An algebraic description of Boolean functions

Massimiliano Sala (msala@bcri.ucc.ie)
Boole Centre for Research in Informatics, UCC Cork, Ireland

Ilaria Simonetti (simonet@mat.unimi.it)
Department of Mathematics, University of Milano, Italy.

Abstract

We compute the non-linearity of Boolean functions with Gröbner basis techniques. Moreover, we extend our approach to classify functions with maximum non-linearity.

Keywords: Gröbner basis, Boolean function, non-linearity.

1 Introduction

Any function from $(\mathbb{F}_2)^n$ to $\mathbb{F}_2$ is called a Boolean function. Boolean functions are important in symmetric cryptography, since they are used in the confusion layer of ciphers. An affine Boolean function does not provide an effective confusion. To overcome this, we need functions which are as far as possible from being an affine function. The effectiveness of these functions is measured by a parameter called "non-linearity" ([Carar]).

In this paper, we compute the non-linearity of Boolean functions with Gröbner basis techniques. Moreover, we extend our approach to classify functions with maximum non-linearity.

2 Preliminaries and notation

Let $\mathbb{F}_2$ be the field with 2 elements. Let $n \geq 1$ be an integer. From now on, n and an ordering on vectors in $(\mathbb{F}_2)^n = \{v_1, \ldots, v_{2^n}\}$ are understood.
We recall that a *Boolean function* is a function $f : (\mathbb{F}_2)^n \to \mathbb{F}_2$. We denote by $\mathcal{B}_n$ the set of all Boolean functions. It is well-known that f can be expressed as a polynomial in $\mathbb{F}_2[X] = \mathbb{F}_2[x_1, \ldots, x_n]$, as follows

$$f = \sum_{S \subset \{1,\ldots,n\}} b_S X_S \,, \text{ where } X_S = x_{i_1} \cdots x_{i_{|S|}},\ S = \{i_1, \ldots, i_{|S|}\}\,.$$

Definition 2.1. *Let $f, g \in \mathcal{B}_n$. The* **distance** *$d(f,g)$ between f and g is the number of $v \in (\mathbb{F}_2)^n$ such that $f(v) \neq g(v)$.*

We denote by $\mathcal{A}_n$ the set of all affine Boolean functions:

$$\mathcal{A}_n = \{a_0 + \sum_{i=1}^{n} a_i x_i \mid a_i \in \mathbb{F}_2\}\,,$$

where $a_i = a_{\{i\}}$ and $a_0 = a_\emptyset$.

Let A and B be the following variable sets: $A = \{a_i\}_{0\leq i\leq n}$, $B = \{b_S\}_{S\subset\{1,\ldots,n\}}$. We denote by $\mathfrak{g}_n \in \mathbb{F}_2[A,X] \subset \mathbb{F}_2[A,B,X]$, $\mathfrak{f}_n \in \mathbb{F}_2[B,X] \subset \mathbb{F}_2[A,B,X]$ the following polynomials:

$$\mathfrak{g}_n = a_0 + \sum_{i=1}^{n} a_i x_i\,, \quad \mathfrak{f}_n = \sum_{S\subset\{1,\ldots,n\}} b_S X_S\,.$$

Definition 2.2 ([Carar]). *Let $f \in \mathcal{B}_n$. The* **non-linearity** *$\mathrm{N}(f)$ of f is the minimum of the distances between f and any affine function:*

$$\mathrm{N}(f) = \min_{\alpha\in\mathcal{A}_n} d(f,\alpha)\,.$$

We denote by ν_n the following natural number:

$$\nu_n = \max_{f\in\mathcal{B}_n} \mathrm{N}(f)\,.$$

An upper bound of the non-linearity for a Boolean function f is [Carar]:

$$\mathrm{N}(f) \leq \nu_n \leq 2^{n-1} - 2^{\frac{n}{2}-1}\,.$$

This upper bound can only be met if n is even, and such functions are called **bent functions**.

