Applied Mathematics Letters 25 (2012) 739–744

Contents lists available at SciVerse ScienceDirect

Applied Mathematics Letters

journal homepage: www.elsevier.com/locate/aml

On the boolean partial derivatives and their composition

A. Martín del Rey[a,*], G. Rodríguez Sánchez[b], A. de la Villa Cuenca[c]

[a] Department of Applied Mathematics, E.P.S. de Ávila, Universidad de Salamanca, C/ Hornos Caleros 50, 05003-Ávila, Spain
[b] Department of Applied Mathematics, E.P.S. de Zamora, Universidad de Salamanca, Avda. Requejo 33, 49022-Zamora, Spain
[c] Department of Applied Mathematics and Computation, E.T.S.I. (ICAI) Universidad Pontificia Comillas, C/ Alberto Aguilera 23, 28015-Madrid, Spain

ARTICLE INFO

Article history:
Received 26 May 2011
Received in revised form 12 October 2011
Accepted 13 October 2011

Keywords:
Boolean functions
Boolean derivative

ABSTRACT

The main goal of this work is to introduce the relation between the partial boolean derivatives of an n-variable boolean function and their directional boolean derivatives.

1. Introduction and preliminaries

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over the Galois field $\mathbb{F}_2 = \{0, 1\}$, and set $\{e_1, \ldots, e_n\}$ as its standard basis, that is,

$$e_1 = (1, 0, \ldots, 0), e_2 = (0, 1, 0, \ldots, 0), \ldots, e_n = (0, \ldots, 0, 1). \tag{1}$$

For two vectors $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$ and $y = (y_1, \ldots, y_n) \in \mathbb{F}_2^n$, we can define the XOR addition operation as follows:

$$x \oplus y = (x_1 \oplus y_1, \ldots, x_n \oplus y_n) \in \mathbb{F}_2^n. \tag{2}$$

An n-variable boolean function is a map of the form $f : \mathbb{F}_2^n \to \mathbb{F}_2$. The set of all n-variable boolean functions is denoted by $\mathcal{BF}_n$ and its cardinality is $|\mathcal{BF}_n| = 2^{2^n}$. The vector

$$t_f = (f(v_0), f(v_1), \ldots, f(v_{2^n-1})) \in \mathbb{F}_2^{2^n}, \tag{3}$$

where $v_0 = (0, \ldots, 0), v_1 = (0, \ldots, 0, 1), \ldots, v_{2^n-1} = (1, \ldots, 1)$, is called the truth table of f. Note that for $1 \le i \le 2^n - 1$, v_i is the binary representation of i written as a vector of length 2^n.

The usual representation of a boolean function f is by means of its algebraic normal form (ANF for short) which is the n-variable polynomial representation over $\mathbb{F}_2$, that is,

$$f(x_1, \ldots, x_n) = a_0 \oplus \bigoplus_{\substack{1 \le k \le n \\ 1 \le i_1, i_2, \ldots, i_k \le n}} a_{i_1, i_2, \ldots i_k}, x_{i_1}, x_{i_2}, \ldots, x_{i_k}, \tag{4}$$

where $a_0, a_{i_1,\ldots,i_k} \in \mathbb{F}_2$. The degree of the ANF is the algebraic degree of the function. The simplest boolean functions, considering their ANF, are the affine boolean functions: $f(x_1, \ldots, x_n) = a_0 \oplus a_1x_1 \oplus a_2x_2 \oplus \cdots \oplus a_nx_n$, where $a_0, a_1, \ldots, a_n \in \mathbb{F}_2$. If $a_0 = 0$, we have the linear boolean functions and they are denoted by $l_a(x)$ with $a = (a_1, \ldots, a_n) \in \mathbb{F}_2^n$.

* Corresponding author. Tel.: +34 920 353500x3785; fax: +34 920 353501.
E-mail addresses: delrey@usal.es (A. Martín del Rey), gerardo@usal.es (G. Rodríguez Sánchez), avilla@dmc.icai.upcomillas.es (A. de la Villa Cuenca).

