N_0 of a function of degree 2 and n variables:

f	w_0	N_0
$x_1x_2 + x_3x_4 + \cdots + x_{2k-1}x_{2k} + x_{2k+1}$	0	$\frac{1}{2^k}$
$x_1x_2 + x_3x_4 + \cdots + x_{2k-1}x_{2k}$	$\frac{1}{2^k}$	$\frac{1}{2^k}$
$x_1x_2 + x_3x_4 + \cdots + x_{2k-1}x_{2k} + 1$	$-\frac{1}{2^k}$	$\frac{1}{2^k}$.

(This follows, for example, by applying Theorems 3.4, 2.4, and Lemma 2.3 for
$x_1x_2 + x_3x_4 + \cdots + x_{2k-1}x_{2k} + x_{2k+1} = \underbrace{(x_1x_2) \oplus \cdots \oplus (x_1x_2)}_{k} \oplus x_1$.) □

This table shows that if $N(f) = N(g)$ and $wt(f) = wt(g)$, equivalently, $N_0(f) = N_0(g)$ and $w_0(f) = w_0(g)$, then f and g must be affine equivalent. Indeed, the nonlinearity will fix the integer k, while the weight will show to which of the 3 above categories a function f of degree 2 belongs.

Lemma 3.12 (1) *Let f be a function of n variables such that the functions of $n-1$ variables $f_1 = f(0, x_2, \ldots, x_n)$ and $f_2 = f(1, x_2, \ldots, x_n)$ have their respective weights equal to their nonlinearities, i.e. $wt(f_1) = N(f_1)$ and $wt(f_2) = N(f_2)$. Then $wt(f) = N(f)$.*
(2) *More generally, if f is a function of n variables such that for any $(a_1, a_2, \ldots, a_k) \in \mathbb{F}_2^k$, we have*

$$wt(f(a_1, a_2, \ldots, a_k, x_{k+1}, \ldots, x_n)) = N(f(a_1, \ldots, a_k, x_{k+1}, \ldots, x_{n+1})).$$

Then $wt(f) = N(f)$.

Proof. (1) Suppose $f = f(x_1, \ldots, x_n)$ and let $l = a_1x_1 + \ldots + a_nx_n + a_0$ denote an affine function. Note that showing that $wt(f) = N(f)$ means showing that the minimum

$$\min_l wt(f + l) = \min_{a_0, \ldots, a_n \in \mathbb{F}_2} wt(f(x_1, \ldots, x_n) + a_1x_1 + \ldots + a_nx_n + a_0)$$

is attained for $l = 0$, i.e. $a_1 = a_2 = \ldots = a_n = a_0 = 0$.

We have

$$\begin{aligned}
&wt(f(x_1, \ldots, x_n) + a_1x_1 + \ldots + a_nx_n + a_0) \\
&\quad = wt(f(0, x_2, \ldots, x_n) + a_2x_2 + \ldots + a_nx_n + a_0) \\
&\qquad + wt(f(1, x_2, \ldots, x_n) + a_2x_2 + \ldots + a_nx_n + a_1 + a_0) \\
&\quad \geq wt(f(0, x_2, \ldots, x_n)) + wt(f(1, x_2, \ldots, x_n)) \\
&\quad = wt(f(x_1, \ldots, x_n)).
\end{aligned}$$

Thus $wt(f + l) \geq wt(f)$ for all $l = a_1x_1 + \ldots + a_nx_n + a_0$, which means, as noticed above, that $wt(f) = N(f)$.

(2) It follows from (1) by induction.

□

We can now state and prove one of our main results, which confirms the case $n = 3p$ of a conjecture of Cusick and Stănică [3, p. 300]:

Theorem 3.13 *If $n = 3p$ is a multiple of 3, then the function*

$$f_{n,3} = x_1x_2x_3 + x_2x_3x_4 + \ldots + x_{n-2}x_{n-1}x_n + x_{n-1}x_nx_1 + x_nx_1x_2$$

has $wt(f_{n,3}) = N(f_{N,3})$.

Proof. We examine the functions of $n-n/3=2p$ variables obtained from $f_{n,3}$ by replacing $x_3, x_6, x_9, \ldots, x_{3p}$ by 0 and 1 (there are 2^p such functions) so we use $x_3=a_1, x_6=a_2, \ldots, x_{3p}=a_p,\ a_1, a_2, \ldots, a_p \in \{0,1\}$. We have several cases:

• if all $a_i's$ are 1, then we get the function:

$$x_1x_2+x_2x_4+x_4x_5+x_4x_5+x_5x_7+x_7x_8+x_7x_8+\ldots$$
$$\ldots+x_{n-2}x_{n-1}+x_{n-1}x_1+x_1x_2=$$
$$=x_2x_4+x_5x_7+x_8x_{10}+\ldots+x_{3k-1}x_{3k+1}+\ldots+x_{3p-1}x_1. \quad (4)$$

• If one of them is 0 and the rest are 1, by the cyclic symmetry we can assume $a_1=a_2=\ldots=a_{p-1}=1; a_p=0$ and we get the function

$$x_1x_2+x_2x_4+x_4x_5+x_4x_5+x_5x_7+x_7x_8+x_7x_8+x_8x_{10}+x_{10}x_{11}+\ldots$$
$$\ldots+x_{3p-5}x_{3p-4}+x_{3p-4}x_{3p-2}+x_{3p-2}x_{3p-1}=$$
$$=x_1x_2+x_2x_4+x_{3p-4}x_{3p-2}+x_{3p-2}x_{3p-1}. \quad (5)$$

This situation can only occur when $p\geq 2$ $(n\geq 6)$; when $p=2$ we have the function $x_1x_2+x_2x_4$, and when $p\geq 3$ we get the function in equation 5.

