



ISSN 1823-626X

Malaysian Journal of Fundamental and Applied Sciences

available online at <http://mjfas.ibnusina.utm.my>



Permutation Groups in Automata Diagrams

Gan Yee Siang^{1*}, Fong Wan Heng², Nor Haniza Sarmin¹ and Sherzod Turaev³

¹Department of Mathematical Sciences, Faculty of Science, Universiti Teknologi Malaysia, 81310 UTM Johor Bahru, Johor, Malaysia

²Ibnu Sina Institute for Fundamental Science Studies, Universiti Teknologi Malaysia, 81310 UTM Johor Bahru, Johor, Malaysia

³Department of Computer Science, Kulliyah of Information and Communication Technology, International Islamic University Malaysia, 50728 Kuala Lumpur, Malaysia

Received 10 December 2012, Revised 9 February 2013, Accepted 17 February 2013, Available online 25 February 2013

ABSTRACT

Automata act as classical models for recognition devices. From the previous researches, the classical models of automata have been used to scan strings and to determine the types of languages a string belongs to. In the study of automata and group theory, it has been found that the properties of a group can be recognized by the automata using the automata diagrams. There are two types of automata used to study the properties of a group, namely *modified finite automata* and *modified Watson-Crick finite automata*. Thus, in this paper, automata diagrams are constructed to recognize permutation groups using the data given by the Cayley table. Thus, the properties of permutation group are analyzed using the automaton diagram that has been constructed. Moreover, some theorems for the properties of permutation group in term of automata are also given in this paper.

| Finite automata | Watson-Crick finite automata | Cayley table | Permutation group | Automata diagram |

© 2013 Ibnu Sina Institute. All rights reserved.
<http://dx.doi.org/10.11113/mjfas.v9n1.79>

1. INTRODUCTION

Since finite automata were first studied by Kleene in 1950 [1], finite automata theory have been widely used in the theories and applications of computer science and mathematics [2, 3]. Mainly, finite automata are considered as recognition devices for the strings of formal languages.

A classic model of automaton consists of a finite set of states, an input alphabet (a finite set of symbols), a transition function, the initial state and a finite set of final states. However, the “classic” automata have the limitation of computational power as they can recognize only the regular languages [3]. Therefore, many types of finite automata have been developed to overcome this limitation. A new variant of finite automata with two reading heads and two input tapes that has been developed based on the concept of the classical model of finite automata, called Watson-Crick finite automata, for the recognition of double stranded strings which are the abstractions of DNA molecules [4].

In our previous papers [5, 6], we have studied various properties of groups using finite automata and Watson-Crick finite automata. In particular, we have shown that the data given in the Cayley tables of Abelian groups can be recognized by both types of automata.

We have found that some properties of Abelian groups can also be obtained from automata transition diagrams. In this paper, we investigate the recognisability of the permutation groups by finite automata and Watson-Crick finite automata.

Moreover, we analyse some properties of permutation groups using *modified deterministic finite automata* over permutation groups and *modified Watson-Crick finite automata* over permutation groups. In addition, we present an example of a finite automaton (the transition diagram) which recognizes the permutation group of the symmetric group of order six, S_3 .

The paper is organized as follows: in Section 2 we recall some basic definitions and notations which are used in sequence. We introduce the modified versions of deterministic finite automata and Watson-Crick finite automata over permutation groups in Section 3. We show that several properties of permutation groups can be analysed using modified deterministic finite automata and modified Watson-Crick finite automata in Section 4. Finally, we summarize our results in Section 5.

2. PRELIMINARIES

We assume that the readers are familiar with the basic concepts of formal language theory and group theory. For further information, readers can refer to [7-9] for formal language theory and [10-12] for group theory.

Definition 1 ([1])

A *deterministic finite automaton* is defined by

$$M = (Q, \Sigma, \delta, q_0, F),$$

where,

*Corresponding author. E-mail: ysgn88@gmail.com
 (Gan Yee Siang) Tel:(60)-17-6284348

- Q is a finite set of internal states,
- Σ is a finite set of symbols called an input alphabet,
- $q_0 \in Q$ is the initial state,
- $F \subseteq Q$ is a set of final states,
- $\delta: Q \times \Sigma \rightarrow Q$ is a transition function.

