# **Deterministic Half Automata and Boolean Mappings**

# Adrian Atanasiu

Faculty of Math. and Comp. Sci., Bucharest University Romania

Abstract: The paper establishes a correspondence between the class of deterministic half automata with at most n states and at most p input characters, and the class of boolean mappings defined over a basic Boole algebra. In this correspondence all main properties of each concept (boolean mapping and half-automaton respectively) are preserved by the other concept.

Keywords: Boole algebra, Boolean mapping, Automata theory.

# **1. INTRODUCTION**

The concepts *half-automaton* and *boolean algebra* are used frequently in fundamental fields as theoretical supports in applications with significant impact like Algorithmic, Linguistics, Mathematical Logic, Bioinformatics, Compiler Construction, Computer Architecture and so on. These concepts are based on different ideas and are used in general in different research areas. We can only find them together in fundamentals of Computer Architecture.

Our paper establishes a strong connection between the formal description of a structure based on the boolean mappings, and the theoretical behaviour of a half-automaton, with possible extensions towards finite automata, finite translators etc.

More precisely, we show that between the class  $\mathcal{HA}(n,p)$  of deterministic half-automata with at most nstates and at most *p* input characters, and class  $\mathcal{BM}(n,p) = \{f \mid f : \mathcal{B}^{n+p} \to \mathcal{B}^n\}$  of mappings defined over a basic Boole algebra  $\mathcal{B} = \{0,1\}$ , a natural correspondence - via a numerical codification - can be established: for each deterministic half-automaton we define a boolean mapping which codifies its behaviour; and viceversa, any boolean mapping  $f \in \mathcal{BM}(n, p)$ with  $n > 0, p \ge 0$  defines at least one deterministic half-automaton. The constructions proposed in this paper are based on the normal disjunctive form of boolean mappings; for some special forms, when one or more variables can be avoided, echivalent deterministic half-automata, having а smaller complexity, can be also proposed.

The results obtained here can be used in different directions. For example, theoretical studies in domains based of one of these two concepts (half-automaton or boolean mapping respectively) can be enriched with and properties functionalities specific to the complementary concept. Or, new domains like information security can be interested by these concepts. The huge number  $\left(2^{n\cdot 2^{n+p}}\right)$ of boolean mappings from BM(n, p) suggests that the number of deterministic half-automata in  $\mathcal{HA}(n,p)$ has approximatively the same order, therefore it can be used as the basis for new encryption systems, electronic signatures or generation of session keys.

The paper contains 5 sections. Section 2 is a short presentation of the terms half-automaton and boolean mapping. Section 3 proves that for any deterministic half-automaton can be obtained – using an associated algorithm of expansion – a boolean mapping in which all functional components of this half-automaton are codified. Section 4 considers the reciprocal problem – to build at least one deterministic half-automaton for each boolean mapping  $f : \mathcal{B}^m \to \mathcal{B}^n$ . Only the  $m \ge n > 0$  case is solved, the n = 0 and 0 < m < n variants being left for a future study. Section 5 contains conclusions and directions for a later work.

# 2. PRELIMINARIES

**Definition 1.** A Deterministic Half - Automaton (DHA) is a structure  $M = (Q, V, \delta)$  where

- 1.  $Q = \{q_0, q_1, ..., q_k\}$  is a nonempty finite set of "states". By convention, we can consider that there is an integer k > 0 such that  $\forall i \in [0,k] \Rightarrow q_i \in Q$ .
- 2. *V* is a nonempty finite set called "input alphabet".
- 3.  $\delta : D \to Q$  is a "transition" mapping defined on a subset  $D \subseteq Q \times V$ .

**Remark 1**. A deterministic finite automaton  $(Q, V, \delta, q_0, F)$  is a DHA  $M = (Q, V, \delta)$  with two

Address correspondence to this author at the Faculty of Math. and Comp. Sci., Bucharest University Romania; Tel: (4-021) 314 2863; Fax: (4-021) 315 6990; E-mail: aadrian@gmail.com

additional requirements concerning Q: there are an initial state  $q_0 \in Q$ , and a nonempty set of final states  $F \subseteq Q$ .

