Necessary Conditions on Balanced Boolean Functions with Maximum Nonlinearity

Faruk Göloğlu[1] and Melek D. Yücel[2]

[1] Dept. of Computer Technology and Information Systems,
Bilkent University
also Institute of Applied Mathematics,
Middle East Technical University
`gologlu@bilkent.edu.tr`

[2] Institute of Applied Mathematics and
Dept. of Electrical and Electronics Engineering
Middle East Technical University
`yucel@eee.metu.edu.tr`

1. At first glance

- Problem: What is the upper bound on the nonlinearity of balanced Boolean functions with $n = 2k$ variables? Specifically, is $2^{n-1} - 2^{\frac{n}{2}-1} - 2$ a sharp bound for $n \geq 8$?
- Tools:
  - Numerical Normal Form (NNF) by Carlet and Guillot [1].
  - Möbius inversion in $\mathbb{F}_2^n$ viewed as a partially ordered set (Rota, [3]).
- Purposes:
  - Find a relation between *algebraic degree* and the *Walsh spectrum*.
  - Try to find necessary conditions for balanced Boolean functions with maximal nonlinearity.

2. Preliminaries

- A *Boolean function* is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$.
- (Hamming) *Weight* of a Boolean function f:

$$\mathrm{wt}(f) = \sum_{a \in \mathbb{F}_2^n} f(a)$$

- f is *balanced* if $\mathrm{wt}(f) = 2^{n-1}$.
- The *discrete Fourier transform* of f:

$$F_f(a) = \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{a \cdot x}$$

- Let $\hat{f} = (-1)^f$, then the *Walsh transform* W_f is defined to be the discrete Fourier transform of $\hat{f}$:

$$F_{\hat{f}}(a) = W_f(a) = \sum_{x \in \mathbb{F}_2^n} \hat{f}(x)(-1)^{a \cdot x} = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus a \cdot x}$$

– Relation between $F_f(a)$ and $W_f(a)$ is given as:

$$W_f(a) = 2^n\delta_0(a) - 2F_f(a)$$

where $\delta_0(a) = 1$ if $a = \mathbf{0}$ and 0 otherwise.

– *Nonlinearity* of f:

$$nl(f) = 2^{n-1} - \frac{1}{2}\mathsf{max}_{a\in\mathbb{F}_2^n}\left\{\left|W_f(a)\right|\right\}$$

– Restrictions on the Walsh spectrum:

- Parseval's equality:

$$\sum_{x\in\mathbb{F}_2^n} W_f^2(x) = 2^{2n}$$

- An immediate fact:

Proposition 1.

* $W_f(a) \equiv 0 \pmod 4,\ \forall a \in \mathbb{F}_2^n$ *if* $\mathrm{wt}(f)$ *is even,*
* $W_f(a) \equiv 2 \pmod 4,\ \forall a \in \mathbb{F}_2^n$ *if* $\mathrm{wt}(f)$ *is odd.*

- A *multiset* is a set where repetition of an element is allowed.
- *Algebraic normal form (ANF)* of f:

$$f(x_1,\ldots,x_n) = \bigoplus_{u \in \mathbb{F}_2^n} a_u \left(\prod_{i=1}^{n} x_i^{u_i} \right), \ a_u \in \mathbb{F}_2 \tag{1}$$

- The *algebraic degree* of f: degree of (1).
- A *partially ordered set* P is a set of elements with an order relation $\succeq$ and an equality $=$, such that the following axioms hold:

P1: $x \succeq x$ for all $x \in P$ (reflexive).

P2: if $x \succeq y$ and $y \succeq z$ then $x \succeq z$ for all $x, y, z \in P$ (transitive).

P3: if $x \succeq y$ and $y \succeq x$ then $x = y$ for all $x, y \in P$ (antisymmetric).

3. Numerical Normal Form [Carlet and Guillot]

NNF is an integer valued polynomial representation of Boolean functions.

- Coefficients:

$$\lambda_u = (-1)^{\mathrm{wt}(u)} \sum_{a \in \mathbb{F}_2^n \,|\, a \preceq u} (-1)^{\mathrm{wt}(a)} f(a)$$

- Recovery of DFT:

$$F_f(a) = (-1)^{\mathrm{wt}(a)} \sum_{u \in \mathbb{F}_2^n \,|\, a \preceq u} 2^{n-\mathrm{wt}(u)} \lambda_u \tag{2}$$

- An immediate consequence of a theorem of Carlet and Guillot [2]:

  Corollary 1. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a balanced Boolean function with even $n \geq 6$. If $nl(f) = 2^{n-1} - 2^{\frac{n}{2}-1} - 2$ then degree d of f is $n-1$.*

4. A necessary condition on the Walsh spectrum

The following result not only generalizes Proposition 1, but also relates algebraic degree to the Walsh spectrum of the function.

