Annals of the University of Craiova, Mathematics and Computer Science Series
Volume 39(2), 2012, Pages 125–131
ISSN: 1223-6934

On the number of fixed points of a Boolean transformation

Sergiu Rudeanu

Abstract. In [1] the authors determine the Boolean transformations $F : \{0,1\}^2 \longrightarrow \{0,1\}^2$ which have two fixed points, via the semi-tensor product method. In the present paper, using the irredundant solution of a Boolean equation in an arbitrary Boolean algebra, which we have devised in [2], we obtain two generalizations. First we find the fixed points of a Boolean transformation $F : B^2 \longrightarrow B^2$ in an arbitrary Boolean algebra B. Secondly, we describe explicitly the form of the transformations $F : \{0,1\}^2 \longrightarrow \{0,1\}^2$ having exactly k fixed points, for $k = 0, \ldots, 4$.

2010 Mathematics Subject Classification. 06E30, 94C10.
Key words and phrases. Boolean transformation, fixed point, irredundant solution.

In [1] the authors use the technique of semi-tensor product in order to determine all the transformations $F : \{0,1\}^2 \longrightarrow \{0,1\}^2$ which have exactly two fixed points. In the present paper we first recall all necessary well-known prerequisites in §1. In §2 we recall the concept of irredundant solution of a Boolean equation in n variables over an arbitrary Boolean algebra B, introduced in [2], and carry out the complete computation for $n = 2$. Also, as an application we determine explicitly the fixed points of a Boolean transformation $F : B^2 \longrightarrow B^2$ (Proposition 2.2). In §3, by applying Proposition 2.2 for $B = \{0,1\}$, we determine explicitly, for $k = 0, \ldots, 4$, those transformations $F : \{0,1\}^2 \longrightarrow \{0,1\}^2$ which have exactly k fixed points. So, as a by-product we have thus obtained a classification of the 256 transformations.

1. Introduction

In switching theory it is customary to use the name Boolean algebra for the algebra $(\{0,1\}, \vee, \cdot, ', 0, 1)$, where $x \vee y = \max(x, y)$ and $x \cdot y = xy = \min(x, y)$, and the name Boolean function for the functions with arguments and values in $\{0,1\}$.

Yet in algebra the term Boolean algebra has a more general meaning, namely any non-trivial distributive complemented lattice, i.e., any algebra $(B, \vee, \cdot, ', 0, 1)$, where the binary operations $\vee, \cdot$ are idempotent, commutative, associative, each of them distributive over the other, 0 is unit for $\vee$, 1 is unit for $\cdot$, $0 \neq 1$, and x' is the complement of x, i.e., $x \vee x' = 1$ and $x \cdot x' = 0$. There is a plethora of Boolean algebras in mathematics, e.g. in probability theory, functional analysis, mathematical logic, etc. Besides the two-element Boolean algebra $\{0,1\}$, another standard example of Boolean algebras is provided by the fields of subsets $(\mathcal{P}(S), \cup, \cap, ', \varnothing, S)$, where $'$ denotes set complementation.

For an arbitrary Boolean algebra B, the term Boolean function is reserved to the algebraic functions over B, that is, those functions which are obtained from variables and constants of B by superpositions of the operations $\vee, \cdot$ and $'$. It is proved that a

Received October 5, 2012.

function $f : B^n \longrightarrow B$ is Boolean if and only if it can be represented in the canonical disjunctive form (CDF)

$$f(x_1,\ldots,x_n) = \bigvee_{\alpha_1,\ldots,\alpha_n\in\{0,1\}} c_{\alpha_1\ldots\alpha_n} x_1^{\alpha_1}\ldots x_n^{\alpha_n}\ , \tag{3.1}$$

where $\bigvee$ denotes iterated disjunction (like $\sum$ with respect to $+$), and x^α is defined by $x^1 = x$ and $x^0 = x'$; the elements $c_{\alpha_1\ldots\alpha_n}$ belong to B (in fact, $c_{\alpha_1\ldots\alpha_n} = f(\alpha_1,\ldots,\alpha_n)$). So, while there are $\mid B \mid^{|B|^n}$ functions $f : B^n \longrightarrow B$, only $\mid B \mid^{2^n}$ of them are Boolean functions. It follows that in the two-element Boolean algebra $\{0,1\}$ every function $f : \{0,1\}^n \longrightarrow \{0,1\}$ is Boolean in the above sense, and $\{0,1\}$ is the unique Boolean algebra with this property.