• In all the other cases, we have at least 2 different $0's$, so we have sequences of the form 0 1 1 ... 1 0, separated by strings of 0, in the sequence $a_1, a_2, \ldots, a_p$. We shall use indices modulo n for $x_1, x_2, \ldots, x_n$. In such a sequence, for example, if $x_n=0, x_3=1, x_6=1, \ldots, x_{3k}=1, x_{3k+3}=0$ we obtain, for the part of the function $f_{n,3}$ containing the variables $x_{n-2}, x_{n-1}, x_n, x_1, x_2, \ldots, x_{3k}, x_{3k+1}, x_{3k+2}, x_{3k+3}$, the function

$$x_1x_2+x_2x_4+x_4x_5+x_4x_5+x_5x_7+x_7x_8+x_7x_8+x_8x_{10}+\ldots$$
$$\ldots+x_{3k-2}x_{3k-1}+x_{3k-1}x_{3k+1}+x_{3k+1}x_{3k+2}=$$
$$=x_1x_2+x_2x_4+x_5x_7+\ldots+x_{3k-1}x_{3k+1}+x_{3k+1}x_{3k+2} \quad (6)$$

if the sequence of $1's$ has at least 2 $1's$, so in this example $k\geq 3$. Otherwise, if the sequence is 0 1 0 (for the consecutive values of the $a_i's$) we get the function

$$x_1x_2+x_2x_4+x_4x_5. \quad (7)$$

By the change of variables $x_1 \leftarrow x_1+x_4$, this is affine equivalent to

$$x_1x_2+x_4x_5. \quad (8)$$

The above 3 cases show that, if we evaluate $a_1, a_2, \ldots, a_p$ arbitrarily and divide the (cyclic, i.e. $a_{p+1}=a_1$) sequence $a_1, a_2, \ldots, a_p$ into subsequences of the type 0 1 1 ... 1 0, we obtain, for each such sequence, an expression of the type $(4)-(8)$ in $f_{n,3}$, but the variables of all these expressions do not overlap, so we get a function of the type

$$g_1 \oplus g_2 \oplus \ldots \oplus g_n$$

with $g_1, g_2, \ldots, g_n$ of the types $(4)-(8)$. Furthermore, the functions from $(4)-(8)$ are affine equivalent to or can be split into a function of the form

$$h_1 \oplus h_2 \oplus \ldots \oplus h_s$$

where h_i is either x_1x_2 or $x_1x_2+x_2x_3$ (the "names" of the variables here are "generic"). But $x_1x_2+x_2x_3 \equiv x_1x_2$ by the change of variables $x_1 \leftarrow x_1 + x_3$, so we have shown in fact that any evaluation of the variables $x_3, x_6, \ldots, x_{3p} = x_n$ at 0 and 1 yields a function of the $2p$ variables $x_2, x_4, x_5, x_7, \ldots, x_{3k-1}, x_{3k+1}, \ldots, x_{3p-1}$ which is affine equivalent to a function

$$f_1 \oplus f_2 \oplus \ldots \oplus f_t$$

where $f_1 = f_2 = \ldots = f_t = x_1x_2$.
Since $wt(x_1 \cdot x_2) = N(x_1 \cdot x_2)$, by Theorem 2.4 it follows that $wt(f_1 \oplus f_2 \oplus \ldots \oplus f_t) = N(f_1 \oplus f_2 \oplus \ldots f_t)$ where $f_1 = f_2 = \ldots = f_t = x_1x_2$.
We can now use Lemma 3.12 (2): since for any replacement of the variables $x_3, x_6, \ldots, x_n = x_{3p}$ with 0 and 1, we obtain a function of $2p$ variables which has its weight equal to its nonlinearity, it follows that $wt(f_{n,3}) = N(f_{n,3})$. □

References

[1] Carlet, C., Dobbertin, H., Leander, G: Normal extensions of bent functions. IEEE Transactions on Information Theory 50, 2880-2885 (2004).

[2] Cusick T.W., Stănică, P.: Cryptographic Boolean Functions and Applications. San Diego. Academic Press 2009.

[3] Cusick, T.W., Stănică, P.: Fast evaluation, weights and nonlinearity of rotation symmetric functions. Discrete Mathematics 258, 289-301 (2002).

[4] Kim, H., Park S-M., Hahn, S.G.: On the weight and nonlinearity of homogeneous rotation symmetric Boolean functions of degree 2. Discrete Applied Mathematics 157, 428-432 (2009).

[5] Pieprzyk, J.P., Qu, C.X.: Fast hashing and rotation-symmetric functions. J. Universal Computer Science 5, 20-31 (1999).

[6] Seberry, J., Zhang, X-M., Xheng, Y.: On constructions and nonlinearity of correlation immune functions. Eurocrypt, 1993.

Lavinia Corina CIUNGU
University of Central Oklahoma,
100 N University Drive, Edmond, OK 73013, USA
e-mail: lciungu@uco.edu

Received: 18.04.2011