Bull. Math. Soc. Sc. Math. Roumanie
Tome 49(97) No. 1, 2006, 87–98

On unary lattice functions and Boolean functions

by
Sergiu Rudeanu

To Professor Ion D. Ion on the occasion of his 70th Birthday

Abstract

We study several properties of lattice and Boolean functions of one argument: being a translation, an endomorphism, a closure operator, and properties related to the composition of functions. The latter properties include inversability, commutativity and the existence of classes of lattice/Boolean functions that are commutative subgroups. It turns out that these semigroups are also lattices. We obtain as a by-product a characterization of distributive lattices.

Key Words: Distributive lattice, Boolean function, lattice function, endomorphism, translation, commutativity of composition.
2000 Mathematics Subject Classification: Primary: 06E30, Secondary 06B99.

The general concept of algebraic function [2] means a function built up from variables and constants by superpositions of the basic operations of the algebra. By a *lattice function* and a *Boolean function* we mean the specializations of this universal-algebraic concept to lattices and Boolean algebras, respectively. The monographs [8],[9] survey these concepts from an algebraic point of view.[1]

In this paper we study lattice and Boolean functions of one argument. We are mainly interested in properties such as being a translation or a closure operator, the existence of fixed points and properties related to the composition of functions: inversability, commutativity of two functions and the existence of classes of lattice/Boolean functions that are commutative semigroups with respect to composition. It turns out that these semigroups are also lattices with respect to the conjunction and disjunction defined pointwise. As a by-product we obtain a characterization of distributive lattices in terms of unary lattice functions and endomorphisms.

[1] Although some of the chapters in [8],[9] are devoted to them, the applications of Boolean functions would deserve a companion monograph.

*

Let $(L;\cdot,\vee)$ be a lattice; the meet operation $\cdot$ will usually be replaced by concatenation. We recall that, according to universal algebra, the set $LF1$ of *lattice functions* $f : L \longrightarrow L$ is defined recursively as follows: (i) the identity function x and the constant functions b ($b \in L$) are in $LF1$; (ii) if f, g are in $LF1$, then fg and $f \vee g$ are in $LF1$, where these functions are defined pointwise, i.e., $(fg)(x) = f(x)g(x)$ and $(f \vee g)(x) = f(x) \vee g(x)$; (iii) every member of $LF1$ is obtained by applying the above rules (i) and (ii).

As shown by rule (ii), the functions in $LF1$ form a sublattice $(LF1;\cdot,\vee)$ of the pointwise defined lattice $(L^L;\cdot,\vee)$.

Thus the functions of the following forms are lattice functions:

$$x \ , \ b \ , \ ax \ , \ x \vee b \ , \ ax \vee b \tag{1}$$

where $a, b \in L$. *If the lattice L is distributive, then the functions of the form* (1) *exhaust the set LF1 of unary lattice functions.* For the functions of the form (1) are closed with respect to meet and join. To see this we must check 30 cases. Here is one of them:

$$(ax \vee b)(cx \vee d) = (ac \vee ad \vee bc)x \vee bd \ , \tag{2}$$

$$(ax \vee b) \vee (cx \vee d) = (a \vee c)x \vee (b \vee d) \ . \tag{3}$$

Moreover, if the distributive lattice L is also *bounded*, that is, it has *least element* 0 and *greatest element* 1, then *the unary lattice functions are simply those of the form*

$$f(x) = ax \vee b \ . \tag{4}$$

For

$$x = 1 \cdot x \vee 0 \ , \ b = 0 \cdot x \vee b \ , \ ax = ax \vee 0 \ , \ x \vee b = 1 \cdot x \vee b \ . \tag{5}$$

Remark 1 (J.C. Abbott[2]). A distributive lattice is bounded if and only if its unary latice functions coincide with the functions of the form (4). The "if" part follows from the fact that we have in particular the expansion $x = ax \vee b$, which implies $b \leq x$ for all x, that is, $b = 0$. Then the expansion $x = ax$ implies $x \leq a$ for all x, that is, $a = 1$. □

The following easy remarks are well known. In a distributive lattice the representation (4) can be replaced by

$$f(x) = \bar{a}x \vee b, \text{ where } \bar{a} \geq b \ : \tag{6}$$

take $\bar{a} = a \vee b$. If, moreover, the lattice is bounded, then (4) implies $b = f(0)$ and $a \vee b = f(1)$, while the representation (6) is unique: $\bar{a} = f(1)$, $b = f(0)$.