The transition mapping can be extended to a partial defined mapping  $\delta \; : \; Q \times V^* \to Q$  by

$$\begin{array}{l} \delta(q,\epsilon)=q,\\ \delta(q,a\alpha)=\delta(\delta(q,a),\alpha), \quad \forall (q,a)\in D, \; \alpha\in V^*. \end{array}$$

where  $V^* = \{a_1 a_2 \dots a_k \mid a_i \in V, k \ge 0\}$  is the infinite set of words generated by characters from V (the case k = 0 corresponds to the empty word  $\epsilon$ ).

The DHA  $M = (Q, V, \delta)$  accepts |Q| languages<sup>1</sup>; namely

$$\forall q \in Q, \ L_q = \{ w \in V^* \mid \exists p \in Q, \ p = \delta(q, w) \}.$$

An oriented graph  $\Gamma_M$  can be attached to a half automaton  $M = (Q, V, \delta)$  as follows:

- The set of nodes is Q;
- The set of vertices is denoted by the elements of V;
- $p = \delta(q, a) \Leftrightarrow$  there is an oriented vertex denoted by a, from q to p.

In this work we consider a Boole algebra  $\mathcal{B} = \{0,1\}$  with operations

**Definition 2.** Let us consider m, n positive integers. A boolean mapping is any mapping

$$f : \mathcal{B}^m \to \mathcal{B}^n.$$

**Theorem 1.** The number of boolean mappings  $f : \mathcal{B}^m \to \mathcal{B}^n$  is  $2^{n \cdot 2^m}$ .

Regarding other issues about automata theory and boolean algebras, as well as for language-theoretic considerations not detailed here, the reader is referred to [1-4, 6, 8] and the references given therein. In the same topic, but with different results, the reader can consult also [5, 7].

# 3. THE REPRESENTATION OF DHA USING BOOLEAN MAPPINGS

In this paper we will consider only *DHA* (Deterministic Half Automata).

Let  $M = (Q, V, \delta)$  be a DHA. Using a binary codification, we can associate to M a boolean mapping

$$f_M : \{0,1\}^m \to \{0,1\}^n$$

where m, n are positive integers which will be defined later in this section.

The correspondence is established as follows:

i. For  $Q = \{q_0, q_1, ..., q_k\}$ , let *n* be the minimal positive number such that  $k \le 2^n$ . We define the codification (injective mapping)

$$\phi : Q \to \{0,1\}^n$$

defined  $\phi(q_i) = [i]_2^n$  (where  $[i]_2^n$  denotes the binary representation of the integer *i* written on *n* bits).

A similar codification is defined for the input alphabet  $V = \{a_1,...,a_s\}$ : let p be the minimal positive integer such that  $s \leq 2^p$ , and

$$\psi : V \to \{0,1\}^p$$

be defined  $\psi(a_i) = [i]_2^p$  .

**Remark 2.** If k = 1 (or s = 1) then n = 0 (respectively p = 0), and we will consider (by convention)  $\{0,1\}^0 = \{0\}$ .

ii. If at least one of codifications  $\phi, \psi$  is not oneto-one, then we will "expand" the half automaton M to another DHA (denoted M) where |Q|, |V| are powers of 2, using the next procedure:

#### Algorithm Expand

Input:  $M = (Q, V, \delta)$ .

**Output:**  $\overline{M} = (Q_1, V_1, \delta_1), |Q| = 2^n, |V| = 2^p$ .

1. If  $|Q| = 2^n, |V| = 2^p$ , then  $Q_1 = Q, V_1 = V$  exit; else

2. If  $|Q| = 2^n$  and  $|V| < 2^p$ , then  $n \leftarrow n+1$ , goto (3).

3. If  $|Q| < 2^n$ ,  $|V| \le 2^p$ , then  $2^n - |Q|$  new states  $q_{k+1}, \dots q_{2^n-1}$  will be added, and the mapping  $\phi$  will be extended in a natural way to  $Q_1 = Q \cup \{q_{k+1}, \dots, q_{2^n-1}\}$  (thus  $\phi$  becomes a surjective mapping).