Definition 2 ([13])

A *Watson-Crick finite automaton* is a 6-tuple

$$M = (Q, \rho, \Sigma, s_0, F, \delta)$$

where,

- Σ is an alphabet,
- Q is a set of internal states,
- $\rho \subseteq \Sigma \times \Sigma$ is a symmetric relation (the complementarity relation),
- $s_0 \in Q$ is the initial state,
- $F \subseteq Q$ is a set of final states,
- $\delta: Q \times (\Sigma, \Sigma) \rightarrow 2^Q$ is a transition function such that $(s, (x, y)) \neq \emptyset$ only for finitely many triples $(s, x, y) \in Q \times \Sigma \times \Sigma$.

Definition 3 ([7])

A *transition diagram* is a diagram with a finite number of vertices and arrows for the edges between two vertices, such that vertices represent the states, the arrows represent the transition functions and the labels on the edges are current values of the input symbol.

Definition 4 ([7])

A string is said to be *accepted* by an automaton if the automaton is in one of its final states when the end of the string is reached. For the string which is not accepted by automaton then it is said to be rejected.

Next, we cite the definitions of modified deterministic finite automata and Watson-Crick finite automata over Abelian groups, and explain the recognition of permutation groups by these types of automata in examples.

Definition 5 ([6])

Let G be an Abelian group. A *modified deterministic finite automaton over G* are defined as

$$M = (Q, \Sigma, G, q_0, F, \delta),$$

where,

- $Q \subseteq G$ is a finite set of internal states,
- $\Sigma \subseteq G$ is a finite set of symbols called an input alphabet,
- $q_0 \in Q$ is the initial state,
- $F \subseteq Q$ is a set of final states,

- $\delta: Q \times \Sigma \rightarrow Q$ is a transition function such that with the Cartesian product of Q and Σ , a binary operation “*” of the group is associated.

Definition 6 ([6])

Let G be an Abelian group. A *modified Watson-Crick finite automaton over G* are defined as

$$M = (Q, \Sigma, \rho, G, s_0, F, \delta),$$

where,

- $Q \subseteq G$ is a finite set of internal states,
- $\Sigma \subseteq G$ is an input alphabet,
- $\rho \subseteq \Sigma \times \Sigma$ is the complementarity relation,
- $s_0 \in Q$ is the initial state,
- $F \subseteq Q$ is a set of final states,
- $\delta: Q \times (\Sigma, \Sigma) \rightarrow Q$ is a transition function such that with the Cartesian product of Q and (Σ, Σ) , a binary operation “*” of the group is associated.

For the Cayley table, all data of the group are written in the table. So, a group is said to be *accepted* by an automaton if the Cayley table of the group is recognized by the automaton.

In the following examples, we construct the automata diagrams of a modified finite automaton and modified Watson-Crick finite automaton over Abelian groups, which recognize the Abelian group of \mathbb{Z}_2 and the direct product of Abelian group $\mathbb{Z}_1 \times \mathbb{Z}_4$ respectively.

Example 1

For the group $\mathbb{Z}_2 = \{0, 1\}$, its Cayley table is illustrated in Table 1.

Table 1. Cayley table for \mathbb{Z}_2

+	0	1
0	0	1
1	1	0

Then, the group \mathbb{Z}_2 can be recognized by an automaton whose transition diagram is shown in Fig. 1.

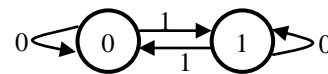


Fig. 1. A transition diagram of the automaton for \mathbb{Z}_2

Example 2

Given a group $\langle \mathbb{Z}_1 \times \mathbb{Z}_4, + \rangle$ where

$$\mathbb{Z}_1 \times \mathbb{Z}_4 = \{0\} \times \{0, 1, 2, 3\}.$$

Then, $\mathbb{Z}_1 \times \mathbb{Z}_4 = \{(0, 0), (0, 1), (0, 2), (0, 3)\}$ and the Cayley table of $\mathbb{Z}_1 \times \mathbb{Z}_4$ is shown in Table 2.