Definition 2.3. *For any two vectors $v_1, v_2 \in (\mathbb{F}_2)^n$, the* **Hamming distance**, *$d(v_1,v_2)$, between v_1 and v_2 is the number of coordinates in which the two vectors differ. For any $v \in (\mathbb{F}_2)^n$, we denote by $w(v)$ the weight of v, i.e. the number of coordinates where v differs from zero.*

We consider a map from $\mathcal{B}_n$ to $(\mathbb{F}_2)^{2^n}$, which sends a Boolean function f into a vector $\underline{f}$, obtained by evaluating f in all $v \in (\mathbb{F}_2)^n$.
We denote by $S_{\mathcal{A}_n}(f)$ the set

$$S_{\mathcal{A}_n}(f) = \{\underline{f} + \underline{g} \mid g \in \mathcal{A}_n\} \subset (\mathbb{F}_2)^{2^n}\,.$$

The following lemma is obvious:

Lemma 2.4. *Let f, g be two Boolean functions. Then*

$$d(f,g) = d(\underline{f}, \underline{g}) = w(\underline{f} + \underline{g}) .$$

Therefore, computing the non-linearity of $f \in \mathcal{B}_n$ is the same as finding the minimum weight of vectors in set $S_{\mathcal{A}_n}(f)$.
We can extend the evaluation to polynomials $\mathfrak{g}_n$ and $\mathfrak{f}_n$ as follows:

$$\underline{\mathfrak{g}_n} = (\mathfrak{g}_n(A, v_1), \ldots, \mathfrak{g}_n(A, v_{2^n})) \in \mathbb{F}_2[A] ,$$

$$\underline{\mathfrak{f}_n} = (\mathfrak{f}_n(B, v_1), \ldots, \mathfrak{f}_n(B, v_{2^n})) \in \mathbb{F}_2[B] .$$

For the remainder of this section, we recall some definitions and results about the weight of vectors in $(\mathbb{F}_2)^n$, taken from [GOS06], and [Gue05].
We denote by $E[Y]$ the following set of polynomials in $\mathbb{F}_2[Y] = \mathbb{F}_2[y_1, \ldots, y_m]$: $E[Y] = \{y_1^2 + y_1, \ldots, y_m^2 + y_m\}$, where $m \geq 1$ is an integer, understood from now on.

Definition 2.5. *Let $1 \leq t \leq m$ and $\mathsf{m} \in \mathbb{F}_2[Y]$. We say that m is a* **simple t-monomial** *if:*

$$\mathsf{m} = y_{h_1} \cdots y_{h_t}, \text{ where } h_1, \ldots, h_t \in \{1, \ldots, m\} \text{ and } h_l \neq h_j, \forall l \neq j ,$$

i.e. a monomial in $\mathbb{F}_2[Y]$ such that $\deg_{y_{h_i}}(\mathsf{m}) = 1$ for any $1 \leq i \leq t$. We denote by $\mathcal{M}_{m,t}$ the set of all simple t-monomials in $\mathbb{F}_2[Y]$.

Let $t \in \mathbb{N}$, with $1 \leq t \leq m$ and let $I_{m,t} \subset \mathbb{F}_2[Y]$ be the following ideal

$$I_{m,t} = \langle \{\sigma_t, \ldots, \sigma_m\} \cup E[Y] \rangle ,$$

where σ_i are the elementary symmetric functions:

$$\begin{aligned}
\sigma_1 &:= y_1 + y_2 + \cdots + y_m, \\
\sigma_2 &:= y_1y_2 + y_1y_3 + \cdots + y_1y_m + y_2y_3 + \cdots + y_{m-1}y_m, \\
&\cdots \\
\sigma_{m-1} &:= y_1y_2y_3 \cdots y_{m-2}y_{m-1} + \cdots + y_2y_3 \cdots y_{m-1}y_m, \\
\sigma_m &:= y_1y_2 \cdots y_{m-1}y_m.
\end{aligned}$$

We also denote by $I_{m,m+1}$ the ideal $\langle E[Y] \rangle$.

For any $1 \leq i \leq m$, let P_i be the set which contains all vectors in $(\mathbb{F}_2)^m$ of weight i, $P_i = \{v \in (\mathbb{F}_2)^m \mid w(v) = i\}$, and let Q_i be the set which contains all vectors of weight up to i, $Q_i = \sqcup_{0 \leq j \leq i} P_j$.

Theorem 2.6. *Let t be an integer such that $1 \leq t \leq m$. Then the vanishing ideal $\mathcal{I}(Q_t)$ of Q_t is*

$$\mathcal{I}(Q_t) = I_{m,t+1} ,$$

and its reduced Gröbner basis G is

$$G = E[Y] \cup \mathcal{M}_{m,t}\,, \qquad \textit{for } t \geq 2\,,$$
$$G = \{y_1, \ldots, y_m\}\,, \qquad \textit{for } t = 1\,.$$

Let $I \subset \mathbb{F}_2[Y]$ be an ideal and let Y' be a subset of Y. We denote by $I_{Y'}$ the elimination ideal of I, i.e. $I_{Y'} = I \cap \mathbb{F}_2[Y']$.