The latter results were generalized by Goodstein [1] to functions of several variables; see also [9], Ch.3, §3.

[2] Private communication.

The last prerequisite is the concept of *translation*, introduced by Szász [11],[12] for semilattices and lattices. A function $f : L \longrightarrow L$ is called a *meet translation* (*join translation*) if it satifies the identity $f(xy) = f(x)y$ (the identity $f(x \vee y) = f(x) \vee y$). Several papers [3]–[7] , [11] , [12] study translations of lattices, partially ordered sets and graphs.

*

We are now in a position to carry out the program announced in the introduction.

Proposition 1 below is motivated by the following results. Szász [11] proved that a lattice is distributive if and only if every meet translation (join translation) is an endomorphism. Schweigert [10] proved that a lattice is distributive if and only if every lattice function $f : L \longrightarrow L$ is *idempotent* (i.e., it satisfies $f \circ f = f$); for a slight extension see [9], Proposition 3.3.2[3].

Proposition 1. *A lattice L is distributive if and only if every lattice function $f : L \longrightarrow L$ is an endomorphism.*

Proof. If L is distributive, we check that all the functions (1) are endomorphisms. The following computation is typical:

$$a \cdot xy \vee b = ax \cdot ay \vee b = (ax \vee b)(ay \vee b) \ ,$$

$$a(x \vee y) \vee b = ax \vee ay \vee b = (ax \vee b) \vee (ay \vee b) \ .$$

If L is not distributive, then, according to a well-known theorem, two cases are possible.

(i) L includes a *diamond* sublattice $\{o, a, b, c, e\}$, which means that o is the least element of the sublattice, e is its greatest element, while the elements a, b, c are pairwise incomparable. Then the function $x \vee a$ is not an endomorphism, because $bc \vee a = o \vee a = a$, while $(b \vee a)(c \vee a) = e \cdot e = e$.

(ii) L includes a *pentagon* sublattice $\{o, a, b, c, e\}$, which means that $o < a < b < e$ and $o < c < e$, while the elements a and c are incomparable and so are the elements b and c. Then $bc \vee a = o \vee a = a$, while $(b \vee a)(c \vee a) = be = b$. □

Corollary 1. *The following conditions are equivalent for a bounded lattice L:*

(i) *L is distributive;*

(ii) *every lattice function $f : L \longrightarrow L$ is idempotent;*

(iii) *every lattice function $f : L \longrightarrow L$ is an endomorphism;*

(iv) *every lattice function $f : L \longrightarrow$ is an idempotent endomorphism.*

Proof. By Schweigert's result and Proposition 1. □

We have seen that *in a bounded distributive lattice every function $f : L \longrightarrow L$ is of the form* (4).

Proposition 2. *In the above property none of the two hypotheses can be dispensed with.*

[3]where L^n should read L.

Proof. Remark 1 shows that the existence of the least and greatest elements is essential. To prove that distributivity cannot be dispensed with, we will prove that the property fails for the diamond lattice.

Using the same notation as for case (i) in the proof of Proposition 1, we are going to prove that the lattice function $(ax \vee b)(bx \vee c)$ cannot be represented in the form (4). Suppose, by way of contradiction, that an identity of the form

$$(ax \vee b)(bx \vee c) = px \vee q$$

holds. Taking $x := o$ we get $bc = q$; so $q = o$. Therefore, taking $x := a$, we obtain $c = pa \leq a$, which is false. □

Remark 2. Since the diamond is a modular lattice, we have proved even more: distributivity cannot be replaced by modularity. □

Conjecture. L is a bounded distributive lattice if and only if every lattice function $f : L \longrightarrow L$ is of the form (4).

