数理解析研究所講究録
第 1809 巻 2012 年 119-127

Algebraic Structure Theory of Automata

Masami Ito
Faculty of Science, Kyoto Sangyo University
Kyoto 603-8555, Japan
e-mail ito@cc kyoto-su ac jp

Abstract

The present paper is a survey article on algebraic structures of automata In the first part, we consider representations of strongly connected automata and in the second part, first we define the layers of an automaton Then we deal with the poset of subautomata of an automaton and we consider the class of single bottom automata, and we provide the composition of a single loop automaton and a strongly connected automaton together with its automorphism group

keywords: automaton, strongly connected automaton, automorphism group of an automaton, layer of an automaton, group-matrix type automaton, poset, subautomaton, semilattice, single bottom automaton, decomposition of an automaton, composition of automata

1 Introduction

Let X be a nonempty finite set, called an *alphabet* An element of X is called a *letter* By X^*, we denote the free monoid generated by X Let $X^+ = X^* \setminus \{\epsilon\}$ where ϵ denotes the empty word of X^*, i e the identity of X^* An element of X^* is called a *word* over X We denote the cardinality of a finite set A by $|A|$

Let $\mathcal{A} = (S, X, \delta)$ where (1) S and X are nonempty finite sets called a *state set* and an *alphabet*, respectively and (2) δ is a function called a *state* *transition function* such that $\delta(s,a) \in S$ for any $s \in S$ and any $a \in X$. Then $\mathcal{A}$ is called an *automaton.*

Notice that the above δ can be extended to the following function in a natural way, i.e. $\delta(s,\epsilon) = s$ and $\delta(s,au) = \delta(\delta(s,a),u)$ for any $s \in S$, any $u \in X^*$ and any $a \in X$.

Regarding more detailed information on words and automata, see [3] and [5].

Now we introduce some notions on posets (partially ordered sets). Let $(A,\preceq)$ be a poset and let $a \in A$. Then a is called a *minimal element* if $b \preceq a$ and $b \in A$ imply $b = a$. Let $b \in A$. Then b is called a *maximal element* if $b \preceq a$ and $a \in A$ imply $a = b$. Two posets $(A_1,\preceq_1)$ and $(A_2,\preceq_2)$ are said to be *isomorphic*, denoted by $(A_1,\preceq_1) \cong (A_2,\preceq_2)$ if there exists a bijection ρ of A_1 onto A_2 satisfying the condition: For any $a,b \in A_1$, $a \preceq_1 b$ if and only if $\rho(a) \preceq_2 \rho(b)$.

A poset $(A,\preceq)$ is called an *upper semilattice* if for any $a,b \in A$ there exists the least upper bound of a and b. Notice that there exists a unique maximal element, i.e. the maximum element in a finite upper semilattice.

2 Structures of strongly connected automata

In this section, we provide the structure of a strongly connected automaton with respect to its automorphism group.

Definition 1 An automaton $\mathcal{A} = (S,X,\delta)$ is said to be *strongly connected* if for any $s,t \in S$, there exist words $u,v \in X^*$ such that $\delta(s,u) = t$ and $\delta(t,v) = s$.

Definition 2 Let $\mathcal{A} = (S,X,\delta)$ and $\mathcal{B} = (T,X,\theta)$ be two automata. Then a bijection ρ of S onto T is called an *isomorphism* of $\mathcal{A}$ onto $\mathcal{B}$ if ρ satisfies the following condition: For any $s \in S$ and $a \in X$, we have $\rho(\delta(s,a)) = \theta(\rho(s),a))$.

If $\mathcal{A} = \mathcal{B}$, then an isomorphism is called an *automorphism.*

Notice that the set of all automorphisms forms a group. By $G(\mathcal{A})$, we denote the set of all automorphisms of $\mathcal{A}$.

The following result can be seen in [2], [5] and [8].

Proposition 1 *Let $\mathcal{A} = (S, X, \delta)$ be a strongly connected automaton and let ρ, ξ be two automorphisms of $\mathcal{A}$. Then $\rho = \xi$ if $\rho(s) = \xi(s)$ for some $s \in S$.*

By the above lemma, we have the following fundamental result (see [2], [5] and [8]).

Theorem 1 *Let $\mathcal{A} = (S, X, \delta)$ be a strongly connected automaton. Then there exists a positive integer n such that $|S| = n|G(\mathcal{A})|$.*

Before providing the structure of a strongly connected automaton, we define a group-matrix type automaton.