Boolean equations are equations expressed in terms of Boolean functions. Every Boolean equation $f = g$ is equivalent to the Boolean equation $fg' \vee f'g = 0$, and every system of Boolean equations $f_j = 0$ $(j = 1,\ldots,m)$ is equivalent to the single Boolean equation $\bigvee_{j=1}^m f_j = 0$.

The Boolean equation in one unknown $ax \vee bx' = 0$ has solutions if and only if $ab = 0$, in which case the set of solutions is the interval $[b, a'] = \{x \in B \mid b \le x \le a'\}$, where the order relation $\le$ satisfies $x \le y \iff xy = x \iff xy' = 0$. Equivalently, the solution set has the parametric representation $x = a't \vee bt'$.

More generally, the Boolean equation in n unknowns $f(x_1,\ldots,x_n) = 0$ has solutions if and only if $\prod_{A\in\{0,1\}^n} f(A) = 0$. One of the methods for solving such an equation is the successive elimination of variables, which has two stages. The first one iterates the following step. One writes the equation in the form

$$f(x_1,\ldots,x_{n-1},1)x_n \vee f(x_1,\ldots,x_{n-1},0)x_n' = 0\ ,$$

which is regarded as an equation in x_n, so that the consistency condition is

$$f(x_1,\ldots,x_{n-1},1)f(x_1,\ldots,x_{n-1},0) = 0\ .$$

This equation has (at most) $n-1$ unknowns and the procedure continues until all the variables have been eliminated. The second stage follows in reverse order the equations constructed in the first stage, introducing in turn each of the solutions $x_1, x_2, \ldots$ into the previous equation. In §2 we will explicitly apply this technique for $n = 2$.

A representation theorem says that every Boolean algebra is isomorphic to a field of sets, therefore all the set-theoretical computation rules are valid in arbitrary Boolean algebras, e.g. the De Morgan laws. Other useful computation rules are $x \vee x'y = x \vee y$, $x(x' \vee y) = xy$, $(ax \vee bx')(cx \vee dx') = acx \vee bdx'$, $(ax \vee bx')' = a'x \vee b'x'$, $(axy \vee bxy' \vee cx'y \vee dx'y')' = a'xy \vee b'xy' \vee c'x'y \vee d'x'y'$, and in general formula (3.1) yields $f'(x_1,\ldots,x_n) = \bigvee c'_{\alpha_1\ldots\alpha_n} x_1^{\alpha_1}\ldots x_n^{\alpha_n}$. In §2 and §3 we will tacitly use these rules.

Much more about Boolean functions and Boolean equations can be found in [2] and also in [3].

2. Irredundant solutions of Boolean equations

In this section we work in an arbitrary Boolean algebra. First we present the irredundant solution of a Boolean equation, devised in [2], which means a parametric representation of the solutions of a Boolean equation in such a way that there is a bijection between the values given to the parameters and the solutions of the equation. Then we apply this technique in order to obtain an irredundant parametric representation of the fixed points of a Boolean transformation $F : B^2 \longrightarrow B^2$.

Theorem 2.1. ([2], Theorem 2.9) *Suppose $ax \vee bx' = 0$ is a consistent Boolean equation, i.e., $ab = 0$. Then an element $x \in B$ satisfies the equation if and only if it is of the form*

$$x = b \vee t, \text{ where } t \leq a'b' \ , \tag{2.1}$$

in which case the element t is unique.

In other words, (2.1) is the irredundant parametric solution of the equation. By combining Theorem 2.1 with elimination of variables, one obtains an irredundant solution of a consistent Boolean equation in n unknowns. Let us do this explicitly for $n = 2$.