Table 2. Cayley table for $\mathbb{Z}_1 \times \mathbb{Z}_4$

+	(0,0)	(0,1)	(0,2)	(0,3)
(0,0)	(0,0)	(0,1)	(0,2)	(0,3)
(0,1)	(0,1)	(0,2)	(0,3)	(0,0)
(0,2)	(0,2)	(0,3)	(0,0)	(0,1)
(0,3)	(0,3)	(0,0)	(0,1)	(0,2)

Using the Cayley table, we can construct an automaton recognizing the group. The transition diagram is shown in Fig. 2.

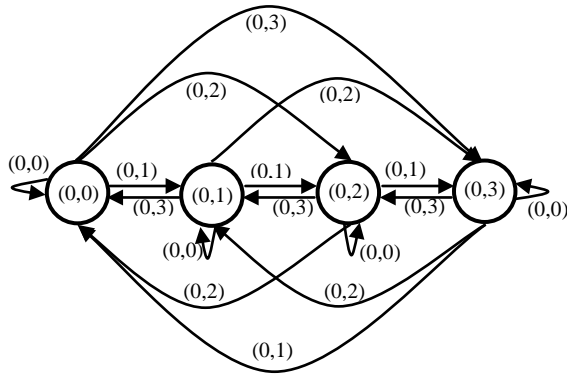


Fig. 2. A transition diagram of the automaton for $\mathbb{Z}_1 \times \mathbb{Z}_4$.

3. AUTOMATA DIAGRAMS FOR PERMUTATION GROUPS

Before we relate automata to permutation groups, we give the definition of a permutation group.

Definition 7 ([10])

Given a non-empty set X ; a permutation of X is a bijection $\alpha: X \rightarrow X$. The set S_X of all permutation of X under the composition of mappings is called *permutation group*.

Next, we define modified versions of finite automata and Watson-Crick finite automata which recognize permutation groups.

Definition 8

Let P be permutation group. A *modified deterministic finite automaton over P* is defined as

$$M = (Q, \Sigma, P, q_0, F, \delta),$$

where,

- $Q \subseteq P$ is a finite set of internal states,

- $\Sigma \subseteq P$ is a finite set of symbols called an input alphabet,
- $q_0 \in Q$ is the initial state,
- $F \subseteq Q$ is a set of final states,
- $\delta: Q \times \Sigma \rightarrow Q$ is a transition function such that with the Cartesian product of Q and Σ , a binary operation “ \circ ” (the compositions of maps) of the group is associated.

It immediately follows that for any permutation group, one can easily construct a modified deterministic finite automaton which accepts the permutation group. As an example, we construct the transition diagram of an automaton accepting the permutation group S_3 .

Example 3

Given a finite set $A = \{1, 2, 3\}$. The group of all permutations of A is denoted by S_3 . Thus,

$$S_3 = \{(1), (123), (132), (23), (13), (12)\}.$$

For short, we denote the permutation group S_3 by

$$S_3 = \{\rho_0, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}.$$

The Cayley table for S_3 is shown in Table 3. Thus, we can construct the transition diagram of an automaton for the permutation group of S_3 based on the Cayley table as illustrated in Fig. 3.

For the direct product of permutation groups we can also construct a modified variant of Watson-Crick finite automata which recognizes the direct product of permutation groups.

Definition 9

Let P be a permutation group. A *modified Watson-Crick finite automaton over P* is defined as

$$M = (\Sigma, \rho, Q, P, s_0, F, \delta),$$

where,

- $\Sigma \subseteq P$ is an input alphabet,
- $\rho \subseteq \Sigma \times \Sigma$ is the complementarity relation,
- $Q \subseteq \rho$ is a finite set of internal states,
- $s_0 \in Q$ is the initial state,
- $F \subseteq Q$ is a set of final states,
- $\delta: Q \times (\Sigma, \Sigma) \rightarrow Q$ is a transition function such that with the Cartesian product of Q and (Σ, Σ) , a binary operation “ \circ ” of the group is associated.

The recognition of modified Watson-Crick automaton is illustrated in Fig. 4 for $S_2 \times S_2$.

Example 4

Given the direct product of permutation groups $S_2 \times S_2$, such that

$$S_2 \times S_2 = \{((1), (1)), ((1), (12)), ((12), (1)), ((12), (12))\}.$$

The Cayley table for $S_2 \times S_2$ is shown in Table 4. The transition diagram of an automaton for $S_2 \times S_2$ is shown in Fig. 4.