Definition 3 Let G be a finite group. Then G^0 is the set $G \cup \{0\}$ in which we introduce two operations $\cdot$ and $+$:

(1) For any $g, h \in G$, we define $g \cdot h$ as the group operation in G.
(2) For any $g \in G$, we define $g \cdot 0 = 0 \cdot g = 0$ and $0 \cdot 0 = 0$.
(3) For any $g \in G$, we define $g + 0 = 0 + g = g$ and $0 + 0 = 0$.
(4) For any $g, h \in G$, $g + h$ is not defined.

Definition 4 Let G be a finite group and let n be a positive integer. We consider an $n \times n$ matrix $(f_{pq}), f_{pq} \in G^0, p, q = 1, 2, \ldots, n$. If an $n \times n$ matrix (f_{pq}) satisfies the following conditions, then (f_{pq}) is called a *group-matrix of order* n on G: For any $p' = 1, 2, \ldots, n$, there exists a unique number $q' = 1, 2, \ldots, n$ such that $f_{p'q'} \neq 0$.

By $M_n(G)$, we denote the set of all group-matrices of order n on G. Then $M_n(G)$ forms a semigroup under the following operation:

$$(f_{pq})(g_{pq}) = \left(\sum_{k=1}^{n} f_{pk} g_{kq}\right).$$

Definition 5 Let G be a finite group and n be a positive integer. We consider a vector $(f_p), f_p \in G^0, p = 1, 2, \ldots, n$. A vector (f_p) is called a *group-vector of order* n on G, if there exists a unique number $p' = 1, 2, \ldots, n$ such that $f_{p'} \neq 0$. We denote by $V_n(G)$ the set of all group-vectors of order n on G. For any $(f_p) \in V_n(G)$ and any $(g_{pq}) \in M_n(G)$, we define the following multiplication:

$$(f_p)(g_{pq}) = \left(\sum_{k=1}^{n} f_k g_{kp}\right).$$

Under this operation, we have $(f_p)(g_{pq}) \in V_n(G)$.

Definition 6 Let $G$ be a finite group and $n$ be a positive integer. An automaton $\mathcal{A} = (V_n(G), X, \delta_\Psi)$ is called a *group-matrix type automaton of order* $n$ on $G$ (or an $(n, G)$-*automaton*) if the following conditions are satisfied:

(1) $V_n(G)$ is the set of states.
(2) $X$ is a set of inputs.
(3) $\Psi$ is a function of $X$ into $M_n(G)$.
(4) δ_Ψ is defined by $\delta_\Psi(\mathbf{f}, a) = \mathbf{f}\Psi(a)$ where $\mathbf{f} \in V_n(G)$ and $a \in X$.

Theorem 2 ([4], [5]) Let $\mathcal{A} = (S, X, \delta)$ be a strongly connected automaton with $n = |S|/|G(\mathcal{A})|$. Then there exists an $(n, G)$-automaton isomorphic to $\mathcal{A}$.

Definition 7 An $(n, G)$-automaton $\mathcal{A}$ is said to be *regular* if $\mathcal{A}$ is strongly connected and $G(\mathcal{A})$ is isomorphic to $G$.

Necessary and sufficient conditions for a given group-matrix type automaton to be regular are provided in [4], [5] and [7]. The proof of following theorem is given in [4] and [5].

Theorem 3 *Let $G$ be a finite group and let $n$ be a positive integer. Then we can determine all regular $(n, G)$-automata.*

3 Layers of an automaton

Let $\mathcal{A} = (S, X, \delta)$ be an automaton. We define the equivalence relation $\sim$ on $S$ as follows: For $s, t \in S$, $s \sim t$ if and only if there exist $u, v \in X^*$ such that $\delta(s, u) = t$ and $\delta(t, v) = s$ hold.

Definition 8 Let $\mathcal{A} = (S, X, \delta)$ be an automaton. For $p \in S$, we define the subset T_p of $S$ by $\{s \in S \mid p \sim s\}$. This subset T_p is called a *layer* of $S$.

For two layers T_p and T_q, we define a partial order $\preceq_\mathcal{A}$ as follows: $T_p \preceq_\mathcal{A} T_q$ if there exists a word $u \in X^*$ such that $\delta(q, u) = p$.

By $\mathcal{P}(A)$, we denote the poset $(\{T_p \mid p \in S\}, \preceq_\mathcal{A})$.

