Kragujevac Journal of Mathematics
Volume 36 Number 2 (2012), Pages 177–187.

ON POSITIVE, LINEAR AND QUADRATIC BOOLEAN FUNCTIONS

SERGIU RUDEANU

Abstract. In [1], [2] it was proved that a function $f : \{0,1\}^n \longrightarrow \{0,1\}$ is positive if and only if it is increasing, it is linear if and only if it satisfies

$$f(X) \vee f(Y) = f(XY) \vee f(X \vee Y) \tag{*}$$

and it is quadratic if and only if it satisfies

$$f(XY \vee XZ \vee YZ) \leq f(X) \vee f(Y) \vee f(Z). \tag{**}$$

In this paper we work with an arbitrary Boolean algebra B and with arbitrary Boolean functions $f : \mathsf{B}^n \longrightarrow \mathsf{B}$, that is, algebraic functions over B. We prove a refined generalization of the characterization of positive functions, we prove that a Boolean function satisfies (*) if and only if it is linear in each variable, and we prove that every quadratic Boolean function satisfies (**). Moreover, a Boolean function $f : \mathsf{B}^2 \longrightarrow \mathsf{B}$ is linear if and only if it satisfies (*) and a Boolean function $f : \mathsf{B}^3 \longrightarrow \mathsf{B}$ is quadratic if and only if it satisfies (**).

The term *Boolean function* over an arbitrary Boolean algebra $(\mathsf{B}, \vee, \cdot, ', 0, 1)$ designates the algebraic functions $f : \mathsf{B}^n \longrightarrow \mathsf{B}$, that is, the functions which can be obtained from variables and constants of B by superpositions of the basic operations $\vee, \cdot, '$. In the Boolean algebra $(\{0,1\}, \vee, \cdot, ', 0, 1)$, where $x \vee y = \max\{x, y\}$, $x \cdot y = \min\{x, y\}$ is also denoted simply xy, and $x' = 1 - x$, every function : $\{0,1\}^n \longrightarrow \{0,1\}$ is Boolean; besides, {0,1} is the only Boolean algebra with this property. The monograph [5] is devoted to Boolean functions in this general sense and to Boolean equations, meaning equations expressed by Boolean functions $f : \mathsf{B}^n \longrightarrow \mathsf{B}$. See also the continuation [6].

At the time when [5] was written, the functions $f : \{0,1\}^n \longrightarrow \{0,1\}$ were termed *truth functions* or *switching functions*, terms reminiscent of their roles in logic and in

Key words and phrases. Boolean function, positive linear function, linear Boolean function, quadratic Boolean function.

2010 *Mathematics Subject Classification.* 06E30.

Received: October 10, 2012.

switching theory, respectively, and distinguishing them from Boolean functions in the general sense. In the last decades a huge literature is devoted to truth functions and their numerous applications in science and technology; see e.g. the recent monographs [3], [4]. These compendia reveal that in most cases the results are mainly based on specific properties of the algebra {0,1} rather than on general properties of Boolean algebras.

Under the given circumstances the author deeply regrets that people working in this field are using the term "Boolean algebra" for the algebra {0,1} and "Boolean functions" for truth functions, thus using the general terminology for the particular case.

On the other hand it may be interesting to see whether certain isolated results can be generalized from truth functions to arbitrary Boolean functions. The present Note tackles such a particular problem.

Among other results, in [1] (see also [2]) the following theorems were proved about a truth function $f : \{0,1\}^n \longrightarrow \{0,1\}$:

1) f is positive, i.e., $f|_{x_i=0} \leq f|_{x_i=1}$, if and only if it is increasing, i.e., $X \leq Y \Rightarrow f(X) \leq f(Y)$;
2) f is linear, i.e., all its prime implicants are literals, if and only if it satisfies the functional equation (*) $f(X) \vee f(Y) = f(XY) \vee f(X \vee Y)$, where XY and $X \vee Y$ are defined componentwise, and
3) f is quadratic if and only if it satisfies the functional equation (**) $f(XY \vee XZ \vee YZ) \leq f(X) \vee f(Y) \vee f(Z)$.

In the present Note, after several prerequisites which make the work self-contained, we obtain the following results:

1') we generalize and refine Theorem 1) to Boolean functions,
2') we prove that a Boolean function satisfies property (*) if and only if it is linear in each variable, and for $n = 2$ condition (*) characterizes the linear Boolean functions $f : \mathsf{B}^2 \longrightarrow \mathsf{B}$, and
3') every quadratic Boolean function satisfies property (**), and for $n = 3$ condition (**) characterizes the quadratic Boolean functions $f : \mathsf{B}^3 \longrightarrow \mathsf{B}$.