If neither  $\psi$  is an one-to-one mapping, then we will

<sup>|</sup>A| denotes the number of elements of the finite set A.

add new "dummy" elements to V, until the input alphabet will have  $2^p$  elements. Let  $V_1 \supseteq V$  be the new input alphabet.

## **End Expand**

In the second phase, we will build  $\overline{M}=(Q_1,V_1,\delta_1)$ , where the mapping  $\delta_1~:~Q_1\times V_1\to Q_1$  is defined by

$$\begin{split} &\delta_1(q,a)=\,\delta(q,a),\quad \forall (q,a)\in D\,,\\ &\delta_1(q,a)=\,q_{2^n-1},\quad \forall (q,a)\in (Q_1\times V_1)\setminus D\,. \end{split}$$

**Definition 3.** The half automaton M build from M, is called the "extension" of M.

iii. For every half automaton M, a boolean mapping  $f_M : \{0,1\}^{n+p} \to \{0,1\}^n$  can be associated (eventually using the extension M):

$$f_M(\phi(x),\psi(a)) = \phi(y) \Leftrightarrow \delta_1(x,a) = y, \quad \forall x,y \in Q_1, a \in V_1.$$

Also, we shall use notation

 $Im(f_M) = \{ p \in Q_1 \mid f_M(\phi(q), \psi(a)) = \phi(p) \}.$ 

From **Algorithm Expand** the next result can be proved:

**Corollary 1.** 
$$\forall (q, w) \in Q \times V^*, \, \delta(q, w) = \delta_1(q, w).$$

\_\_\_\_\_ Therefore the behavior of extended half-automaton  $\overline{M}$  restricted to the set Q of states and the input alphabet V is identical with the behavior of the deterministic half-automaton M. This extension of M to  $\overline{M}$  is necessary because the number of entries of a boolean mapping is a power of 2.

**Example 1.** Let  $M = (\{q_0, q_1, q_2\}, \{a, b, c\}, \delta)$  be a DHA with



Because  $|Q| \models |V| = 3 < 2^2$ , we will add a new state  $q_3$  and a dummy character d. The new DHA is  $\overline{M} = (\{q_0, q_1, q_2, q_3\}, \{a, b, c, d\}, \delta_1)$ , where



$$\frac{q}{\phi(q)} \frac{q_0}{00} \frac{q_1}{01} \frac{q_2}{10} \frac{q_3}{10} \qquad \frac{x}{\psi(x)} \frac{a}{00} \frac{b}{01} \frac{c}{10} \frac{d}{10}$$
(1)

A boolean mapping (constructed with these definitions for  $\phi$  and  $\psi$ ) is

$$f_M : \{0,1\}^4 \to \{0,1\}^2$$

defined as follows:

A simplified analytic form of this mapping is (where notation  $\phi(x) = x_1 x_2$ ,  $\psi(a) = y_1 y_2$  is used):

$$\begin{array}{l} f_{M}(x_{1},x_{2},y_{1},y_{2})=(x_{1}y_{2}+y_{1}y_{2}+x_{1}y_{1}y_{2}+x_{1}x_{2}y_{1}+x_{2}y_{1}y_{2},\\ \overline{x_{2}y_{1}y_{2}},x_{1}x_{2}+x_{2}y_{1}+y_{1}y_{2}+x_{2}y_{1}y_{2}) \end{array}$$

**Example 2.** (A justification of step 2 in Algorithm Expand)

Let us consider  $M = (\{q_0, q_1\}, \{a, b, c\}, \delta)$  with



Because  $|V| = 3 < 2^2$ , a dummy character ' d ' must be added in V. But all states of Q are already

used; if we set  $\delta_1(q_i,d) \in \{q_0,q_1\}$ , new words will be accepted by M, having character ' d ' included.