Proposition 2.1. *Suppose*

$$axy \vee bxy' \vee cx'y \vee dx'y' = 0 \tag{2.2}$$

is a consistent Boolean equation, i.e.., $abcd = 0$. Then a pair (x, y) satisfies (2.2) *if and only if it is of the form*

$$x = cd \vee t, \text{ where } t \leq (a' \vee b')(c' \vee d') \ , \tag{2.3.1}$$

$$y = bt \vee d(b \vee c')t' \vee u, \text{ where } u \leq a'b't \vee (c'd' \vee a'b'cd)t' \ , \tag{2.3.2}$$

in which case the pair (t, u) is unique.

Proof. Writing (2.2) in the form

$$(ax \vee cx')y \vee (bx \vee dx')y' = 0 \ , \tag{2.4.1}$$

the elimination of y yields $(ax \vee cx')(bx \vee dx') = 0$, that is,

$$abx \vee cdx' = 0 \ . \tag{2.4.2}$$

Since $ab \cdot cd = 0$, equation (2.4.2) is consistent, therefore its irredundant solution is (2.3.1) by Theorem 2.1.

In the second stage of the elimination process we introduce the solution (2.3.1) of (2.4.2) into equation (2.4.1). We have $x = cdt' \vee t$, $x' = (c' \vee d')t'$, hence

$$ax \vee cx' = at \vee acdt' \vee cd'\,t' = at \vee c(ad \vee d'\,)t' \ ,$$

$$bx \vee dx' = bcdt' \vee bt \vee c'dt' = bt \vee d(bc \vee c'\,)t' \ ,$$

hence equation (2.4.1) becomes the equation in y

$$[at \vee c(a \vee d')t']y \vee [bt \vee d(b \vee c')t']y' = 0 \ , \tag{2.4.1$'$}$$

which is consistent because of (2.4.2). By applying Theorem 2.1 to equation (2.4.1$'$) we get

$$y = bt \vee d(b \vee c'\,)t' \vee u \ ,$$

where

$$u \leq [at \vee c(a \vee d'\,)t']'\,[bt \vee d(b \vee c'\,)t']' = [a't \vee (c' \vee a'd)t']\,[b't \vee (d'\, \vee b'c)t']$$

$$= a'b't \vee (c' \vee a'd)(d' \vee b'c)t' = a'b't \vee (c'd' \vee a'b'cd)t' \ .$$

So (2.3.2) is the irredundant parametric solution of (2.4.1) by Theorem 2.1.

Therefore the elimination of variables ensures that the pair (2.3.1),(2.3.2) is a parametric solution of (2.2). If (x, y) satisfies (2.2) then x satisfies (2.4.2), hence t is uniquely determined. Then y satisfies (2.4.1$'$), hence u is uniquely determined. □

A *Boolean transformation* is a map $F : B^n \longrightarrow B^m$ of the form $F = (f_1, \ldots, f_m)$, where $f_1, \ldots, f_m : B^n \longrightarrow B$ are Boolean functions. If $m = n$ then F may have *fixed points*, that is, vectors $(x_1, \ldots, x_n) \in B^n$ such that $F(x_1, \ldots, x_n) = (x_1, \ldots, x_n)$. The possible fixed points are the solutions of the system of Boolean equations $f_i(x_1, \ldots, x_n) = x_i$ $(i = 1, \ldots, n)$, so that we can determine whether fixed points do exist and obtain an irredundant parametric representation of them. We carry out below the complete computation for $n = 2$.

Proposition 2.2. *Consider a Boolean transformation* $F = (f, g) : B^2 \longrightarrow B^2$, *where*

$$f(x,y) = axy \vee bxy' \vee cx'y \vee dx'y' \ , \tag{2.5.1}$$

$$g(x,y) = pxy \vee qxy' \vee rx'y \vee sx'y' \ . \tag{2.5.2}$$

Then F *has fixed points if and only if*

$$ap \vee bq' \vee c'r \vee d's' = 1 \ , \tag{2.6}$$

in which case

$$x = (c \vee r')(d \vee s) \vee t, \ \textit{where } t \leq (ap \vee bq')(c'r \vee d's') \ , \tag{2.7.1}$$

$$\begin{gathered} y = (b' \vee q)t \vee (d \vee s)(b' \vee q \vee c'r)t' \vee u, \ \textit{where} \\ u \leq apbq't \vee [c'rd's' \vee apbq'(c \vee r')(d \vee s)]t' \end{gathered} \tag{2.7.2}$$

is an irredundant parametric representation of the fixed points.