Prerequisites

Let $(\mathsf{B}, \vee, \cdot, ', 0, 1)$ be an arbitrary Boolean algebra. Note that $\{0,1\}$ is a Boolean subalgebra of B and every two-element Boolean algebra is isomorphic to the algebra $\{0,1\}$ described above.

Further, let n be a positive integer. We use a vectorial notation like $X = (x_1, \ldots, x_n)$, $Y = (y_1, \ldots, y_n), \cdots \in \mathsf{B}^n$ and $A = (\alpha_1, \ldots, \alpha_n)$, $B = (\beta_1, \ldots, \beta_n), \cdots \in \{0,1\}^n$. The set B^n is a Boolean algebra under the componentwise defined operations $\vee, \cdot, '$, with zero $\mathbf{0} = (0, \ldots, 0)$ and one $\mathbf{1} = (1, \ldots, 1)$.

The *maxterms* are the 2^n Boolean functions defined by $X^A = x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ for $A \in \{0,1\}^n$, where x^α are the Boolean functions defined by $x^1 = x$ and $x^0 = x'$. The basic

property of *Boolean functions* is that they are characterized by the existence of the *canonical disjunctive form*

$$f(X) = \bigvee_{A\in\{0,1\}^n} c_A X^A \,,$$

where the coefficients $c_A \in \mathsf{B}$ are uniquely determined by $c_A = f(A)$ $(\forall\, A \in \{0,1\}^n)$. Therefore every Boolean function $f : \mathsf{B}^n \longrightarrow \mathsf{B}$ is determined by its restriction to $\{0,1\}^n$ and conversely, every truth function $f : \{0,1\}^n \longrightarrow \{0,1\}$ can be extended to a unique Boolean function $f : \mathsf{B}^n \longrightarrow \mathsf{B}$.

This immediately implies that two Boolean functions coincide if and only if their restrictions to $\{0,1\}^n$ coincide. In other words, if $f, g : \mathsf{B}^n \longrightarrow \mathsf{B}$ are Boolean functions, then

$$f(X) = g(X) \;\; (\forall\, X \in \mathsf{B}^n) \Longleftrightarrow f(A) = g(A) \;\; (\forall\, A \in \{0,1\}^n) \,;$$

even more generally,

$$f(X) \leq g(X) \;\; (\forall\, X \in \mathsf{B}^n) \Longleftrightarrow f(A) \leq g(A) \;\; (\forall\, A \in \{0,1\}^n) \,.$$

These two results are known as the *Müller-Löwenheim verification theorem.*

Every Boolean function $f : \mathsf{B}^n \longrightarrow \mathsf{B}$ reaches its minimum $\prod_{A\in\{0,1\}^n} f(A)$ and its maximum $\bigvee_{A\in\{0,1\}^n} f(A)$; as a matter of fact, the range of f is the interval determined by these values.

A Boolean equation $ax \vee bx' = 0$ is consistent if and only if $ab = 0$, or equivalently, $b \leq a'$, in which case the solution set is the interval $[b, a'] = \{x \in \mathsf{B} \mid b \leq x \leq a'\}$.

The computation rules $x \leq y \Longleftrightarrow xy' = 0$, $\quad x = y \Longleftrightarrow xy' \vee x'y = 0$ and $x_k = 0 \;\; (k = 1, \ldots, m) \Longleftrightarrow \bigvee_{k=1}^m x_k = 0$ enable the reduction of every system of Boolean equations and/or inequalities to a single equation of the form $f(X) = 0$, where f is a Boolean function. To write down the consistency condition of such an equation it is convenient to proceed by successive elimination of variables. The current step of this process is the following. To eliminate a variable x write the equation in the form $\alpha x \vee \beta x' \vee \gamma = 0$, where the Boolean functions α, β and γ do not depend on x. Then the consistency condition of the equation $f(X) = 0$ is the same as the consistency condition of the equation $\alpha\beta \vee \gamma = 0$.

1. Positive Boolean functions

The definition of *positive* Boolean functions and of *increasing* or *isotone* Boolean functions are the same as for truth functions. The equivalence of these properties can be generalized to Boolean functions and refined as follows.