*

It has been noted that every lattice L can be embedded into a bounded lattice $\bar{L}$. To be specific, if L has no least element (no greatest element), then a new element 0 (a new element 1) is added to L and one defines $x \cdot 0 = 0 \cdot x = 0$ and $x \vee 0 = 0 \vee x = x$ (one defines $x \cdot 1 = 1 \cdot x = x$ and $x \vee 1 = 1 \vee x = 1$) for every $x \in \bar{L}$. If L has already least element 0 (greatest element 1), then this is left as least element (greatest element). So $L = \bar{L}$ iff L is bounded (for instance, if L is complete, or, more particularly, if L is finite). Besides, if L is distributive, so is $\bar{L}$.

Notation. In the following $(L; \cdot, \vee)$ is a *distributive lattice.*

Proposition 3. *If* card$L \geq 2$*, then every unary lattice function on* L *can be uniquely extended to a unary lattice function on* $\bar{L}$.

Proof. The unary lattice functions on L are of the forms described in (1). These expressions generate lattice functions on $\bar{L}$ as well, so that the extensions do exist.

We prove uniqueness in five steps; at each step we are given a function $f : L \longrightarrow L$ having one of the forms given in (1). Let $g : \bar{L} \longrightarrow \bar{L}$ be a lattice function which extends f. Then g is of the form $g(x) = px \vee q$ $(\forall x \in \bar{L})$, hence $f(x) = px \vee q$ $(\forall x \in L)$. We shall start from the latter identity and prove that p and q determine a unique function g: namely, g is the function of the form (4) such that f is obtained from g as shown in (5). Unless otherwise stated, the identities are meant to hold in L.

1. From $x = px \vee q$ we deduce $q = 0$, $p = 1$ as in Remark 1.

2. Suppose $b = px \vee q$, where $b \in L$.

If $b = 0$, then $q = 0$ and $px = 0$. As $L \neq \{0\}$, it follows that $p \neq 1$. So $p = 0$ or $p \in L$; in the latter case we take $x := p$ and obtain $p = 0$ again. Thus $p = q = 0$.

If $b = 1$, then $q \neq 0$, otherwise $1 = px$ would imply $p = x = 1$, which contradicts $L \neq \{1\}$. So $q = 1$ or $q \in L$; in the latter case we take $x := q$ and obtain $1 = q$ again. Thus $q = 1$ and the function g is unique: $g(x) = 1$ $(\forall x \in \bar{L})$.

If $b \in L$ and $b \notin \{0, 1\}$, we note that $q \leq b$ implies $q \neq 1$. But $q \neq 0$, otherwise $b = px$ would imply $b \leq x$, which contradicts $b \neq 0$. Therefore $q \in L$ and we can take $x := q$, which yields $b = q$, so that $b = px \vee b$. Then $p \neq 1$, otherwise $b = x \vee b$ would imply $x \leq b$, which contradicts $b \neq 1$. Therefore $p = 0$ or $p \in L$; in the latter case we take $x := p$ and obtain $b = p \vee b$, i.e., $p \leq b$. Hence $p \leq b$ in both cases, while $q = b$. Thus the function g is unique: $g(x) = b$ $(\forall x \in \bar{L})$.

3. If $ax = px \vee q$, where $a \in L$, then $q \leq ax \leq x$, hence $q = 0$ and $ax = px$. Taking $x := a$ we obtain $a = pa$, that is, $a \leq p$. Since $a = 1$ reduces to the previous case 1, while $a = 0$ reduces to the previous case 2 with $b = 0$, we can suppose $a \notin \{0, 1\}$. Then $p \neq 1$, otherwise $ax = x$ would imply $x \leq a$, hence $a = 1$. Besides, $a \leq p$ implies $p \neq 0$. Therefore $p \in L$ and we can take $x := p$, which yields $ap = p$, that is $p \leq a$, hence $p = a$. Thus $p = a$ and $q = 0$.

4. If $x \vee b = px \vee q$, where $b \in L$, we apply formula (6) and obtain $x \vee b = \bar{p}x \vee q$, where $q \leq \bar{p}$. Then $x \leq \bar{p}x \vee q \leq \bar{p} \vee q = \bar{p}$, hence $\bar{p} = 1$ and $x \vee b = x \vee q$. Moreover, since $b = 0$ is the previous case 1, while $b = 1$ is the previous case 2, we can assume $b \notin \{0, 1\}$.