Theorem 4 ([6]) Let $(A, \preceq)$ be a finite poset. Then there exists an automaton $\mathcal{A} = (S, X, \delta)$ such that $\mathcal{P}(\mathcal{A}) \cong (A, \preceq)$.

4 Classes of subautomata

In this section, first we characterize the structure of subautomata of an automaton $\mathcal{A}$ based on the layers of $\mathcal{A}$.

Definition 9 Let $\mathcal{A} = (S, X, \delta)$ and $\mathcal{B} = (T, X, \theta)$ be two automata. Then $\mathcal{B}$ is called a *subautomaton* of $\mathcal{A}$ if the following conditions are satisfied: (i) $T \subseteq S$. (ii) $\theta = \delta|_{T \times X}$, i.e. θ is the restriction of δ to $T \times X$.

Theorem 5 ([6]) Let $\mathcal{A} = (S, X, \delta)$ be an automaton and let $\{T_p \mid p \in S\}$ be the set of all layers of $\mathcal{A}$. Then $\mathcal{B} = (T, X, \theta)$ is a subautomaton of $\mathcal{A}$ if and only if the following conditions are satisfied: (i) There exist $T_{p_1}, T_{p_2}, \cdots, T_{p_r}$ such that $T = \{q \in S \mid \exists i \in \{1, 2, \ldots, r\}, T_q \preceq_{\mathcal{A}} T_{p_i}\}$. (ii) $\theta(s, a) = \delta(s, a)$ for $s \in T$ and $a \in X$.

Now we consider classes of subautomata of an automaton. By $\mathcal{S}(\mathcal{A})$, we denote the set of all subautomata of $\mathcal{A}$. Let $\mathcal{B}, \mathcal{C} \in \mathcal{S}(\mathcal{A})$. By $\mathcal{B} \sqsubseteq \mathcal{C}$, we mean that $\mathcal{B}$ is a subautomaton of $\mathcal{C}$. Then $\sqsubseteq$ is a partial order on $\mathcal{S}(\mathcal{A})$. Hence $(\mathcal{S}(\mathcal{A}), \sqsubseteq)$ is a poset.

Proposition 2 ([6]) $(\mathcal{S}(\mathcal{A}), \sqsubseteq)$ is a finite upper semilattice.

It might be conjectured that for any finite upper semilattice $\mathcal{L}$ there exists an automaton whose upper semilattice of subautomata is isomorphic to $\mathcal{L}$.

Now we deal with this problem.

Definition 10 A finite upper semilattice $\mathcal{L} = (A, \preceq)$ is called a *tree* if it satisfies the following condition: For any incomparabe elements $b, c \in A$, there is no element $a \in A$ such that $a \preceq b$ and $a \preceq c$.

Proposition 3 ([6]) Let $\mathcal{L} = (A, \preceq)$ be a tree. If the number of minimal elements of $\mathcal{L}$ is greater than 2, then there is no automaton $\mathcal{A}$ such that $(\mathcal{S}(\mathcal{A}), \sqsubseteq) \cong \mathcal{L}$.

We will give a full characterization of $(\mathcal{S}(\mathcal{A}), \sqsubseteq)$ for an automaton $\mathcal{A}$. To this end, we define $\oplus$-compositions of posets and automata.

Definition 11 Let $\mathcal{P}_1 = (A_1, \preceq_1)$ and $\mathcal{P}_2 = (A_2, \preceq_2)$ be two finite posets with $A_1 \cap A_2 = \emptyset$. Moreover, let B be the set of all maximal elements of $\mathcal{P}_1$ and let C be the set of all minimal elements of $\mathcal{P}_2$. Assume that for any $b \in B$ there exists a nonempty subset C_b of C with $\bigcup_{b \in B} C_b = C$. Then we can define the poset $\mathcal{P}_1 \oplus \mathcal{P}_2 = (A_1 \cup A_2, \preceq)$ as follows: (1) For any $i = 1, 2$ and $a, b \in A_i, a \preceq b$ if $a \preceq_i b$. (2) For any $b \in B$ and $c \in C_b, b \preceq c$.

Notic that $\mathcal{P}_1 \oplus \mathcal{P}_2$ is a finite upper semilattice if $\mathcal{P}_1$ and $\mathcal{P}_2$ are finite upper semilattices.