Theorem 1.1. *The following properties are equivalent for a Boolean function* $f : \mathsf{B}^n \longrightarrow \mathsf{B}$*:*

(i) $f|_{x_i=0} \leq f|_{x_i=1} \;\; (i = 1, \ldots, n)$*;*
(ii) $X \leq Y \Longrightarrow f(X) \leq f(Y) \;\; (\forall\, X, Y \in \mathsf{B}^n)$*;*
(iii) $f(XY) \leq f(X) \;\; (\forall\, X, Y \in \mathsf{B}^n)$*;*
(iv) $f(X) \leq f(X \vee Y) \;\; (\forall\, X, Y \in \mathsf{B}^n)$*;*

(v) $A \leq B \Longrightarrow f(A) \leq f(B)$ $(\forall\, A, B \in \{0,1\}^n)$;
(vi) $f(AB) \leq f(A)$ $(\forall\, A, B, \in \{0,1\}^n)$;
(vii) $f(A) \leq f(A \vee B)$ $(\forall\, A, B \in \{0,1\}^n)$.

Proof. The equivalences (ii)$\Longleftrightarrow$(iii)$\Longleftrightarrow$(iv) are valid in the more general case of a function $f : L^n \longrightarrow L$ where L is a lattice.

The equivalences (ii)$\Longleftrightarrow$(v), (iii)$\Longleftrightarrow$(vi) and (iv)$\Longleftrightarrow$(vii) are established by the Müller-Löwenheim verification theorem.

(i)$\Rightarrow$(v): Suppose $A, B \in \{0,1\}^n$ satisfy $A \leq B$. If $A = B$ then (v) is trivial. If $A < B$ then $\alpha_i \leq \beta_i$ for all $i \in \{1, \ldots, n\}$ and there are some indices i for which $\alpha_i < \beta_i$. Let m be the number of those indices i for which $\alpha_i = 0$ and $\beta_i = 1$; so $0 < m \leq n$. Let further

$$A = A^0 < A^1 < \cdots < A^m = B$$

be the sequence obtained from A by changing in turn the 0s of A into 1s. Then

$$f(A) = f(A^0) \leq f(A^1) \leq \cdots \leq f(A^m) = f(B).$$

(ii)$\Rightarrow$(i): Trivial. □

2. Linear Boolean functions

A truth function f is called *linear* if either it is the constant function 0 or it can be written as a disjunctions of literals (that is, x_i or x_i'). We generalize this definition to Boolean functions as follows.

Definition 2.1. A *linear Boolean function* is a function $f : \mathsf{B}^n \longrightarrow \mathsf{B}$ which can be written in the form

$$f(X) = \bigvee_{i=1}^{n} (c_i x_i \vee d_i x_i') \quad (\forall\, X \in \mathsf{B}^n), \tag{2.1}$$

where the constants c_i and d_i are in B $(i = 1, \ldots, n)$.

So, the class of linear functions is indeed a subclass of the class of Boolean functions. Note that the constant functions and the Boolean functions of one variable are linear. The problem of characterizing linear Boolean functions is not trivial for $n \geq 2$.

Lemma 2.1. *Every linear Boolean function $f : \mathsf{B}^n \longrightarrow \mathsf{B}$ satisfies the identity*

$$f(X) \vee f(Y) = f(XY) \vee f(X \vee Y) \quad (\forall\, X, Y \in \mathsf{B}^n). \tag{2.2}$$

Proof. It follows from (2.1) that

$$f(X) \vee f(Y) = \bigvee_{i=1}^{n} (c_i(x_i \vee y_i) \vee d_i(x_i' \vee y_i')),$$

$$f(XY) \vee f(X \vee Y) = \bigvee_{i=1}^{n} (c_i x_i y_i \vee d_i(x_i' \vee y_i') \vee c_i(x_i \vee y_i) \vee d_i x_i' y_i')$$
$$= \bigvee_{i=1}^{n} (c_i(x_i \vee y_i) \vee d_i(x_i' \vee y_i')).$$

□

To prove a partial converse of Lemma 2.1 we need two preliminaries.