Theorem 1. *Let* $f : \mathbb{F}_2^n \to \mathbb{F}_2$ *be a Boolean function with* $n \geq 3$ *and NNF coefficients* λ_u, $u \in \mathbb{F}_2^n$. *Then:*

- *If* $d = n - 1$, *then:*
  - $W_f(u) \equiv 0 \pmod 8$ *for all* $u \in I$,
  - $W_f(u) \equiv 4 \pmod 8$ *for all* $u \in J$,
- *If* $d < n - 1$, *then* $W_f(u) \equiv k \pmod 8$ *for all* $u \in \mathbb{F}_2^n$, *with* $k = 4$ *or* $k = 0$, *depending on* $\lambda_{\mathbf{1}}$.
- *If* $d = n$, *let* r *be the terms in ANF with degree* $d - 1$.
  - *if* $r = n$, *then* $W_f(u) \equiv k \pmod 8$ *for all* $u \in \mathbb{F}_2^n$, *with* $k = 6$ *or* $k = 2$, *depending on* $\lambda_{\mathbf{1}}$,
  - *otherwise*
    - $W_f(u) \equiv 2 \pmod 8$ *for all* $u \in I$,
    - $W_f(u) \equiv 6 \pmod 8$ *for all* $u \in J$,

for two index sets $I, J \subseteq \mathbb{F}_2^n$, *with* $I \cap J = \emptyset$, $I \cup J = \mathbb{F}_2^n$ *and* $|I| = |J| = 2^{n-1}$.

5. Weight Spectrum

- The *subspace weight* of f for all $u \in \mathbb{F}_2^n$:

$$s_u = \sum_{a \preceq u} f(a) \qquad (3)$$

- s_u is simply the weight of $f|_E$, the restriction of f to the subspace E, where $E = \{v \in \mathbb{F}_2^n \,|\, v \preceq u\}$
- We can view $\mathbb{F}_2^n$ as a locally finite partially ordered set with a greatest lower bound; hence we can employ Möbius inversion. By Möbius inversion and (3):

$$f(u) = (-1)^{\mathrm{wt}(u)} \sum_{a \in \mathbb{F}_2^n \,|\, a \preceq u} (-1)^{\mathrm{wt}(a)} s_a$$

- The discrete Fourier transform of f can be defined in terms of subspace weights. In the sequel, $\bar{a}$ denotes the complement of a.

Proposition 2. *Let f be a Boolean function and s_u be the subspace weight coefficients of f for all $u \in \mathbb{F}_2^n$. Then:*

$$F_f(a) = (-1)^{\mathrm{wt}(\bar{a})} \sum_{u \in \mathbb{F}_2^n \,|\, \bar{a} \preceq u} (-1)^{\mathrm{wt}(u)} 2^{n-\mathrm{wt}(u)} s_u$$

Proof is in the manner of Carlet and Guillot.

The following theorem gives a restriction on the weight structure of the hyperplanes of a balanced Boolean function having maximum nonlinearity.

Theorem 2. *Let n be even and $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a balanced Boolean function. f has nonlinearity $nl(f) = 2^{n-1} - 2^{\frac{n}{2}-1} - 2$, only if*

(a) $2^{n-2} - 2^{\frac{n}{2}-2} - 1 \leq s_u \leq 2^{n-2} + 2^{\frac{n}{2}-2} + 1$ *if* $\mathrm{wt}(u) = n-1$, *and*

(b) $2^{n-3} - 2^{\frac{n}{2}-2} - 2^{\frac{n}{2}-3} - 1 \leq s_u \leq 2^{n-3} + 2^{\frac{n}{2}-2} + 2^{\frac{n}{2}-3} + 1$ *if* $\mathrm{wt}(u) = n-2$

6. A sketch of Proof of Theorem 1

- Complete proof can be found in the paper.
  We will just prove $d = n - 1$ case.
- We will make use of the following:

Lemma 1. *Let* $A = \{* z_1, \ldots, z_n *\}$, $z_i \in \mathbb{Z}$ *be a multiset. Let the subset sum* S_X *be defined on the subsets* $X \subseteq A$ *as:*

$$S_X = \begin{cases} 0 & \text{if } X = \emptyset, \\ \sum_{x \in X} x & \text{otherwise.} \end{cases}$$

Then

$$|\{X \subseteq A \,|\, S_X \text{ is even}\}| = \begin{cases} 2^{n-1} & \text{if } \exists z_i \in A \text{ s.t. } z_i \text{ is odd}, \\ 2^n & \text{otherwise.} \end{cases}$$

Proof (of Theorem 1). Let $\Lambda_w = \{* \lambda_i \mid \mathrm{wt}(i) = w *\}$ be the multi-set of NNF coefficients with weight w of f. In the following formula, let $X_{w,a} \subseteq \Lambda_w$ for $0 \leq w < n$, and $S_{X_{w,a}}$ be the subset sum of the subset corresponding to a. By (2) the discrete Fourier transform of f at a can be written as:

$$F_f(a) = (-1)^{\mathrm{wt}(a)} \left[\lambda_{1\dots1} + 2S_{X_{n-1,a}} + 2^2 S_{X_{n-2,a}} + \cdots + 2^n S_{X_{0,a}}\right]$$

where for any $a \in \mathbb{F}_2^n, X_{w,a} \subseteq \Lambda_w$ for $0 \leq w < n$ is completely determined by:

$$X_{w,a} = \{\lambda_i \mid \mathrm{wt}(i) = w \ and \ i \succeq a\}$$

Recall that

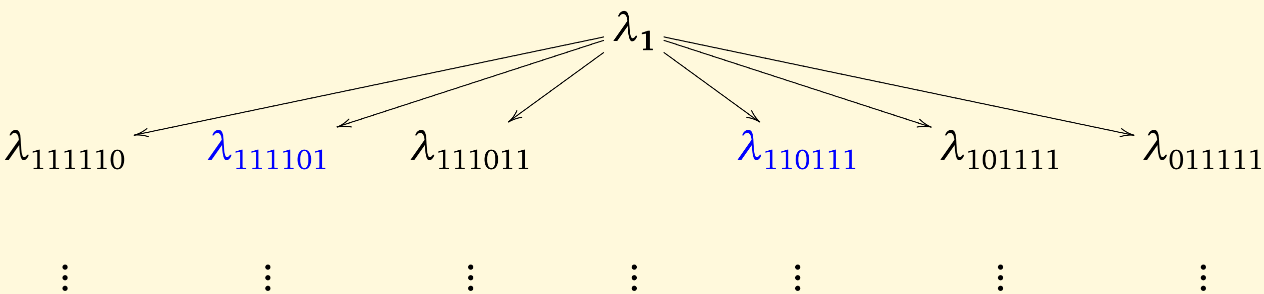
$$W_f(a) = 2^n \delta_0(a) - 2F_f(a)$$

Then we have:

$$W_f(a) = (-1)^{\mathrm{wt}(a)+1}\left[2\lambda_{1\dots1} + 2^2 S_{X_{n-1,a}} + 2^3 S_{X_{n-2,a}} + \cdots + 2^{n+1} S_{X_{0,a}}\right] \quad (4)$$

for any $0 \neq a \in \mathbb{F}_2^n$.

Let $a = 110101$ then $S_{X_{n-1,a}}$ consists of the λ's that are printed blue.



By the fact that at least one λ_u with $\mathrm{wt}(u) = n-1$ is odd and Lemma 1, since $d = n-1$ (indeed $a_u \equiv \lambda_u \pmod 2$), half of $a \in \mathbb{F}_2^n$ corresponds to even subset sums and the other half of $a \in \mathbb{F}_2^n$ corresponds to odd subset sums. Since λ_1 is even and by (4) we reach the conclusion.

Questions and Comments

References

1. Carlet, C., and Guillot, P. A new representation of Boolean functions. In *Proceedings of AAECC'13* (1999), no. 1719 in Lecture Notes in Computer Science.
2. Carlet, C., and Guillot, P. Bent, resilient functions and the numerical normal form. *DIMACS Series in Discrete Mathematics and Theoretical Computer Science 56* (2001), 87–96.
3. Rota, G.-C. *On the foundations of Combinatorial Theory*. Springer Verlag, 1964.