Proof. The fixed points are characterized by the equations $f(x,y) = x$ and $g(x,y) = y$. The equivalent equations $fx' \vee f'x = 0$ and $gy' \vee g'y = 0$ are

$$cx'y \vee dx'y' \vee a'xy \vee b'xy' = 0 \ ,$$

$$qxy' \vee sx'y' \vee p'xy \vee r'x'y = 0 \ .$$

This system is equivalent to the single equation

$$(a' \vee p')xy \vee (b' \vee q)xy' \vee (c \vee r')x'y \vee (d \vee s)x'y' = 0 \ , \tag{2.8}$$

whose consistency condition $(a' \vee p')(b' \vee q)(c \vee r')(d \vee s) = 0$ is equivalent to (2.6).

If (2.6) is fulfilled, the irredundant parametric solution of (2.8) is obtained by applying Proposition 2.1. We see that (2.3.1) and (2.3.2) reduce to (2.7.1) and (2.7.2), respectively. □

3. Classifying the transformations of $\{0,1\}^2$ by the number of their fixed points

The transformations $F : \{0,1\}^2 \longrightarrow \{0,1\}^2$ can be classified according to the number of their fixed points. In this section we provide explicit descriptions of the five classes of this partition.

We recall that

$$F(x,y) = (axy \vee bxy' \vee cx'y \vee dx'y', \, pxy \vee qxy' \vee rx'y \vee sx'y')$$

and we introduce the following shorthand of notation:

$$a' \vee p' = A, \ b' \vee q = B, \ c \vee r' = C, \ d \vee s = D \ , \tag{3.1}$$

so that the equation (2.8) of fixed points becomes

$$Axy \vee Bxy' \vee Cx'y \vee Dx'y' = 0 \tag{3.2}$$

and the consistency condition (2.6) is

$$A' \vee B' \vee C' \vee D' = 1 \ . \tag{3.3}$$

The solution (2.3) can be written

$$x = CD \vee t, \ t \leq \alpha \ , \tag{3.4.1}$$

$$\alpha = (A' \vee B')(C' \vee D') \ , \tag{3.4.1$'$}$$

$$y = Bt \vee D(B \vee C')t' \vee u, \ u \leq \beta(t) \ , \tag{3.4.2}$$

$$\beta(t) = A'B't \vee (C'D' \vee A'B'CD)t' \ . \tag{3.4.2$'$}$$

Now everything takes the values 0,1. Since the solution provided by Proposition 2.1 is irredundant, the number of fixed points equals the number of possible values of the pair (t, u). If $\alpha = 0$ then $t = 0$, while if $\alpha = 1$ then t takes both values 0 and 1. For a given t, $\beta(t) = 0$ forces $u = 0$, while u takes both values 0 and 1 if $\beta(t) = 1$.

Notation. Let $\mathcal{C}_k$ denote the class of transformations F having exactly k fixed points.

Proposition 3.1. *The class $\mathcal{C}_0$ is characterized by*

$$A = B = C = D = 1 \ .$$

Proof. This is the negation of (3.3). □

Lemma 3.1. *Equation* (3.2) *is consistent and $\alpha = 0$ if and only if $A' \vee B' = CD$. This implies $\beta(0) = A'B' \vee C'D'$.*

Proof. The first two conditions, which are $(A' \vee B') \vee (C' \vee D') = 1$ and $(A' \vee B')(C' \vee D') = 0$, express the fact that $A' \vee B'$ is the complement of $C' \vee D'$, that is, $A' \vee B' = (C' \vee D')' = CD$. This implies $A'B' \leq CD$, hence $C'D' \vee A'B'CD = C'D' \vee A'B'$. □