Lemma 2.2. *If a Boolean function $f : \mathsf{B}^n \longrightarrow \mathsf{B}$ satisfies* (2.2) *then it satisfies also*

$$f(1, Y) \vee f(0, Z) = f(0, Y) \vee f(1, Z) \ \ (\forall\, Y, Z \in \mathsf{B}^{n-1}), \tag{2.3}$$

or equivalently,

$$f(1, B) \vee f(0, C) = f(0, B) \vee f(1, C) \ \ (\forall\, B, C \in \{0,1\}^{n-1}). \tag{2.3'}$$

Proof. It follows from (2.2) that each side of (2.3) equals $f(0, YZ) \vee f(1, Y \vee Z)$. □

A weaker property is the following:

Definition 2.2. A Boolean function $f : \mathsf{B}^n \longrightarrow \mathsf{B}$ is *linear in a variable* x_i if it can be written in the form $f(X) = ax_i \vee bx_i' \vee g(Y)$, where $g : \mathsf{B}^{n-1} \longrightarrow \mathsf{B}$ is a Boolean function of the remaining variables.

Lemma 2.3. *If a Boolean function $f : \mathsf{B}^n \longrightarrow \mathsf{B}$ satisfies* (2.2)*, then it is linear in each variable.*

Proof. Since condition (2.2) is invariant to any permutation of the variables, it suffices to prove that f is linear in x_1. We will prove that condition (2.2) implies the existence of some elements $a, b \in \mathsf{B}$ and of a Boolean function $g : \mathsf{B}^{n-1} \longrightarrow \mathsf{B}$ such that

$$f(x, Y) = ax \vee bx' \vee g(Y) \ \ (\forall\, x \in \mathsf{B},\ \forall\, Y \in \mathsf{B}^{n-1}). \tag{2.4}$$

Indeed, identity (2.4) is equivalent to the system

$$f(1, Y) = a \vee g(Y) \ \ (\forall\, Y \in \mathsf{B}^{n-1}),$$
$$f(0, Y) = b \vee g(Y) \ \ (\forall\, Y \in \mathsf{B}^{n-1}),$$

which is equivalent to the equation

$$f(1, Y)a'g'(Y) \vee f'(1, Y)a \vee f'(1, Y)g(Y) \vee$$
$$\vee f(0, Y)b'g'(Y) \vee f'(0, Y)b \vee f'(0, Y)g(Y) = 0 \ \ (\forall\, Y \in \mathsf{B}^{n-1}),$$

which in its turn is equivalent to the system

$$f'(1, Y)a \vee f(1, Y)g'(Y)a' = 0 \ \ (\forall\, Y \in \mathsf{B}^{n-1}) \tag{2.5.1}$$
$$f'(0, Y)b \vee f(0, Y)g'(Y)b' = 0 \ \ (\forall\, Y \in \mathsf{B}^{n-1}), \tag{2.5.2}$$
$$[f'(1, Y) \vee f'(0, Y)]g(Y) = 0 \ \ (\forall\, Y \in \mathsf{B}^{n-1}). \tag{2.5.3}$$

Identity (2.5.1) holds if and only if the element $a \in B$ satisfies

$$f(1,Y)g'(Y) \leq a \leq f(1,Y) \ \ (\forall\, Y \in \mathsf{B}^{n-1}).$$

This happens if and only if

$$\max_{Y}[f(1,Y)g'(Y)] \leq a \leq \min_{Y} f(1,Y),$$

that is,

$$\bigvee_{B\in\{0,1\}^{n-1}} f(1,B)g'(B) \leq a \leq \prod_{C\in\{0,1\}^{n-1}} f(1,C), \tag{2.6.1}$$

and similarly, (2.5.2) is equivalent to

$$\bigvee_{B\in\{0,1\}^{n-1}} f(0,B)g'(B) \leq b \leq \prod_{C\in\{0,1\}^{n-1}} f(0,C). \tag{2.6.2}$$

Besides, the Müller-Löwenheim verification theorem shows that equation (2.5.3) is equivalent to

$$\bigvee_{B\in\{0,1\}^{n-1}} [f'(1,B) \vee f'(0,B)]g(B) = 0. \tag{2.6.3}$$

Therefore, taking into account that a Boolean function $g : \mathsf{B}^n \longrightarrow \mathsf{B}$ is determined by the values $g(B),\ B \in \{0,1\}^n$, it follows that the function f is of the form (2.4) if and only if the system (2.6) is consistent with respect to a, b and $g(B),\ B \in \{0,1\}^{n-1}$.