Table 3. Cayley table for permutation group S_3

\circ	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

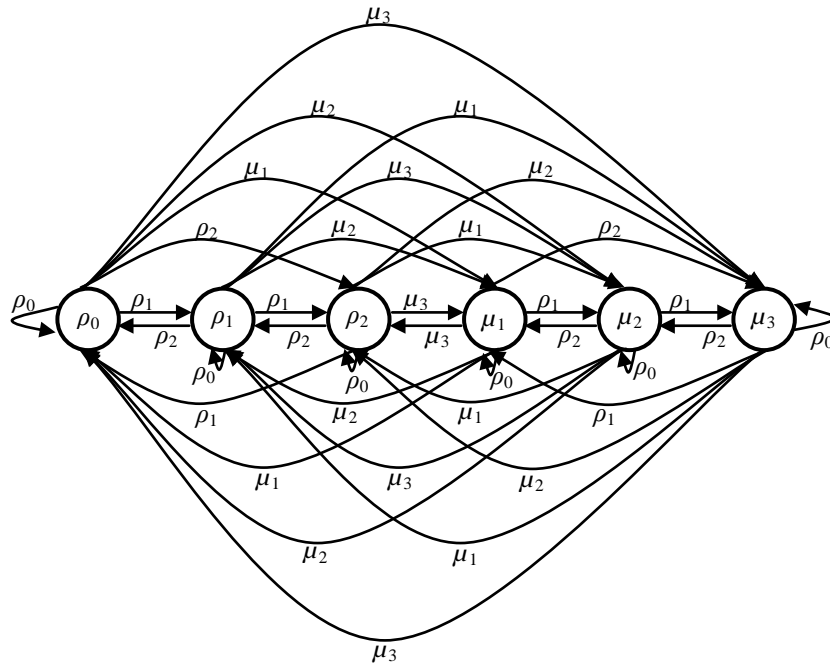


Fig. 3. Automaton diagram for permutation group of S_3 .

Table 4. Cayley table for permutation group $S_2 \times S_2$

\circ	$((1), (1))$	$((1), (12))$	$((12), (1))$	$((12), (12))$
$((1), (1))$	$((1), (1))$	$((1), (12))$	$((12), (1))$	$((12), (12))$
$((1), (12))$	$((1), (12))$	$((1), (1))$	$((12), (12))$	$((12), (1))$
$((12), (1))$	$((12), (1))$	$((12), (12))$	$((1), (1))$	$((1), (12))$
$((12), (12))$	$((12), (12))$	$((12), (1))$	$((1), (12))$	$((1), (1))$

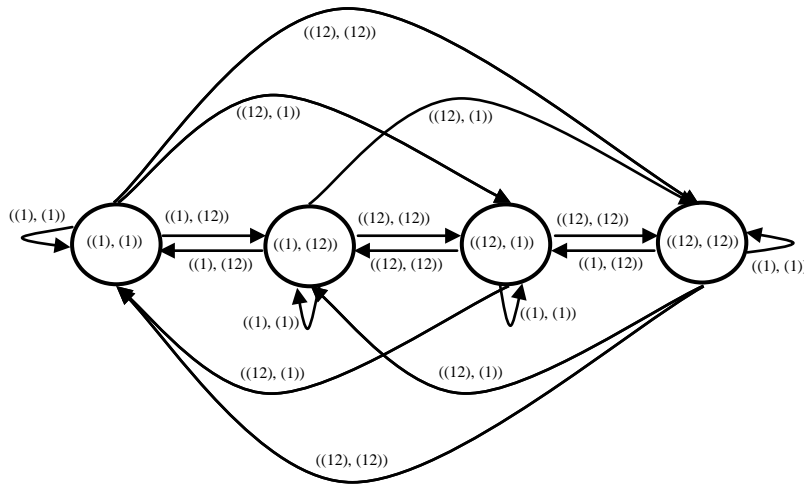


Fig. 4. The transition diagram of an automaton for permutation group $S_2 \times S_2$

Again, it is easy to show that for each direct product of two permutation groups, one can construct a modified Watson-Crick automaton over a permutation group for the direct product of permutation groups. Moreover, we can analyse some properties of permutation groups using the transition diagrams of the corresponding automata.