Taking $x := b$ we get $b = b \vee q$, that is, $q \leq b$, hence $q \neq 1$. We have also $q \neq 0$, otherwise $x \vee b = x$ would contradict $b \neq 1$. Therefore $q \in L$ and we can take $x := q$, which yields $q \vee b = q$, that is, $b \leq q$, hence $q = b$. Thus $\bar{p} = 1$ and $q = b$.

5. Using the representation (6), the last case is $ax \vee b = px \vee q$, where $a, b \in L$, $a \geq b$ and $p \geq q$. We can also assume that $a, b \notin \{0, 1\}$, since the 0–1 values for a or b yield the cases studied before.

Taking $x := a$, we obtain $a = a \vee b = pa \vee q \leq p \vee q = p$.

Taking $x := b$ we obtain $b = pb \vee q$, hence $q \leq b$.

Since $q = 0$ would imply $b \leq px \leq x$, in contradiction with $b \neq 0$, it follows that $q \neq 0$, hence $p \neq 0$.

Since $p = 1$ would imply $x \leq ax \vee b \leq a \vee b = a$, in contradiction with $a \neq 1$, it follows that $p \neq 1$, hence $q \neq 1$.

The above inequalities imply that $p, q \in L$. Taking $x := p$ we obtain

$$a = a \vee b = ap \vee b = pp \vee q = p \, .$$

Taking $x := q$ we obtain

$$b \leq aq \vee b = p \vee q = q \, ,$$

therefore $b = q$. Thus $a = p$ and $b = q$. □

Corollary 2. *In order to prove a hereditary property of unary lattice functions on a distributive lattice, it suffices to prove it in the case of a bounded distributive lattice, with the functions written in the form* (4).

Proof. This amounts to proving the property for the extensions g constructed in the proof of Proposition 3. $\square$

It follows from [12], Corollaries 3 and 5, that in a distributive lattice the meet translations are the functions of the form ax. It seems natural to ask which lattice functions ar join translations?

Proposition 4. *The following properties are equivalent for a unary lattice function f:*

(i) *f is a join translation;*

(ii) *f is a closure operator* (i.e., isotone, extensive and idempotent)*;*

(iv) *f is of the form $x \vee b$* (including the identity function x and the constant function 1, if any).

Proof. In view of Corollary 2, we can work in a bounded distributive lattice. We set $f(x) = ax \vee b$, or, equivalently, $f(x) = (a \vee b)x \vee b$.

(i)$\Longleftrightarrow$(iii): Condition (i) reads $a(x \vee y) \vee b = ax \vee b \vee y$ and it implies $y \leq a(x \vee y) \vee b \leq a \vee b$, that is, $a \vee b = 1$, therefore $f(x) = x \vee b$. Conversely, the latter function is clearly a join translation.

(ii)$\Longleftrightarrow$(iii): The function f is anyway isotone and idempotent by proposition 1, so that it remains to characterize extensivity. This means $x \leq f(x)$, that is, $x \leq ax \vee b$, which implies $x \leq a \vee b$, therefore $a \vee b = 1$. So $f(x) = x \vee b$ and conversely, the latter function is clearly extensive. $\square$

The next problem to be studied is commutativity. We say that two functions $f, g : L \longrightarrow L$ *commute*, if $f \circ g = g \circ f$. A subset $F \subset L^L$ will be called *commutative* provided every two members of F commute.

Lemma 1. *Suppose $f(x) = ax \vee b$ and $g(x) = cx \vee d$. Then*

$$f(g(x)) = acx \vee ad \vee b \tag{7}$$

and $f \circ g = g \circ f$ if and only if

$$ad \vee b = cb \vee d\,. \tag{8}$$

Proof. Checking formula (7) is routine. It follows from (7) that the property of commutativity reads

$$acx \vee ad \vee b = cax \vee cb \vee d\,,$$

which implies the sufficiency of condition (8) and also the necessity, by taking $x := bd$. $\square$

We see that in general f and g do not commute. We will point out several commutative classes of unary lattice functions. They appear to be also lattices.