Therefore at least a new state would be necessary. But |Q|=2; so, we have to add new states until the next power of 2 is reached by |Q|:  $Q_1 = \{q_0, q_1, q_2, q_3\}$ .

The new transition mapping is:



The boolean mapping associated is (with the same notations from (1)):

$\phi(x)$	$0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1 \ $
	$0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0 \ $
$\psi(a)$	$0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ $
	$0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1$
$f_M(\phi(x),\psi(a))$	$0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1 \ $
	0101101111111111

with a reduced analytic form (of course, this is only a variant obtained from the normal disjunctive form showed by the table above):

$$f_M(x_1, x_2, y_1, y_2) = (x_1 + y_1 y_2, x_1 + x_2 y_1 + x_2 \overline{y}_2).$$

**Theorem 2.** The boolean mapping  $f_M$  defines at most two *DHAs*.

**Proof.** Let us consider a boolean mapping  $f_M : \{0,1\}^m \to \{0,1\}^n, \ m \ge n \ge 1$ .

- First of all, it defines a  $\mathit{DHA}\ M_1 = (\mathit{Q}_1, \mathit{V}_1, \delta_1)$  where:

 $Q_1 = \mathit{Im}(f_M) = \{q_i \mid 0 \leq i \leq 2^n - 1\}, \quad V_1 = \{a_i \mid 0 \leq i \leq 2^{m-n} - 1\}$  and

$$\delta_1(q, a) = \{ p \mid f_M(\phi(q), \psi(a)) = \phi(p) \}.$$

(Obviously  $\forall (q,a) \in Q_1 \times V_1$ ,  $\mid \delta_1(q,a) \mid = 1$ .)

- Second, if  $\forall a \in V_1, f_M(\underline{11...1}_n, \psi(a)) = \underline{11...1}_n$ , then a new  $DHA \ M_2 = (Q_2, V_2, \delta_2)$  can be found, with  $M_2 = M_1$  Namely:

$$Q_{2} = Q_{1} \setminus \{q \mid \delta_{1}(q, a) = q_{2^{n}-1}, \forall a \in V_{1}\}, \\ V_{2} = \{a \in V_{1} \mid \exists q \in Q_{2}, f_{M}(\phi(q), \psi(a)) \in Q_{2}\}, \\ \delta_{2}(q, a) = \delta_{1}(q, a), \forall (q, a) \in Q_{2} \times V_{2}.$$

**Remark.3** In fact a boolean mapping  $f_M$  does not offer in the DHA (associated above) the real form of characters from the input alphabet V; only a codification  $\{a_1, a_2, \ldots\}$  can be delivered. The reader can replace these formal characters with its own letters.

#### 4. BOOLEAN MAPPINGS DESCRIBED BY DHAs

Let us consider now the reciprocal problem: if

 $f : \{0,1\}^m \to \{0,1\}^n, \ m \ge n > 0$ 

is a boolean mapping, there exists a *DHA* which conserves its characteristics ?

Two cases may arise:

**4.1. THE CASE** m > n > 0:

Theorem 3. Let

 $f : \{0,1\}^m \to \{0,1\}^n, \quad m > n > 0$ 

be a boolean mapping. Then there is a  $DHA \quad M = (Q, V, \delta)$  with  $f = f_M$ .