0893-9659/$ – see front matter
doi:10.1016/j.aml.2011.10.013

The Hamming weight of a boolean vector x is denoted by $wt(x)$ and is defined as the number of ones in the vector x. In this sense, the Hamming weight of a boolean function f is the Hamming weight of its truth table t_f. An n-variable boolean function f is said to be balanced if its weight is exactly 2^{n-1}, that is, if the number of ones equals the number of zeros of its truth table.

2. The partial derivative of a boolean function

The notion of the boolean derivative was introduced by Vichniac (see [1]) and it is defined as follows:

Definition 1. The partial derivative of an n-variable boolean function f with respect to the ith variable x_i is another n-variable boolean function, D_if, defined as follows:

$$\begin{aligned} &D_if : \mathbb{F}_2^n \to \mathbb{F}_2 \\ &x \mapsto D_if(x) = f(x) \oplus f(x \oplus e_i), \end{aligned} \tag{5}$$

that is,

$$D_if(x) = f(x_1, \dots, x_i, \dots, x_n) \oplus f(x_1, \dots, x_i \oplus 1, \dots, x_n). \tag{6}$$

The notion of the boolean derivative is very important and useful in, for example, cryptography (see [2]).

Example 1. Let us consider the four-variable boolean function whose ANF is $f(x_1, x_2, x_3, x_4) = 1 \oplus x_3 \oplus x_1x_2 \oplus x_2x_3 \oplus x_1x_2x_3 \oplus x_2x_3x_4$; then, as simple CALCULATIONS show, $D_1f(x_1, x_2, x_3, x_4) = x_2 \oplus x_2x_3$.

This definition allows one to state a derivation rule similar to the derivation rule for multivariate polynomials over real numbers:

Lemma 1. *Let f be an n-variable boolean function whose ANF is (4). Then for each variable x_i we have*

$$f(x) = g_i(x \oplus x_ie_i) \oplus x_ih_i(x \oplus x_ie_i), \tag{7}$$

where h_i and g_i are $(n-1)$-variable boolean functions which do not depend on the variable x_i. Moreover, if f does not depend on the variable x_i then $h_i = 0$.

Proof. Set $1 \leq i \leq n$; then the n-variable boolean function f can be factored by taking the common factor x_i, and consequently f can be written as follows:

$$f(x) = g_i(x_1, \dots, \widehat{x_i}, \dots, x_n) \oplus x_ih_i(x_1, \dots, \widehat{x_i}, \dots, x_n), \tag{8}$$

where g_i and h_i are $(n-1)$-variable boolean functions which do not depend on x_i. For the sake of simplicity we set $x \oplus x_ie_i = (x_1, \dots, \widehat{x_i}, \dots, x_n)$; then,

$$f(x) = g_i(x \oplus x_ie_i) \oplus x_ih_i(x \oplus x_ie_i), \tag{9}$$

thus finishing the proof. □

Example 2. Let us consider the four-variable boolean function whose ANF is $f(x_1, x_2, x_3, x_4) = x_1 \oplus x_2x_3 \oplus x_3x_4 \oplus x_2x_3x_4$. Then,

$$\begin{aligned} f(x_1, x_2, x_3, x_4) &= x_2x_3 \oplus x_3x_4 \oplus x_2x_3x_4 \oplus x_1 \\ &= x_1 \oplus x_3x_4 \oplus x_2(x_3 \oplus x_3x_4) \\ &= x_1 \oplus x_3(x_2 \oplus x_4 \oplus x_2x_4) \\ &= x_1 \oplus x_2x_3 \oplus x_4(x_3 \oplus x_2x_3). \end{aligned} \tag{10}$$

Proposition 1. *Let f be an n-variable boolean function. Then,*

$$D_if(x) = h_i(x \oplus x_ie_i). \tag{11}$$

Proof. By definition, $D_if(x) = f(x) \oplus f(x \oplus e_i)$, and taking into account the last lemma, this yields

$$D_if(x) = g_i(x \oplus x_ie_i) \oplus x_ih_i(x \oplus x_ie_i) \oplus g_i(x \oplus x_ie_i) \oplus (x_i \oplus 1)h_i(x \oplus x_ie_i) = h_i(x \oplus x_ie_i), \tag{12}$$

thus finishing the proof. □

As a consequence, the partial derivative (with respect to one variable) reduces the algebraic degree of the boolean function by 1.