Definition 12 Let $\mathcal{A}_1 = (S_1, X, \delta_1)$ and $\mathcal{A}_2 = (S_2, X, \delta_2)$ be two automata with $S_1 \cap S_2 = \emptyset$, let $\mathcal{B}$ be the set of all minimal layers of $\mathcal{A}_1$ and let $\mathcal{C}$ be the set of all maximal layers of $\mathcal{A}_2$. Assume that for any $B \in \mathcal{B}$ there exists a maximal layer C_B in $\mathcal{C}$ with $\{C_B \mid B \in \mathcal{B}\} = \mathcal{C}$. Then a $\oplus$-*composition* of $\mathcal{A}_1$ and $\mathcal{A}_2$, $\mathcal{A}_1 \oplus \mathcal{A}_2 = (S_1 \cup S_2, X, \delta)$ can be defined as follows: (1) $\delta(s, x) = \delta_1(s, x)$ if $x \in X, s \in S_1$ and s is not in a minimal layer of $\mathcal{A}_1$. (2) $\delta(t, x) = \delta_2(t, x)$ for any $t \in S_2$ and $x \in X$. (3) If $s \in B$ with $B \in \mathcal{B}$ and $x \in X$, then any state in C_B can be assigned as $\delta(s, x)$.

Then we have the following lemma.

Lemma 1 ([6]) Let $\mathcal{A} = \mathcal{B} \oplus \mathcal{C}$. Then $(\mathcal{S}(\mathcal{A}), \sqsubseteq) \cong (\mathcal{S}(\mathcal{C}), \sqsubseteq) \oplus (\mathcal{S}(\mathcal{B}), \sqsubseteq)$.

Now we characterize the structure of $(\mathcal{S}(\mathcal{A}), \sqsubseteq)$ for an automaton $\mathcal{A}$.

Definition 13 Let n be a positive integer. Then a finite upper semilattice $\mathcal{L}(n)$ is an upper semilattice such that $\mathcal{L}(n) \cong (P(\{1, 2, \ldots, n\}), \subseteq)$ where $P(\{1, 2, \ldots, n\})$ is the set of all subsets of $\{1, 2, \ldots, n\}$ and $\subseteq$ is the inclusion relation on $P(\{1, 2, \ldots, n\})$.

Then we have the following:

Proposition 4 ([6]) Let $\mathcal{A} = (S, X, \delta)$ be an automaton. Then there exist positive integers $n_1, n_2, \ldots, n_k$ such that $(\mathcal{S}(\mathcal{A}), \sqsubseteq) \cong \mathcal{L}(n_1) \oplus \mathcal{L}(n_2) \oplus \cdots \oplus \mathcal{L}(n_k)$.

Definition 14 An upper semilattice $\mathcal{L}$ is said to be *of Ps-type* if $\mathcal{L} \cong \mathcal{L}(n_1) \oplus \mathcal{L}(n_2) \oplus \cdots \oplus \mathcal{L}(n_k)$ for some positive integers $n_1, n_2, \ldots, n_k$.

Proposition 5 ([6]) Let $\mathcal{L}$ be a Ps-type upper semillatice, i.e. $\mathcal{L} \cong \mathcal{L}(n_1) \oplus \mathcal{L}(n_2) \oplus \cdots \oplus \mathcal{L}(n_r)$. Then there exists an automaton $\mathcal{A}$ such that $(\mathcal{S}(\mathcal{A}), \sqsubseteq) \cong \mathcal{L}(n_1) \oplus \mathcal{L}(n_2) \oplus \cdots \oplus \mathcal{L}(n_r)$.

By the above propositions, we have:

Theorem 6 ([6]) Let $\mathcal{L}$ be a finite upper semilattice. Then there exists an automaton $\mathcal{A}$ such that $(\mathcal{S}(\mathcal{A}), \sqsubseteq) \cong \mathcal{L}$ if and only if $\mathcal{L}$ is a Ps-type upper semilattice.

5 Cyclic automata and single bottom automata

In this section, we deal with two kinds of special automata.

Definition 15 An automaton $\mathcal{A} = (S, X, \delta)$ is said to be *cyclic* if the following conditions are satisfied: (1) There exists $s_0 \in S$ which is called a *generator* of $\mathcal{A}$. (2) For any $s \in S$, there exists $u \in X^*$ such that $\delta(s_0, u) = s$.

Proposition 6 ([6]) Let $\mathcal{A} = (S, X, \delta)$ be a cyclic automaton. Then $\mathcal{A}$ has a unique maximal layer, which is maximum in $\mathcal{P}(\mathcal{A})$.