**Proof.** The proof is similar with proof of Theorem 2. We define the *DHA*  $M = (Q, V, \delta)$  as following:

$$-Q = \{q_i \mid 0 \le i \le 2^n - 1\}$$
; Therefore  $\phi(q_i) = [i]_2^n$ ;

$$-V = \{a_i \mid 0 \le i \le 2^{m-n} - 1; \text{ Therefore } \psi(a_i) = [i]_2^{m-n}; \}$$

$$-\forall (\boldsymbol{q}_i, \boldsymbol{a}_j) \in Q \times V \Rightarrow \delta(\boldsymbol{q}_i, \boldsymbol{a}_j) = \phi^{-1}(f(\phi(\boldsymbol{q}_i), \psi(\boldsymbol{a}_j))) + (\boldsymbol{q}_i, \boldsymbol{q}_j) = \phi^{-1}(f(\phi(\boldsymbol{q}_i), \psi(\boldsymbol{a}_j))) = \phi^{-1}(f(\phi(\boldsymbol{q}_i), \psi(\boldsymbol{a}_j))) = \phi^{-1}(f(\phi(\boldsymbol{q}_i), \psi(\boldsymbol{a}_j)) = \phi^{-1}(f(\phi(\boldsymbol{q}_i), \psi(\boldsymbol{a}_j)) = \phi^{-1}(f(\phi(\boldsymbol{q}_i), \psi(\boldsymbol{a}_j))) = \phi^{-1}(f(\phi(\boldsymbol{q}_i), \psi(\boldsymbol{a}_j)) = \phi^{-1}(f(\phi(\boldsymbol{q}_i), \psi(\boldsymbol{a}_j)) = \phi^{-1}(f(\phi(\boldsymbol{q}_i), \psi(\boldsymbol{a}_j))) = \phi^{-1}(f(\phi(\boldsymbol{q}_i), \psi(\boldsymbol{a}_j)) = \phi^{-1}(f(\phi(\boldsymbol{q}_j), \psi(\boldsymbol{a}_j)) = \phi^{-1}$$

The mapping  $\phi$  is one-to-one, therefore  $\phi^{-1}$  is well defined by  $\phi^{-1}([r]_2^m) = q_r$ .

It is easy to prove that  $M = (Q, V, \delta)$  is a *DHA* which corresponds to all requirements.

**Example 3.** Let  $n \ge 2$  be an integer. There are  $2^{2^n}$  boolean mappings  $f : \{0,1\}^n \to \{0,1\}$ ; therefore there are  $2^{2^n}$  deterministic half automata  $M = (Q, V, \delta)$ , where  $|Q| = 2^{n-1}, V = \{a, b\}$ .

In particular, for n = 2 there are 16 boolean mappings, summarized below:

 $\phi(q)$   $\psi(x)$  (1) (2) (3) (4) (5) (6) (7) (8) (9) (10) (11) (12) (13) (14) (15) (16) 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 1 0 0 0 0 1 1 1 1 0 0 0 0 1 0 1  $0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0$ 1

From the proof of Theorem 3 it results  $\phi^{-1}(0) = q_0, \phi^{-1}(1) = q_1, \psi^{-1}(0) = a, \psi^{-1}(1) = b$ .

Besides, we shall denote  $L_i^j$  the language  $L_{q_i}$  (i = 0,1) generated by boolean function (j)  $(1 \le j \le 16)$  from the table above, and we shall represent these languages using regular expressions [2, 4].

#### 4.2. The Case m = n :

If  $\epsilon$  -moves ( $\delta(q,\epsilon) = p$  for some  $p,q \in Q$ ) are accepted in a DHA, then the construction proposed above can be applied also to boolean mappings with m = n > 0.

#### Theorem 4. Let

$$f : \{0,1\}^n \to \{0,1\}^n$$

be a boolean mapping.

Then there exists a DHA  $M = (Q, V, \delta)$  where  $V = \phi$  and  $f = f_M$ .

Inverse, any deterministic half automaton  $M = (Q, V, \delta)$  with  $V = \phi$ , is completely defined by a boolean mapping  $f_M : \{0,1\}^n \to \{0,1\}^n$  (where n is a positive integer).