4. SOME PROPERTIES OF PERMUTATION GROUPS IN TERMS OF AUTOMATA

In this section, we show that several properties of permutation groups can be expressed in terms of properties of the transition diagrams, for the corresponding modified finite automata.

Lemma 1

For a modified deterministic finite automaton over a permutation group P , the element assigned to a transition is the identity element of the permutation group if and only if the transition is a self-loop transition of a state, i.e., a transition $e_{ij} = (a_i, a_j)$ is labelled by the identity element if and only if $a_i = a_j$ for some $a_i, a_j \in P$.

Proof. Let b be an element of the group P associated with the transition e_{ij} from node a_i to node a_j such that

$$b \in \{b_k : \delta(a_i, b_k) = a_j, \text{ for all } a_i, a_j \in Q \text{ and } b_k \in \Sigma\}.$$

By construction, if $\delta(a_i, b_k) = a_j$ then $a_j = a_i \circ b_k$. Thus, $b_k = a_i^{-1} \circ a_j$. Suppose that $a_i = a_j$, then $b_k = a_j^{-1} \circ a_j$ and we can easily conclude that $a_j^{-1} \circ a_j$ is the identity element of the permutation group P . Therefore, b is the identity element associated with e_{ij} .

Conversely, suppose that the label of the transition from node a_i to node a_j is the identity element b of the permutation group. By definition, $\delta(a_i, b) = a_j$. On the other hand, $a_i \circ b = a_j$. Since b is the identity element, $a_i \circ b = a_i$, it follows that $a_j = a_i$, correspondingly, $\delta(a_i, b) = a_i$. \square

Lemma 2

For a modified deterministic finite automaton M over a permutation group P , if the transition is not self-loop, then the element associated with the transition from node $a_i \in Q$ to $a_j \in Q$ is the inverse of the element associated with transition from node $a_j \in Q$ to $a_i \in Q$, i.e., if $e_{ij} = (a_i, a_j)$ is labelled by $b \in P$ then $e_{ji} = (a_j, a_i)$ is labelled by b^{-1} .

Proof. Suppose that a transition $e_{ij} = (a_i, a_j)$ is not self-loop ($i \neq j$), then there is an element b_1 such that $\delta(a_i, b_1) = a_j$. By definition,

$$a_i \circ b_1 = a_j. \tag{1}$$

On the other hand, for the transition $e_{ji} = (a_j, a_i)$, there is an element b_2 such that $\delta(a_j, b_2) = a_i$. By definition,

$$a_j \circ b_2 = a_i. \tag{2}$$

Substitute (2) into (1),

$$(a_j \circ b_2) \circ b_1 = a_j.$$

By the group associativity law,

$$a_j \circ (b_2 \circ b_1) = a_j.$$

By cancellation law,

$$(a_j)^{-1} \circ a_j \circ (b_2 \circ b_1) = (a_j)^{-1} \circ a_j.$$

Thus, $b_2 \circ b_1$ is the identity element, i.e., $(b_2)^{-1} = b_1$. The identity of $b_1 \circ b_2$ can also be shown by using similar arguments. \square

Theorem 1

If P is a permutation group of n elements, then P is recognized by a modified deterministic finite automaton M with $n!$ states and $(n!)^2$ transitions.

Proof. Let P be a permutation group of n elements. Then $|P| = n!$. Let M be a modified deterministic finite automaton

accepting P . By Definition 8, M also has $n!$ states. For each state a_i of M , there is one self-loop transition by Lemma 1, one outgoing transition to each state a_j with $i \neq j$ and one incoming transition from each state a_j with $i \neq j$ by Lemma 2. Then the total number of transitions is

$$|Q| \times |Q| = |P| \times |P| = (n!) \times (n!) = (n!)^2. \quad \square$$

The similar relationships between the direct products of permutation groups and modified Watson-Crick finite automata over permutation groups can be obtained by using the same arguments of the proofs of Lemmas 1, 2 and Theorem 1.