3 Computing the non-linearity

In this section we show how to use Theorem 2.6 to compute the non-linearity for a Boolean function f.
We define an ideal where $\mathfrak{g}_n$ plays the role of a generic affine function. A point in its variety corresponds to an affine function with distance from f at most $t-1$.

Definition 3.1. *Let $f \in \mathcal{B}_n$. We denote by $J_t^n(f)$ the ideal in $\mathbb{F}_2[A]$:*

$$\begin{aligned} J_t^n(f) &= \langle \{\mathsf{m}(\mathfrak{g}_n(A, v_1) + f(v_1), \ldots, \mathfrak{g}_n(A, v_{2^n}) + f(v_{2^n})) \mid \mathsf{m} \in \mathcal{M}_{2^n,t}\} \cup E[A] \rangle \\ &= \langle \{\mathsf{m}(\underline{\mathfrak{g}_n} + \underline{f}) \mid \mathsf{m} \in \mathcal{M}_{2^n,t}\} \cup E[A] \rangle\,. \end{aligned}$$

Remark 3.2. Since $E[A] \subset J_t^n(f)$, $J_t^n(f)$ is zero-dimensional and radical ([Sei74]).

Lemma 3.3. *Let $f \in \mathcal{B}_n$. Let $t \in \mathbb{N}$ such that $1 \leq t \leq 2^n$. Then the following statements are equivalent:*

(1) $\mathcal{V}(J_t^n(f)) \neq \emptyset$

(2) $\exists u \in S_{\mathcal{A}_n}(f)$ *such that* $w(u) \leq t-1$

(3) $\exists \alpha \in \mathcal{A}_n$ *such that* $d(f, \alpha) \leq t-1\,.$

Proof.
(2)⇔(3).Obvious.
(1)⇒(2). Let $V = (\bar{a}_0, \bar{a}_1, \ldots, \bar{a}_n) \in \mathcal{V}(J_t^n(f))$ and let $u = (\mathfrak{g}_n(V, v_1), \ldots, \mathfrak{g}_n(V, v_{2^n}))$, which is an element in $S_{\mathcal{A}_n}(f)$. We have that $\mathsf{m}(u) = 0$ for all $\mathsf{m} \in \mathcal{M}_{2^n,t}$ and that $u \in (\mathbb{F}_2)^{2^n}$. So $u \in \mathcal{V}(I_{2^n,t})$ and, for Theorem 2.6, $u \in Q_{t-1}$, i.e. $w(u) \leq t-1$.
(2)⇒(1).It can be proved by reversing the above argument. □

From Lemma 3.3 we immediately have the following theorem.

Theorem 3.4. *Let $f \in \mathcal{B}_n$. The non-linearity* $\mathrm{N}(f)$ *is the minimum t such that $\mathcal{V}(J_{t+1}^n(f)) \neq \emptyset$.*

From this theorem we can derive an algorithm to compute the non-linearity for a function $f \in \mathcal{B}_n$, by computing any Gröbner basis of $J_t^n(f)$.

$j = 1$
While $\mathcal{V}(J_j^n(f)) = \emptyset$ **do**
$j := j + 1$;
Output $j - 1$

Remark 3.5. If f is not affine, we can start our check from $J_2^n(f)$.

Example 3.6. Lef $f : (\mathbb{F}_2)^3 \to \mathbb{F}_2$ be the Boolean function:

$$f(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2 + 1\,.$$

We want to compute $\mathrm{N}(f)$ and clearly f is not affine. We compute vector $\underline{f}$ and we take a generic affine function $\mathfrak{g}_3$, so that:
$\underline{f} = (1, 1, 0, 1, 1, 0, 0, 0)$,
$\underline{\mathfrak{g}_3} = (a_0, a_0 + a_1, a_0 + a_2, a_0 + a_1 + a_2, a_0 + a_3, a_0 + a_1 + a_3, a_0 + a_2 + a_3, a_0 + a_1 + a_2 + a_3)$.
So $\underline{f} + \underline{\mathfrak{g}_3} = (a_0 + 1, a_0 + a_1 + 1, a_0 + a_2, a_0 + a_1 + a_2 + 1, a_0 + a_3 + 1, a_0 + a_1 + a_3, a_0 + a_2 + a_3, a_0 + a_1 + a_2 + a_3) = (p_1, p_2, \ldots, p_8)$.
Ideal $J_2^3(f)$ is the ideal generated by

$$J_2^3(f) = \langle \{p_1p_2, p_1p_3, \ldots, p_7p_8\} \cup \{a_0^2 + a_0, a_1^2 + a_1, a_2^2 + a_2, a_3^2 + a_3\} \rangle\,.$$