Proposition 3.2. *The class $\mathcal{C}_1$ is characterized by*

$$A'B' = C'D' = 0 \textit{ and } A' \vee B' = CD \ .$$

Proof. Follows by Lemma 3.1, since having a single fixed point means that the consistency condition (3.3) is fulfilled and both t and u are fixed at 0, which happens if and only if $\alpha = 0$ and $\beta(0) = 0$. □

Proposition 3.3. *The class $\mathcal{C}_2$ consists of two families of transformations, whose characteristic functions are*

$$A'B' \vee C'D' = 1 \textit{ and } A' \vee B' = CD$$

and

$$A' = B \textit{ and } C' = D \ .$$

Proof. There exist exactly two fixed points if and only if the consistency condition (3.3) is joined to the following alternative: either $t = 0$ and u is free in $\{0, 1\}$, or t is free in $\{0, 1\}$ and u is fixed to 0 no matter the value of t. This alternative is equivalent to the following one: either $\alpha = 0$ and $\beta(0) = 1$ or $\alpha = 1$ and $\beta(0) = \beta(1) = 0$.

According to Lemma 1 the first possibility is expressed by $A' \vee B' = CD$ and $A'B' \vee C'D' = 1$.

The second possibility amounts to (3.3) and $A' \vee B' = C' \vee D' = 1$ and $C'D' \vee A'B'CD = A'B' = 0$. The second condition implies (3.3) and can be written $AB \vee CD = 0$, while the last two conditions become $C'D' \vee A'B' = 0$. We have obtained $AB = A'B' = 0$ and $CD = C'D' = 0$; but $xy \vee x'y' = 0 \Longleftrightarrow x' = y$. □

Proposition 3.4. *The class $\mathcal{C}_3$ is characterized by*

$$A' \vee B' = C' \vee D' = 1 \textit{ and } A \vee B = C'D' \ .$$

Proof. It is necessary that t be free in $\{0, 1\}$, that is, $A' \vee B' = C' \vee D' = 1$. This also implies the consistency condition (3.3).

Now there are two possibilities in order to have exactly 3 fixed points: either one fixed point with $t = 0$ and 2 fixed points with $t = 1$, or 2 fixed points with $t = 0$ and one fixed point with $t = 1$. This amounts to either $\beta(0) = 0$ and $\beta(1) = 1$, or $\beta(0) = 1$ and $\beta(1) = 0$. In other words, this condition is $\beta(0) = \beta'(1)$, that is, $C'D' \vee A'B'CD = A \vee B$. But $CD = 0$ by the first condition, so the latter condition reduces to $C'D' = A \vee B$. □

Proposition 3.5. *The class $\mathcal{C}_4$ is a singleton characterized by*

$$A = B = C = D = 0\ .$$

Proof 1. There are 4 fixed points (the whole set $\{0,1\}$) iff t and u are free in $\{0,1\}$, that is, iff $\alpha = \beta(0) = \beta(1) = 1$, which implies (3.3). This amounts to

$$(A' \vee B')(C' \vee D') = C'D' \vee A'B'CD = A'B' = 1\ .$$

The last equation is equivalent to $A = B = 0$, so that it remains $C' \vee D' = C'D' \vee CD = 1$, hence $CD = 0$, therefore $C'D' = 1$, that is $C = D = 0$. □

Proof 2. Clearly the unique transformation having 4 fixed points is $F(x,y) = (x,y)$. So we have the identities

$$axy \vee bxy' \vee cx'y \vee dx'y' = x,\ pxy \vee qxy' \vee rx'y \vee sx'y' = y\ ,$$

which hold iff $a = b = 1,\ c = d = 0,\ p = r = 1,\ q = s = 0$, that is, $A = B = C = D = 0$. □

Finally let us compute the cardinalities of the five classes.