Proposition 5. (i) *Each of the following classes of lattice functions is a sublattice of $(LF1; \cdot, \vee)$ and a commutative subgroup of $(LF1; \circ)$: 1) the functions of the form $ax \vee b$ with fixed b; 2) the functions of the form $ax \vee b$ with fixed a and $b \leq a$.*

(ii) *The latter functions satisfy $f \circ g = g \circ f = f \vee g$.*

Proof. 1) Applying formulas (2),(3) and (7) with $d = b$, we obtain

$$(fg)(x) = (ac \vee ab \vee bc)x \vee b \ , \ (f \vee g)(x) = (a \vee c)x \vee b$$

and

$$f(g(x)) = acx \vee b = g(f(x) \ .$$

2) Applying formulas (2),(3) and (7) with $c = a$ and $b, d \leq a$, we obtain $bd \leq b \vee d \leq a$ and

$$(fg)(x) = ax \vee bd \ , \ (f \vee g)(x) = ax \vee b \vee d$$

and

$$f(g(x)) = ax \vee d \vee b = g(f(x)) = (f \vee g)(x) \ .$$

□

Corollary 3. (i) *The following are particular cases of the classes of functions in Proposition 5:* $1'$) *the functions of the form* ax *(including the identity* x *and the constant function* 0*);* $2'$) *the functions of the form* $x \vee b$ *(including the identity* x *and the constant function* 1*).*

Proof. From Proposition 5 via Corollary 2. □

Remark 3. The functions of the form $ax \vee b$ with fixed $a \neq 1$, form a sublattice of $(LF1; \cdot, \vee)$ and a non-commutative subgroup of $(LF1; \circ)$. For, taking $c = a$ we obtain $(fg)(x) = ax \vee bd$, $(f \vee g)(x) = ax \vee b \vee d$, while $(f \circ g)(x) = ax \vee ad \vee b$ and $(g \circ f)(x) = ax \vee ab \vee d$. Take e.g. $b = a$ and $d \not\leq a$. □

The papers [11],[12] study also the fixed points of translations. Using the well-known notation

$$[p, q] = \{x \in L \mid p \leq x \leq q\} \ , \ [p) = \{x \in L \mid p \leq x\} \ , \ (p] = \{x \in L \mid x \leq p\} \ ,$$

we can state:

Remark 4. The sets of fixed points of the functions (1) are

$$L \ , \{b\} \ , \ (a] \ , \ [b) \text{ and } [b, a \vee b] \ , \tag{9}$$

respectively. For clearly $ax \vee b = x \Longrightarrow b \leq x \leq a \vee b$ and conversely, the latter inequalities imply $(a \vee b)x \vee b = x \vee b = x$. □

*

Now we are going to undertake a parallel study in the case when the lattice L is a Boolean algebra $(B; \cdot, \vee, ', 0, 1)$. Let us recall a few prerequisites.

The Boolean functions $f : B \longrightarrow B$ are characterized by the fact that they can be written in the canonical form[4] $f(x) = ax \vee bx'$, where $a = f(1)$ and $b = f(0)$.

[4]Due to Boole himself and rediscovered by Shannon.

The set $FB1$ of unary Boolean functions is a Boolean subalgebra of the pointwise defined Boolean algebra B^B.

The following computational rules are very useful:

$$a \le b \Longleftrightarrow ab' = 0 \ , \ a = b \Longleftrightarrow ab' \vee a'b = 0 \ , \ (ax \vee bx')' = a'x \vee b'x' \ .$$

It is also convenient to use the ring sum $x + y = xy' \vee x'y$, which satisfies the identity $x + x = 0$. Note that $x' = x + 1$ and $x + y = x \vee y \Longleftrightarrow xy = 0$; in particular $ab + cb' = ab \vee cb'$.

The Boolean equation $ax \vee bx' = 0$ ($ax \vee bx' = 1$) has a solution iff $ab = 0$ ($a \vee b = 1$).

The lattice functions of the lattice $(B; \cdot, \vee)$, that is, the functions of the form $f(x) = px \vee q$, coincide with the isotone Boolean functions. As a matter of fact, we can say even more:

Theorem 1. *The following conditions are equivalent for a unary Boolean function f:*

(i) *f is of the form $f(x) = px \vee q$;*
(ii) *f is isotone;*
(iii) *f is a meet endomorphism;*
(iv) *f is a join endomorphism;*
(v) *f is a lattice endomorphism;*
(vi) *f is idempotent;*
(vii) *f has fixed points.*

Proof. As we have already noted, the equivalence (i)$\Longleftrightarrow$(ii) is well known. The equivalences (iii)$\Longleftrightarrow$(iv)$\Longleftrightarrow$(v) and (ii)$\Longleftrightarrow$(iii)$\Longleftrightarrow$(v) follow from [8], Proposition 12.8 with $a = b = 0$ and Proposition 12.9 with $a = 0$, respectively. Thus conditions (i)–(v) are equivalent.