We compute any Gröbner basis of this ideal and we obtain that it is trivial, so $\mathcal{V}(J_2^3(f)) = \emptyset$ and $\mathrm{N}(f) > 1$. Now we have to compute a Gröbner basis for $J_3^3(f)$. We obtain, using degrevlex ordering with $a_3 < a_2 < a_1 < a_0$, that $G(J_3^3(f)) = \{a_2 + a_3 + 1, a_3^2 + a_3, a_1a_3 + a_0 + 1, a_0a_3 + a_0 + a_3 + 1, a_1^2 + a_1, a_0a_1 + a_0 + a_1 + 1, a_0^2 + a_0\}$. So, $\mathrm{N}(f) = 2$ by Theorem 3.4. By inspecting $G(J_3^3(f))$, we also obtain all affine functions having distance 2 from f:

$$\alpha_1 = 1 + x_1 + x_2,\ \ \alpha_2 = 1 + x_2,\ \ \alpha_3 = 1 + x_3,\ \ \alpha_4 = x_1 + x_3\,.$$

4 Classification of Boolean functions with a given non-linearity

In this section we show how to find all Boolean functions with a given non-linearity.

We introduce a new ideal.

Definition 4.1. *We denote by $\mathfrak{I}_t^n$ the ideal in $\mathbb{F}_2[A,B]$ generated by*

$$\langle\{\mathsf{m}((\mathfrak{g}_n+\mathfrak{f}_n)(A,B,v_1),\ldots,(\mathfrak{g}_n+\mathfrak{f}_n)(A,B,v_{2^n}))\mid \mathsf{m}\in\mathcal{M}_{2^n,t}\}\cup E[A,B]\rangle$$
$$=\langle\{\mathsf{m}(\underline{\mathfrak{g}_n}+\underline{\mathfrak{f}_n})\mid \mathsf{m}\in\mathcal{M}_{2^n,t}\}\cup E[A,B]\rangle\,.$$

The key idea here is that a point in $\mathcal{V}(\mathfrak{I}_t^n)$ corresponds to a pair affine function/Boolean function such that their distance is at most $t-1$ (Theorem 3.4) and any such pair corresponds to a point in $\mathcal{V}(\mathfrak{I}_t^n)$. In particular, there are points in $\mathcal{V}(\mathfrak{I}_t^n)$ corresponding to Boolean functions with non-linearity $t-1$ (if such functions exist). However, a Boolean function f with $\mathrm{N}(f)=t-1$ will have no corresponding points in $\mathcal{V}(\mathfrak{I}_{t-1}^n)$. In other words, to find functions with $\mathrm{N}(f)=t$, we have to eliminate from $\mathcal{V}(\mathfrak{I}_{t+1}^n)$ all pairs with a corresponding point in $\mathcal{V}(\mathfrak{I}_t^n)$. To do this, we introduce the following ideal.

Definition 4.2. *For any $t\geq 2$, we denote by $\mathfrak{J}_t^n$ the ideal*

$$\mathfrak{J}_t^n=\langle\mathfrak{I}_t^n\cup\prod_{p\in B(\mathfrak{I}_{t-1}^n)}(p+1)\rangle,$$

where $B(\mathfrak{I}_{t-1}^n)$ is any finite basis for $\mathfrak{I}_{t-1}^n$.

Lemma 4.3. *The definition of $\mathfrak{J}_t^n$ does not depend on the paricular basis $B(\mathfrak{I}_{t-1}^n)$.*

Proof. It follows from the radicality. □

The following theorem comes directly from the previous argument and the obvious fact that a Boolean function f is affine if and only if $\mathrm{N}(f)=0$.