**Proof**. Like in Proof of the Theorem 2, we define the  $DHA \quad M = (Q, V, \delta)$  as follows:

- 1.  $Q = \{q_i \mid 0 \le i \le 2^n 1\};$ 2.  $V = \phi;$
- **3**.  $\delta(q_i, \epsilon) = q_i \quad \Leftrightarrow \quad f([i]_2^n) = [j]_2^n$ .

The theorem is now easy to be proved.

Inverse, for a fixed *DHA M* , we can build *n* and  $\phi$  like in Section 3. Then the boolean mapping  $f_M$  will be defined as follows:

$$\forall q,p \in Q \Big[ f_{\!M}(\phi(q)) = \phi(p) \quad \Leftrightarrow \quad \delta(q,\epsilon) = p \, \Big].$$

Because the input alphabet is empty, the codification mapping  $\psi$  is not necessary.

Therefore  $f_{\!M}$  offers the same information like the  $DHA\ M$  .

**Example 4.** Let us consider n = 1. There are 4 boolean mappings  $f : \{0,1\} \rightarrow \{0,1\}$ , listed in the table

q	(1)	(2)	(3)	(4)
0	0	0	1	1
1	0	1	0	1

The *DHA* s associated for each such mapping are:



and the boolean mappings associated are

$$f_1(x) = 0, \quad f_2(x) = x, \quad f_3(x) = \overline{x}, \quad f_4(x) = 1$$
  
Obviously,  $L_0^i = L_1^i = \{\epsilon\}, 1 \le i \le 4$ 

A study of the case m < n is more difficult, a different abbordation being necessary. This variant will be developped in another future paper.

## 5. FINAL REMARKS

The paper establishes a correspondence between the class of deterministic half automata with at most nstates and at most p input characters, and class of boolean mappings defined over a basic Boole algebra. In this correspondence all main properties of each concept (boolean mapping and half-automaton respectively) are preserved – in codified form by – the other one.

The results obtained here can be used as a start for solving an important problem in automata theory: how many non-echivalent deterministic half-automata with n states and p input characters can be defined? The correspondence with boolean mappings and the fact that their number is known can be a first step in this study.

Also, some cases in this relation (*DHA* versus boolean mapping) are not dealt with: how can be constructed half-automata which preserve properties of mappings  $f : \mathcal{B}^m \to \mathcal{B}^n$  when n = 0 or 0 < m < n? The answer is important and we leave this work for another paper.

#### REFERENCES

- Givant S, Halmos P. Introduction to Boolean Algebras, Undergraduate Texts in Mathematics, Springer. Verlag, 2009.
- [2] Hopcroft JE, Motwani R, Ullman JD. Introduction to Automata Theory, Languages, and Computation (2 ed.). Addison Wesley, 2001.
- [3] Koppelberg S. General Theory of Boolean Algebras. Handbook of Boolean Algebras, Vol. 1 (ed. J. Donald Monk with Robert Bonnet). Amsterdam: North Holland, 1989.
- [4] Lawson MV. Finite automata, Chapman and Hall/CRC, 2004.
- [5] Leiss E. Succinct representation of regular languages by boolean automata, Theoretical Computer Science, Volume 13, 3, pp. 323-330, 1981.
- [6] Parkes A. Introduction to languages, machines and logic: computable languages, abstract machines and formal logic. Springer Verlag, 2002.
- [7] Stankovic R, Astola J. From Boolean Logic to Awitching Circuits and Automata: Towards Modern Infrormation Technology, Springer Verlag, 2011
- [8] Steven R, Givant Paul, Halmos R. Introduction to Boolean algebras, Springer Verlag, 2009.

Received on 3-12-2014

Accepted on 11-12-2014

Published on 12-1-2015

http://dx.doi.org/10.15379/2410-2938.2014.01.01.05

© 2014 Adrian Atanasiu; Licensee Cosmos Scholars Publishing House.

This is an open access article licensed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.org/licenses/by-nc/3.0/), which permits unrestricted, non-commercial use, distribution and reproduction in any medium, provided the work is properly cited.