To prove the equivalence (vi)$\Longleftrightarrow$(i) (which is also known), take $f(x) = ax \vee bx'$. Then

$$f(f(x)) = a(ax \vee bx') \vee b(a'x \vee b'x') = (a \vee a'b)x \vee abx' = (a \vee b)x \vee abx' \ ,$$

therefore $f \circ f = f$ iff $a \vee b = a$ and $ab = b$, which means $b \le a$. The latter condition implies $f(x) = ax \vee bx' \vee bx = ax \vee b$ and conversely, (i) implies $f(x) = (p \vee q)x \vee qx'$.

(vii)$\Longleftrightarrow$(i): The fixed point condition $ax \vee bx' = x$ can be written in the form $(ax \vee bx')x' \vee (a'x \vee b'x')x = 0$, that is, $bx' \vee a'x = 0$, which means $bx' = a'x = 0$, or equivalently, $b \le x \le a$. Therefore fixed points do exist iff $b \le a$. □

Corollary 4. *The only Boolean function which is a Boolean endomorphism is the identiy function x.*

Proof. Given a lattice endomorphism $f(x) = px \vee q$, the missing condition for being a Boolean endomorphism is $f(x') = (f(x))'$, that is, $px' \vee q = (p' \vee x')q'$. This can be written in the equivalent form

$$(px' \vee q)(px \vee q) \vee (p' \vee x)q'(p' \vee x')q' = 0 \ ,$$

which reduces to $q \vee p'q' = 0$, that is, $q = 0$ and $p = 1$. □

Proposition 6. *A Boolean function is a join translation if and only if it is of the form* $x \vee b$.

Comment. This does not follow from Proposition 4, which refers to the functions $px \vee q$ instead of the functions in $BF1$.

Proof. We write the condition of being a join translation in the following equivalent forms:

$$a(x \vee y) \vee bx'y' = ax \vee bx' \vee y \ ,$$

$$(a(x \vee y) \vee bx'y')(a'x \vee b'x')y' \vee (a'(x \vee y) \vee b'x'y')(ax \vee bx' \vee y) = 0 \ ,$$

$$(ax \vee bx')(a'x \vee b'x')y' \vee a'bx'y \vee a'y = 0 \ ,$$

and finally $a'y = 0$. The latter condition is equivalent to $a = 1$, that is, $f(x) = x \vee bx' = x \vee b$. □

Now we pass to the composition of Boolean functions.

Lemma 2. *Let* $f(x) = ax \vee bx'$ *and* $g(x) = cx \vee dx'$. *Then*

$$f(g(x)) = (ac \vee bc')x \vee (ad \vee bd')x' \ . \tag{10}$$

Proof. Routine. □

Let 1_B denote the identity function $1_B(x) = x$. Then we have:

Theorem 2. α) *The following conditions are equivalent for a unary Boolean function f:*

(i) *there is a unary Boolean function g such that* $f \circ g = 1_B$;

(ii) *there is a unary Boolean function g such that* $g \circ f = 1_B$;

(iii) *there is a unary Boolean function g such that* $f \circ g = g \circ f = 1_B$;

(iv) $f \circ f = 1_B$;

(v) *the function f is of the form* $f(x) = x + b$.

β) *When this is the case, the function g is unique, namely* $g = f$.

Proof. In view of Lemma 2, the condition $f \circ g = 1_B$ can be written in the form

$$ac \vee bc' = 1 \ \& \ ad \vee bd' = 0 \ . \tag{11}$$

The first equation has a solution c iff $a \vee b = 1$, while the second equation has a solution d iff $ab = 0$. Thus the system (11) is consistent iff $a = b'$, which amounts to $f(x) = b'x \vee bx' = x + b$. When this holds, system (11) becomes

$$b'c \vee bc' = 1 \ \& \ b'd \vee bd' = 0 \ ,$$

whose unique solution is $c = b'$, $d = b$, that is, $g(x) = b'x \vee bx' = f(x)$. So (i)$\Longleftrightarrow$(v) and $g = f$ is unique. This also implies (i)$\Longleftrightarrow$(iv).