To do this we essentially come back to the old parameters $a, b, \ldots, r, s$, using (3.1). Since the parameters occurring in A, B, C, D are disjoint, we can split the discussion by giving to the new parameters A, B, C, D values 0,1 independently of each other. Taking $A = 0$ amounts to fixing the parameters a, p, while $A = 1$ summarizes 3 cases with respect to a, p; similarly for B, C, D. The technique will consist in splitting the discussion into cases and subcases until we come to small subcases in which the parameters A, B, C, D have fixed values. Each small case describes a family of transformations having 3^k members, where k is the number of parameters A, B, C, D fixed to 1. For each class we finally add the cardinalities of the families described by the small subcases corresponding to that class.

The class $\mathcal{C}_0$ requires no splitting: it has $3^4 = 81$ transformations.

The following lemma facilitates the splitting process.

Lemma 3.2. *The condition $AB = A'B' = 0$ is equivalent to $A' = B$ and there are 6 transformations satisfying this property; similarly for $CD = C'D' = 0$.*

Proof. The first claim was already noticed in the proof of Proposition 3.3. But $A' = B$ means that either $A = 1$ and $B = 0$, or $A = 0$ and $B = 1$. There are 3 transformations in each of the two variants, so there are 6 transformations satisfying $A' = B$. □

For the class $\mathcal{C}_1$ we split the discussion by CD.

If $CD = 0$ we get $A = B = 1$, which describes $3^2 = 9$ possibilities, and it remains $CD = 0$ and $C'D' = 0$, which corresponds to 6 possibilities by Lemma 3.2. Consequently there are $9 \times 6 = 54$ transformations which satisfy the case $CD = 0$.

If $CD = 1$ we get $C = D = 1$, again 9 possibilities, and $A'B' = 0,\ A' \vee B' = 1$, that is $A' = B'' = B$, again 6 possibilities by Lemma 3.2. Therefore we obtain $9 \times 6 = 54$ transformations satisfying $CD = 1$.

In conclusion $\mathcal{C}_1$ has 54 + 54 = 108 members.

For the first family of $\mathcal{C}_2$, if $CD = 0$ then $A = B = 1$, hence $C'D' = 1$, therefore $C = D = 0$; so there are 9 possibilities. If $CD = 1$ then $C = D = 1$, hence $A' \vee B' = A'B' = 1$, therefore $A = B = 0$, so that we get 9 more possibilities. So this family has 9 + 9 = 18 members.

By applying twice Lemma 3.2 we see that the second family of $\mathcal{C}_2$ has $6 \times 6 = 36$ transformations.

Therefore $\mathcal{C}_2$ has $18 + 36 = 54$ members, as was already noticed in [1].

For $\mathcal{C}_3$, if $C'D' = 0$ then $A = B = 0$ and it remains $C' \vee D' = 1$; so $C' = D$, hence 6 transformations by Lemma 3.2. If $C'D' = 1$ then $C = D = 0$ and it remains $A' \vee B' = 1$ and $A \vee B = 1$, that is, $AB = A'B' = 0$, hence another 6 transformations by Lemma 3.2. Therefore $\mathcal{C}_3$ has $6 + 6 = 12$ members.

We have thus proved:

Proposition 3.6. *The cardinalities of the classes $\mathcal{C}_0, \ldots, \mathcal{C}_4$ are given in the following table:*

$\mathcal{C}_0$	$\mathcal{C}_1$	$\mathcal{C}_2$	$\mathcal{C}_3$	$\mathcal{C}_4$
81	*108*	*54*	*12*	*1*

References

[1] H. Li, Y. Wang, Z. Liu, Existence and number of fixed points of Boolean transformations via the semi-tensor product method, *Appl. Math. Letters*, **25** (2012), 1142-1147.

[2] S. Rudeanu, *Boolean Functions and Equations*, North-Holland, Amsterdam & American Elsevier, New York, 1974.

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

(Sergiu Rudeanu) UNIVERSITY OF BUCHAREST, FACULTY OF MATHEMATICS AND INFORMATICS, STR. ACADEMIEI NR. 14, 010014 BUCHAREST, ROMANIA
E-mail address: srudeanu@yahoo.com