The consistency condition of equations (2.6.1) can be written in the following equivalent forms:

$$\bigvee_{B\in\{0,1\}^{n-1}} f(1,B)g'(B) \leq \prod_{C\in\{0,1\}^{n-1}} f(1,C),$$

$$\left[\bigvee_{C\in\{0,1\}^{n-1}} f'(1,C)\right] \bigvee_{B\in\{0,1\}^{n-1}} f(1,B)g'(B) = 0,$$

$$\left[\bigvee_{C\in\{0,1\}^{n-1}} f'(1,C)\right] f(1,B)g'(B) = 0 \ \ (\forall\, B \in \{0,1\}^{n-1}). \tag{2.7.1}$$

Similarly, the consistency condition of (2.6.2) is

$$\left[\bigvee_{C\in\{0,1\}^{n-1}} f'(0,C)\right] f(0,B)g'(B) = 0 \ \ (\forall\, B \in \{0,1\}^{n-1}). \tag{2.7.2}$$

Equation (2.6.3) is consistent and the Boolean functions $g : \mathsf{B}^{n-1} \longrightarrow \mathsf{B}$ which satisfy the equation are characterized by the condition

$$[f'(1,B) \vee f'(0,B)]\, g(B) = 0 \ \ (\forall\, B \in \{0,1\}^{n-1}). \tag{2.7.3}$$

Summarizing, the function f is of the form (2.4) if and only if system (2.6) is consistent, and this happens if and only if system (2.7) is consistent with respect to the unknowns $g(B)$.

System (2.7) can be written in the form

$$\left[f(1,B)\bigvee_{C\in\{0,1\}^{n-1}} f'(1,C)\vee f(0,B)\bigvee_{C\in\{0,1\}^{n-1}} f'(0,C)\right] g'(B)\vee$$
$$\vee\,[f'(1,B)\vee f'(0,B)]\,g(B)=0\ \ (\forall\, B\in\{0,1\}^{n-1}),$$

so that its consistency condition is

$$[f'(1,B)\vee f'(0,B)]\left[f(1,B)\bigvee_{C\in\{0,1\}^{n-1}} f'(1,C)\vee f(0,B)\bigvee_{C\in\{0,1\}^{n-1}} f'(0,C)\right]=0$$
$$(\forall\, B\in\{0,1\}^{n-1}),$$

which can be written in the equivalent forms

$$f'(1,B)f(0,B)\bigvee_{C\in\{0,1\}^{n-1}} f'(0,C)\vee$$
$$\vee f'(0,B)f(1,B)\bigvee_{C\in\{0,1\}^{n-1}} f'(1,C)=0\ \ (\forall\, B\in\{0,1\}^{n-1}),$$
$$f(0,B)f'(1,B)f'(0,C)=f(1,B)f'(0,B)f'(1,C)=0\ \ (\forall\, B,C\in\{0,1\}^{n-1}).$$

The latter condition is fulfilled by Lemma 2.2. □

Lemmas 2.1 and 2.3 can be joined as the main result of this section:

Theorem 2.1. *Every linear Boolean function satisfies* (2.2) *and every Boolean function which satisfies* (2.2) *is linear in each variable.*

Proposition 2.1. *A Boolean function* $f:\mathsf{B}^2\longrightarrow\mathsf{B}$ *is linear if and only if it satisfies* (2.2) *with* $n=2$.

Proof. The "only if" part is valid for arbitrary n by Lemma 2.1. Conversely, if $f:\mathsf{B}^2\longrightarrow\mathsf{B}$ satisfies (2.2), then by Lemma 2.3 identity (2.4) holds, which becomes $f(x,y)=ax\vee bx'\vee g(y)$; but $g(y)=cy\vee dy'$. □

3. Quadratic Boolean functions

The starting point in defining and studying quadratic Boolean functions is the trivial remark that the truth functions of two variables (in particular those of one variable) are quadratic. Therefore the following definition is natural.

Definition 3.1. A *quadratic Boolean function* is a function $f:\mathsf{B}^n\longrightarrow\mathsf{B}$ which can be written in the form

$$f(X)=\bigvee_{i=1}^{n}\bigvee_{j=i}^{n} f_{ij}(x_i,x_j)\ \ (\forall\, X\in\mathsf{B}^n),\tag{3.1}$$

where f_{ij} are Boolean functions.

In particular the expansion (3.1) includes $\bigvee_{i=1}^{n} f_{ii}(x_i, x_i)$, which is a linear Boolean function; this also shows that every linear Boolean function is quadratic. Note that every Boolean function of zero, one or two variables is quadratic. The problem of characterizing quadratic Boolean functions is not trivial for $n \geq 3$.