Theorem 4.4. *(1) With respect to any monomial ordering,*

$$G(\mathfrak{J}_1^n)=\{b_S\}_{\substack{S\subset\{1,\ldots,n\}\\ |S|\geq 2}}\cup\{b_i+a_i\}_{0\leq i\leq n}\,.$$

(2) For any $t\geq 2$, there is a bijective correspondence

$$\mathcal{V}\big((\mathfrak{J}_t^n)_B\big)\longleftrightarrow\{f\in\mathcal{B}_n\mid N(f)=t-1\}\,.$$

Example 4.5. We show how to find all functions in $\mathcal{B}_3$ which have non-linearity equal 1, and those with non-linearity 2.
We have that $\underline{\mathfrak{f}_3}+\underline{\mathfrak{g}_3}=(p_1(A,B),\ldots,p_8(A,B))$, where:
$p_1=a_0+b_0$
$p_2=a_0+a_1+b_0+b_1$
$p_3=a_0+a_2+b_0+b_2$
$p_4=a_0+a_1+a_2+b_0+b_1+b_2+b_{1,2}$
$p_5=a_0+a_3+b_0+b_3$

$p_6 = a_0 + a_1 + a_3 + b_0 + b_1 + b_3 + b_{1,3}$
$p_7 = a_0 + a_2 + a_3 + b_0 + b_2 + b_3 + b_{2,3}$
$p_8 = a_0 + a_1 + a_2 + a_3 + b_0 + b_1 + b_2 + b_3 + b_{1,2} + b_{1,3} + b_{2,3} + b_{1,2,3}$

We compute a Gröbner basis of $\mathfrak{I}_1^3$ with respect to degrevlex with $a_0 < a_1 < a_2 < a_3 < b_0 < b_1 < b_2 < b_3 < b_{1,2} < b_{1,3} < b_{2,3} < b_{1,2,3}$ and we obtain:

$$G(\mathfrak{I}_1^3) = \{b_0 + a_0, b_1 + a_1, b_2 + a_2, b_3 + a_3, b_{1,2}, b_{1,3}, b_{2,3}, b_{1,2,3}\},$$

as expected (Theorem 4.4-1). To find Boolean functions with non-linearity 1 we have to compute $G(\mathfrak{J}_2^3)$. A computation with respect to any ordering provides $G(\mathfrak{J}_2^3)$. Using standard elimination algorithms, we obtain $G((\mathfrak{J}_2^3)_B) = \{b_{1,2,3} + 1\} \cup E[B]$. We have thus proved that all Boolean functions in $\mathcal{B}_3$ having non-linearity 1 are

$$\left\{ x_1x_2x_3 + \sum_{S\subset\{1,2,3\},|S|\leq 2} b_S X_S \right\}. \tag{1}$$

To find Boolean functions with non-linearity 2, we compute $G(\mathfrak{J}_3^3)$. Using again elimination algorithms, we obtain $G((\mathfrak{J}_3^3)_B) = \{b_{1,2,3}, b_{2,3}b_{1,3}b_{1,2} + b_{2,3}b_{1,3} + b_{2,3}b_{1,2} + b_{1,3}b_{1,2} + b_{2,3} + b_{1,3} + b_{1,2} + 1\} \cup E[B]$.
We obtain that all functions in $\mathcal{B}_3$ with non-linearity 2 are:

$$\{f = \sum_{S\subset\{1,2,3\},|S|\leq 2} b_S X_S \mid \deg(f) = 2\}. \tag{2}$$

In conclusion, (1) and (2) provides our claimed classification for $\mathcal{B}_3$.

Acknowledgements

The second author would like to thank her supervisor: the first author.

For their comments and suggestions, the authors heartily thank E. Guerrini, E. Orsini, L. Perret, C. Traverso. This work has been partially supported by STMicroelectronics contract "Complexity issues in algebraic Coding Theory and Crytography".

References

[Carar] C. Carlet, *Boolean methods and models*, ch. Boolean Functions for Cryptography and Error Correcting Codes, Cambridge University Press, to appear.

[GOS06] E. Guerrini, M. Orsini, and M. Sala, *Computing the distance distribution of systematic non-linear codes*, Tech. Report 50, University College Cork, Cork, Ireland, 2006.

[Gue05] Eleonora Guerrini, *On distance and optimality in non-linear codes*, Master's thesis (laurea), University of Pisa, Department of Mathematics, 2005.

[Sei74] A. Seidenberg, *Constructions in algebra*, Trans. Amer. Math. Soc. **197** (1974), 273–313.