We get the condition for $g \circ f = 1_B$ by interchanging in (11) a with c and b with d. We thus obtain

$$ca \vee da' = 1 \ \& \ cb \vee db' = 0 \ ,$$

or equivalently,

$$c'a \vee d'a' \vee cb \vee db' = 0 \ . \tag{12}$$

So $c'a = cb = 0$, hence $a \leq c \leq b'$, therefore $a \leq b'$, and also $d'a' = db' = 0$, hence $a' \leq d \leq b$, therefore $a' \leq b$. It follows that $b' \leq a$, hence $a = b'$, therefore $f(x) = x + b$ again. Now equation (12) becomes

$$c'b' \vee d'b \vee cb \vee db' = 0 \ ,$$

which is equivalent to $c = b'$ & $d = b$, so that $g(x) = f(x)$ again. Therefore (ii)$\Longleftrightarrow$(v) and $g = f$ is unique.

Clearly the equivalence (i)$\Longleftrightarrow$(ii) with unique $g = f$ implies (i)$\Longleftrightarrow$(ii)$\Longleftrightarrow$(iii) with unique g. □

The last topic is commutativity.

Proposition 7. *Two Boolean functions, $f(x) = ax \vee bx'$ and $g(x) = cx \vee dx'$, commute if and only if*

$$a'd = bc' \ , \tag{13}$$

that is,

$$f'(1)g(0) = g'(1)f(0) \ . \tag{14}$$

Proof. In view of Lemma 2, the commutativity condition is equivalent to the system

$$ac + bc' = ca + da' \tag{15.1}$$

$$ad + bd' = cb + db' \tag{15.2}$$

But (15.1) is equivalent to (13), while

$$(15.2) \Longleftrightarrow ad + bd + b = bc + bd + d \Longleftrightarrow ad + d = bc + b \Longleftrightarrow (13) \ .$$

□

Whereas Proposition 7 is quite satisfactory, the commutativity of a class of Boolean functions seems to be a difficult problem; like in the case of distributive latices, we will obtain only sufficient conditions.

Proposition 5 and Remark 1 suggest that it might be useful to work with the sets

$$BF_b = \{f \in BF1 \mid f(x) = ax \vee bx' \ , \ a \in B\} \ , \tag{16}$$

$${}_aBF = \{f \in BF1 \mid f(x) = ax \vee bx' \ , \ b \in B\} \ . \tag{17}$$

We recall that the ideals of a Boolean algebra B are defined as being the ideals of the lattice $(B; \cdot, \vee)$ and they coincide with the ideals of the Boolean ring $(B; \cdot, +, 0, 1)$. The congruence associated with an ideal I is defined by

$$x \equiv y \ (\mathrm{mod} I) \Longleftrightarrow x + y \in I \ ; \tag{18}$$

as a matter of fact, every congruence of the Boolean algebra is obtained in this way. We will denote by e/I the equivalence class of an element $e \in B$ under the congruence (18).

Proposition 8. *A class $K \subset BF_b$ ($K \subset {}_aBF$) is commutative if and only if there exists $e \in B$ such that the members of K are of the form $f(x) = ax \vee bx'$ with $a \in e/(b']$ (of the form $f(x) = ax \vee bx'$ with $b \in e/(a]$).*

Proof. Given $f(x) = ax \vee bx'$ and $g(x) = cx \vee bx'$, the commutativity condition in Proposition 7 can be written in the following equivalent forms:

$$a'b = bc' \iff (a'+c')b = 0 \iff (a+c)b = 0 \iff a+c \leq b' \iff a \equiv c \;(\mathrm{mod}(b']) \;.$$