Proposition 3.1. *Every quadratic Boolean function $f : \mathsf{B}^n \longrightarrow \mathsf{B}$ satisfies the identity*

$$f(XY \vee XZ \vee YZ) \leq f(X) \vee f(Y) \vee f(Z) \quad (\forall\, X, Y, Z \in \mathsf{B}^n). \tag{3.2}$$

Proof. Since the components of the vector $XY \vee XZ \vee YZ$ are $x_iy_i \vee x_iz_i \vee y_iz_i$, it suffices to prove that the functions f_{ij} in (3.1) satisfy

$$f_{ij}(x_iy_i \vee x_iz_i \vee y_iz_i, x_jy_j \vee x_jz_j \vee y_jz_j) \leq f_{ij}(x_i, x_j) \vee f_{ij}(y_i, y_j) \vee f_{ij}(z_i, z_j).$$

Indeed, the functions f_{ij} are of the form

$$f_{ij}(x_i, x_j) = a_{ij}x_ix_j \vee b_{ij}x_ix'_j \vee c_{ij}x'_ix_j \vee d_{ij}x'_ix'_j,$$

therefore, taking into account that $(a \vee b)(a \vee c)(b \vee c) = (a \vee bc)(b \vee c) = ab \vee ac \vee bc$, we have

$$\begin{aligned}
&f_{ij}(x_iy_i \vee x_iz_i \vee y_iz_i,\, x_jy_j \vee x_jz_j \vee y_jz_j) = \\
=&a_{ij}(x_iy_i \vee x_iz_i \vee y_iz_i)(x_jy_j \vee x_jz_j \vee y_jz_j) \vee \\
\vee&b_{ij}(x_iy_i \vee x_iz_i \vee y_iz_i)(x'_j \vee y'_j)(x'_j \vee z'_j)(y'_j \vee z'_j) \vee \\
\vee&c_{ij}(x'_i \vee y'_i)(x'_i \vee z'_i)(y'_i \vee z'_i)(x_jy_j \vee x_jz_j \vee y_jz_j) \vee \\
\vee&d_{ij}(x'_i \vee y'_i)(x'_i \vee z'_i)(y'_i \vee z'_i)(x'_j \vee y'_j)(x'_j \vee z'_j)(y'_j \vee z'_j) = \\
=&a_{ij}(x_iy_i \vee x_iz_i \vee y_iz_i)(x_jy_j \vee x_jz_j \vee y_jz_j) \vee \\
\vee&b_{ij}(x_iy_i \vee x_iz_i \vee y_iz_i)(x'_jy'_j \vee x'_jz'_j \vee y'_jz'_j) \vee \\
\vee&c_{ij}(x'_iy'_i \vee x'_iz'_i \vee y'_iz'_i)(x_jy_j \vee x_jz_j \vee y_jz_j) \vee \\
\vee&d_{ij}(x'_iy'_i \vee x'_iz'_i \vee y'_iz'_i)(x'_jy'_j \vee y'_jz'_j \vee y'_jz'_j),
\end{aligned}$$

while

$$\begin{aligned}
&f_{ij}(x_i, x_j) \vee f_{ij}(y_i, y_j) \vee f_{ij}(z_i, z_j) = \\
=&a_{ij}(x_ix_j \vee y_iy_j \vee z_iz_j) \vee b_{ij}(x_ix'_j \vee y_iy'_j \vee z_iz'_j) \vee \\
\vee&c_{ij}(x'_ix_j \vee y'_iy_j \vee z'_iz_j) \vee d_{ij}(x'_ix'_j \vee y'_iy'_j \vee z'_iz'_j).
\end{aligned}$$

Now it suffices to prove four inequalities $\leq$, that is between the coefficients of a_{ij}, b_{ij} c_{ij} and d_{ij}, respectively. Indeed, first an easy factorization shows that

$$(x_iy_i \vee x_iz_i \vee y_iz_i)(x_jy_j \vee x_jz_j \vee y_jz_j) \leq x_ix_j \vee y_iy_j \vee z_iz_j,$$

so that we have obtained the desired inequalities between the coefficients of a_{ij} and similar inequalities hold between the coefficients of b_{ij}, of c_{ij}, and of d_{ij}. □

Proposition 3.2. *A Boolean function* $f : \mathsf{B}^3 \longrightarrow \mathsf{B}$ *is quadratic if and only if it satisfies* (3.2) *with* $n = 3$.