Lemma 3

For a modified Watson-Crick finite automaton over a permutation group $P_1 \times P_2$, the element assigned to a transition is the identity element of the direct product $P_1 \times P_2$ if and only if the transition is a self-loop transition of a state, i.e., a transition $e_{ij} = (a_i, a_j)$ is labelled by the identity element if and only if $a_i = a_j$ for some $a_i, a_j \in P_1 \times P_2$. \square

Lemma 4

For a modified Watson-Crick finite automaton M over a permutation group $P_1 \times P_2$, if the transition is not self-loop, then the element associated with the transition from node $a_i \in Q$ to $a_j \in Q$ is the inverse of the element associated with transition from $a_j \in Q$ to node $a_i \in Q$, i.e., if $e_{ij} = (a_i, a_j)$ is labelled by $b \in P$ then $e_{ji} = (a_j, a_i)$ is labelled by b^{-1} . \square

Theorem 2

A permutation group $P_1 \times P_2$ with $|P_1| = n!$, $|P_2| = m!$ is recognized by a modified Watson-Crick finite automata with $(n!)(m!)$ states and $((n!)(m!))^2$ transitions. \square

5. CONCLUSIONS

In this research, the relation between the Cayley tables of permutation groups and finite automata is studied. A modified version of deterministic finite automata and modified Watson-Crick finite automata are defined and the relations are explained in examples. It is also shown that permutation groups and the direct products of permutation groups can be simulated by deterministic finite automata and Watson-Crick finite automata if the set of states and the alphabet of an automaton are defined as subsets of a permutation group. Since this paper is one of the preliminary works in this direction there are many open questions and a lot of interesting topics for future research:

- From Theorems 1 and 2 one can notice that the descriptonal complexities of automata are not optimal. Thus, it is interesting to check the possibility of

minimizing the number of states and transitions of automata constructed in Theorems 1 and 2.

- Since this work shows that permutation groups are simulated by modified automata, it is of interest to investigate the properties of permutation groups using automata.
- It is also interesting to generalize the ideas considered in this paper and papers [4, 5] for any type of finite groups, and to show the possibility of the construction of finite automata accepting finite groups.
- The introduction of “group related automata” is also interesting in formal language theory: we can define the families of languages accepted by group which are related to automata and investigate their properties.

ACKNOWLEDGEMENTS

The first author would like to thank the Ministry of Higher Education Malaysia for the financial funding support through MyBrain15 scholarship. The second and third authors would like to thank the Ministry of Higher Education (MOHE) and Research Management Centre (RMC), UTM for the financial funding through Research University Fund Vote No. 05J15.

REFERENCES

- [1] M. V. Lawson. Finite Automata. A CRC press company, New York, 2003.
- [2] M. Maxim, Algorithms, Languages, Automata and Compilers, Jones and Bartlett Publishers, USA, 2010.
- [3] C. Martin-Vide, V. Mitrană and Gh. Păun, Formal Languages and Applications, Springer-Verlag, Berlin, 2004.
- [4] E. Czeizler, L. Kari and A. Salomaa. Theoretical Computer Science 410 (2009), 3250-3260.
- [5] Y. S. Gan, W.H. Fong, N.H. Sarmin and S. Turaev. Malaysian Journal of Fundamental and Applied Sciences, 8(1) (2012), 24-30.
- [6] Y. S. Gan, W.H. Fong, N.H. Sarmin and S. Turaev. American Institute of Physics (AIP), 2012. To appear.
- [7] P. Linz, An Introduction to Formal Languages and Automata, Jones and Bartlett Publishers, USA, 2006.
- [8] J. C. Martin. Introduction to Languages and the Theory of Computation. McGraw-Hill Companies Inc., New York, 2003.
- [9] A. T. Sudkamp, Languages and Machines, Addison Wesley Longman, Inc., USA, 1998.
- [10] L. Walter and J.W. Alan, Introduction to Group Theory, Addison Wesley Longman, USA, 1996.
- [11] C. Predrag. Group Theory, Princeton University Press, USA, 2008.
- [12] M. John. Groups, Graphs and Trees: An Introduction to the geometry of Infinite Groups, University Press, Cambridge, 2008.
- [13] G. Paun, G. Rozenberg, A. Salomaa. DNA Computing. Springer-Verlag Berlin Heidelberg, New York. 1998.