The second part is proved similarly. □

However the sets K in Proposition 8 are not semigroups. But we are going to obtain results that are stronger and more symmetric than Proposition 5 and Remark 3. Define the sets

$$LF_b = \{f \in BF1 \mid f(x) = ax \vee b \;,\; a \in [b)\} \;, \tag{19}$$

$${}_aLF = \{f \in BF1 \mid f(x) = ax \vee b \;,\; b \in (a]\} \;. \tag{20}$$

Remark 5. If $b \leq a$ then $ax \vee b = ax \vee bx \vee bx' = ax \vee bx'$. Therefore $LF_b \subset BF_b$ and ${}_aLF \subset_a BF$. □

Proposition 9. (i) *LF_b (${}_aLF$) is the greatest subsemigroup of $(BF_b;\circ)$ (of $({}_aBF;\circ)$). Moreover, it is a commutative semigroup and also a sublattice of $(BF1;\cdot,\vee)$.*

(ii) *For every $f, g \in LF_b$ we have $f \circ g = g \circ f = fg$ and for every $f, g \in {}_aLF$ we have $f \circ g = g \circ f = f \vee g$.*

Proof. We have $LF_b \subset BF_b$ by Remark 5. Further, take $f, g \in LF_b$, say $f(x) = ax \vee b$ with $b \leq a$ and $g(x) = cx \vee b$ with $b \leq c$. Then $b \leq ac \leq a \vee c$ and using the computation in the proof of Proposition 5, we see that LF_b is a sublattice and a commutative semigroup.

Now let K be a subsemigroup of $(BF_b;\circ)$ and take $f \in K$, say $f(x) = ax \vee bx'$. Then $f \circ f \in K$, hence $f \circ f \in BF_b$. On the other hand, formula (10) with $c = a$ and $d = b$ yields $(f \circ f)(x) = (a \vee ba')x \vee abx'$. It follows that $ab = b$, hence $b \leq a$ and we have $f(x) = ax \vee b$ by Remark 5. Thus $f \in LF_b$ and we have proved that $K \subset LF_b$.

The proof of the second part is similar. □

Remark 6. The elements of the commutative sets LF_b and ${}_aLF$ should be of the forms prescribed in Proposition 8, namely $a \in 1/(b']$ and $b \in 0/(a]$, respectively. Indeed, they can be written in the form $f(x) = ax \vee bx'$ by Remark 5, while the supplementary condition $b \leq a$ can be written in the equivalent forms $b \in 0/(a]$ and $a + 1 = a' \leq b'$, which means $a \in 1/(b']$. □

References

[1] R.L. Goodstein, The solutions of equations in a lattice. Proc. Roy. Soc. Edinburgh, Sect.A, 67(1967), Part III, 231-242.

[2] G. Grätzer, *Universal Algebra*, Second edition. Springer-Verlag, New York 1979. First edition: Van Nostrand, Princeton 1968.

[3] J. Nieminen, Derivations and translations on lattices. Acta Sci. Math. (Szeged) 38(1976), 359-363.

[4] J. Nieminen, The lattice of translations of a lattice. Acta Sci. Math. (Szeged) 39(1977), 109-113.

[5] J. Nieminen, M. Peltola, Translations on graphs. Acta Sci. Math. (Szeged) 66(2000), 455-463.

[6] J. Rachůnek, Translations des ensembles ordonnés. Math. Slovaca 31(1981), 337-340.

[7] J. Rachůnek, Translations of distributive and modular ordered sets. Acta Univ. Palack. Oblomouc. Fac. Rerum Natur. Math. 27(1988), 13-23 (1989).

[8] S. Rudeanu, *Boolean Functions and Equations*, North-Holland, Amsterdam 1974.

[9] S. Rudeanu, *Lattice Functions and Equations*, Springer-Verlag, London 2001.

[10] D. Schweigert, Über idempotent Polynomfunktionen auf Verbänden. Elemente der Mathematik 30/2(1975), 30-32.

[11] G. Szász, Die Translationen der Halbverbänden. Acta Sci. Math. (Szeged) 17(1956), 165-169.

[12] G. Szász, Derivations of lattices. Acta Sci. Math. (Szeged) 37(1975), 149-154.

Received: 15.12.2005

Faculty of Mathematics, University of Bucharest,
Str. Academiei 14, Bucharest,
RO-010014, Romania
E-mail: `srudeanu@yahoo.com`