Proof. The "only if" part is valid for arbitrary n by Proposition 3.1. Conversely, we suppose that a Boolean function $f : \mathsf{B}^3 \longrightarrow \mathsf{B}$ satisfies (3.2) and we will prove that f can be written in the form

$$\begin{aligned} f(x,y,z) =& axy \vee bxy' \vee cx'y \vee dx'y' \vee \\ & \vee hxz \vee ixz' \vee jx'z \vee kx'z' \vee myz \vee nyz' \vee py'z \vee qy'z'. \end{aligned} \tag{3.3}$$

Setting $f(\alpha,\beta,\gamma) = f_{\alpha\beta\gamma}$, identity (3.3) is equivalent to the following system of equations:

$$f_{000} = d \vee k \vee q, \tag{3.4.0}$$
$$f_{001} = d \vee j \vee p, \tag{3.4.1}$$
$$f_{010} = c \vee k \vee n, \tag{3.4.2}$$
$$f_{011} = c \vee j \vee m, \tag{3.4.3}$$
$$f_{100} = b \vee i \vee q, \tag{3.4.4}$$
$$f_{101} = b \vee h \vee p, \tag{3.4.5}$$
$$f_{110} = a \vee i \vee n, \tag{3.4.6}$$
$$f_{111} = a \vee h \vee m. \tag{3.4.7}$$

Our task is to prove that condition (3.2) implies the consistency of system (3.4) with respect to the unknowns $a, \ldots, q$. We obtain the consistency condition of (3.4) by successive elimination of variables.

Equations (3.4.7) and (3.4.6) can be joined into the single equation

$$f'_{111}a \vee f'_{111}(h \vee m) \vee f_{111}a'h'm' \vee f'_{110}a \vee f'_{110}(i \vee n) \vee f_{110}a'i'n' = 0,$$

which can be rewritten as

$$(f'_{111} \vee f'_{110})a \vee (f_{111}h'm' \vee f_{110}i'n')a' \vee f'_{111}(h \vee m) \vee f'_{110}(i \vee n) = 0,$$

which is of the form $\alpha a \vee \beta a' \vee \gamma = 0$, and since

$$\alpha\beta = (f'_{111} \vee f'_{110})(f_{111}h'm' \vee f_{110}i'n') = f'_{111}f_{110}i'n' \vee f'_{110}f_{111}h'm',$$

the result $\gamma \vee \alpha\beta = 0$ of the elimination of a is

$$f'_{111}h \vee f'_{111}m \vee f'_{110}i \vee f'_{110}n \vee f'_{111}f_{110}i'n' \vee f'_{110}f_{111}h'm' = 0. \tag{3.5.1}$$

In the same way we eliminate b from (3.4.5) and (3.4.4), c from (3.4.3) and (3.4.2), d from (3.4.1) and (3.4.0), and we obtain

$$f'_{101}h \vee f'_{101}p \vee f'_{100}i \vee f'_{100}q \vee f'_{101}f_{100}i'q' \vee f'_{100}f_{101}h'p' = 0, \tag{3.5.2}$$
$$f'_{011}j \vee f'_{011}m \vee f'_{010}k \vee f'_{010}n \vee f'_{011}f_{010}k'n' \vee f'_{010}f_{011}j'm' = 0, \tag{3.5.3}$$
$$f'_{001}j \vee f'_{001}p \vee f'_{000}k \vee f'_{000}q \vee f'_{001}f_{000}k'q' \vee f'_{000}f_{001}j'p' = 0. \tag{3.5.4}$$

We rewrite system (3.5) in the following form:

$$(f'_{111} \vee f'_{011})m \vee (f'_{110} \vee f'_{010})n \vee (f'_{101} \vee f'_{001})p \vee (f'_{100} \vee f'_{000})q = 0, \tag{3.6.0}$$

$$(f'_{111} \vee f'_{101})h \vee (f'_{110}f_{111}m' \vee f'_{100}f_{101}p')h' = 0, \tag{3.6.1}$$

$$(f'_{110} \vee f'_{100})i \vee (f'_{111}f_{110}n' \vee f'_{101}f_{100}q')i' = 0, \tag{3.6.2}$$

$$(f'_{011} \vee f'_{001})j \vee (f'_{010}f_{011}m' \vee f'_{000}f_{001}p')j' = 0, \tag{3.6.3}$$

$$(f'_{010} \vee f'_{000})k \vee (f'_{011}f_{010}n' \vee f'_{001}f_{000}q')k' = 0. \tag{3.6.4}$$

By eliminating h, i, j, k from (3.6.1)–(3.6.4) we obtain

$$f'_{111}f'_{100}f_{101}p' \vee f'_{101}f'_{110}f_{111}m' = 0, \tag{3.7.1}$$

$$f'_{110}f'_{101}f_{100}q' \vee f'_{100}f'_{111}f_{110}n' = 0, \tag{3.7.2}$$

$$f'_{011}f'_{000}f_{001}p' \vee f'_{001}f'_{010}f_{011}m' = 0, \tag{3.7.3}$$

$$f'_{010}f'_{001}f_{000}q' \vee f'_{000}f'_{011}f_{010}n' = 0. \tag{3.7.4}$$

We rewrite the system consisting of (3.6.0) and the four equations (3.7) in the form

$$(f'_{111} \vee f'_{011})m \vee (f'_{101}f'_{110}f_{111} \vee f'_{001}f'_{010}f_{011})m' = 0, \tag{3.8.1}$$

$$(f'_{110} \vee f'_{010})n \vee (f'_{100}f'_{111}f_{110} \vee f'_{000}f'_{011}f_{010})n' = 0, \tag{3.8.2}$$

$$(f'_{101} \vee f'_{001})p \vee (f'_{111}f'_{100}f_{101} \vee f'_{011}f'_{000}f_{001})p' = 0, \tag{3.8.3}$$

$$(f'_{100} \vee f'_{000})q \vee (f'_{110}f'_{101}f_{100} \vee f'_{010}f'_{001}f_{000})q' = 0. \tag{3.8.4}$$

The elimination of m, n, p, q yields

$$\begin{aligned} &f'_{111}f'_{001}f'_{010}f_{011} \vee f'_{011}f'_{101}f'_{110}f_{111} \vee f'_{110}f'_{000}f'_{011}f_{010} \vee f'_{010}f'_{100}f'_{111}f_{110} \vee \\ &\vee f'_{101}f'_{011}f'_{000}f_{001} \vee f'_{001}f'_{111}f'_{100}f_{101} \vee f'_{100}f'_{010}f'_{001}f_{000} \vee f'_{000}f'_{110}f'_{101}f_{100} = 0. \end{aligned} \tag{3.9}$$

We have thus proved that (3.9) is the consistency condition of system (3.4). But equation (3.9) consists in fact of 8 conditions of the form

$$f'_{\alpha_1\beta_1\gamma_1}f'_{\alpha_2\beta_2\gamma_2}f'_{\alpha_3\beta_3\gamma_3}f_{\alpha\beta\gamma} = 0. \tag{3.10}$$

It is easy to check that in each case we have

$$(\alpha_1, \beta_1, \gamma_1)(\alpha_2, \beta_2, \gamma_2) \vee (\alpha_1, \beta_1, \gamma_1)(\alpha_3, \beta_3, \gamma_3) \vee (\alpha_2, \beta_2, \gamma_2)(\alpha_3, \beta_3, \gamma_3) = (\alpha, \beta, \gamma).$$

Therefore (3.2) implies

$$f(\alpha, \beta, \gamma) \leq f(\alpha_1, \beta_1, \gamma_1) \vee f(\alpha_2, \beta_2, \gamma_2) \vee f(\alpha_3, \beta_3, \gamma_3)$$

and each condition (3.10) is fulfilled. □

4. Open questions

1. For $n \geq 3$, is it true that a Boolean function linear in each variable is linear?
2. What more can be said about the converse of Proposition 3.1?

Acknowledgement: I thank Silvana Marinković and Dragić Banković for their helpful remarks.

References

[1] O. Ekin, S. Foldes, P.L. Hammer, L. Hellerstein, *Equational characterizations of Boolean function classes.* Discrete Math. **211** (2000), 27–51.
[2] L. Hellerstein, *Characterizations of special classes by functional equations.* Chapter 11 in [3].
[3] Y. Crama, P.L. Hammer, *Boolean Functions: Theory, Algorithms and Applications.* Cambridge Univ. Press, New York 2011.
[4] Y. Crama, P.L. Hammer, (eds), *Boolean Models and Methods in Mathematics, Computer Science and Engineering.* Cambridge Univ. Press, New York 2010.
[5] S. Rudeanu, *Boolean Functions and Equations.* North-Holland, Amsterdam/American Elsevier, New York 1974.
[6] S. Rudeanu, *Lattice Functions and Equations.* Springer-Verlag, London 2001.

University of Bucharest,
Faculty of Mathematics and Informatics,
Romania
E-mail address: srudeanu@yahoo.com