In [6], it is proven that any automaton has at least one minimal layer. Now we define single bottom automata.

Definition 16 An automaton which has a unique minimal layer is called a *single bottom* automaton.

An automaton $\mathcal{A} = (S, X, \delta)$ is said to be *directable* if for any $s, t \in S$, there exists a word $u \in X^*$ such that $\delta(s, u) = \delta(t, u)$.

Remark 1 Let $\mathcal{A} = (S, X, \delta)$ be a directable automaton. Then there exists a word $w \in X^*$ such that for any $s, t \in S, \delta(s, w) = \delta(t, w)$.

Remark 2 Directable automata were first introduced by J. Černý ([1]) and studied by many people with different names, e.g. synchronizable automata, cofinal automata, reset automata etc.

Proposition 7 ([6]) A directable automaton is a single bottom automaton.

6 Decomposition of automata

In this section, we decompose a single bottom automaton into a single loop automaton and a strongly connected automaton.

Definition 17 A single bottom automaton $\mathcal{A} = (S, X, \delta)$ is called a *single loop* automaton if the minimal layer consists of a single state.

Let $\mathcal{A} = (S, X, \delta)$ be a single bottom automaton. Based on $\mathcal{A}$, a single loop automaton $\mathcal{B} = ((S \setminus T_p) \cup \{t\}), X, \theta)$ can be defined as follows: (i) T_p is the unique minimal layer of $\mathcal{A}$ and $t$ is a new state. (ii) For $s \in S \setminus T_p$ and $a \in X, \theta(s, a) = \delta(s, a)$ if $\delta(s, a) \in S \setminus T_p$. (iii) For $s \in S \setminus T_p$ and $a \in X, \theta(s, a) = t$ if $\delta(s, a) \in T_p$. (iv) For $a \in X, \theta(t, a) = t$.

Remark 3 $\mathcal{B}$ is a homomorphic image of $\mathcal{A}$.

Definition 18 Let $\mathcal{C} = (T_p, X, \delta|_{T_p \times X})$ where T_p is the unique minimal layer of $\mathcal{A}$, and $\mathcal{B}$ is defined as before. Then $\{\mathcal{B}, \mathcal{C}\}$ is called a *decomposition* of $\mathcal{A}$.

Regarding the decomposition of a directable automaton, we have:

Proposition 8 ([6]) Let $\mathcal{A}$ be a single bottom automaton and let $\{\mathcal{B}, \mathcal{C}\}$ be its decomposition. Then $\mathcal{A}$ is directable if and only if $\mathcal{C}$ is directable.

7 Composition of automata

In this section, we consider compositions of automata.

Let $\mathcal{B} = (B \cup \{t\}, X, \theta)$ be a single loop automaton where $\{t\}$ is a minimal layer and let $\mathcal{C} = (C, X, \gamma)$ be a strongly connected automaton with $B \cap C = \emptyset$.

Definition 19 An automaton $\mathcal{A} = (B \cup C, X, \delta)$ is defined as follows: (i) For $b \in B$ and $a \in X, \delta(b, a) = \theta(b, a)$ if $\theta(b, a) \in B$. (ii) For $b \in B$ and $a \in X, \delta(b, a) \in C$ if $\theta(b, a) \notin B$. (iii) For $c \in C$ and $a \in X, \delta(c, a) = \gamma(c, a)$. Then the above automaton $\mathcal{A}$ is called a *composition* of $\mathcal{B}$ and $\mathcal{C}$.

Note that in (ii) any state in $C$ can be assigned to $\delta(b, a)$. Therefore, we can construct many different compositions from the same automata.

Let $\{\mathcal{B}, \mathcal{C}\}$ be the decomposition of an automaton $\mathcal{A}$ in Definition 18. Then $\mathcal{A}$ can be regarded as a composition of $\mathcal{B}$ and $\mathcal{C}$. Now consider the automorphism group of $\mathcal{A}$.

Proposition 9 ([6]) Let $\rho \in G(\mathcal{A})$. Then $\rho|_{T_p} \in G(\mathcal{C})$ holds and there exists $\alpha \in G(\mathcal{B})$ which satisfies the following conditions: (i) $\alpha|_{S\setminus T_p} = \rho|_{S\setminus T_p}$. (ii) $\alpha(t) = t$.

From the above proposition, we may be interested in the subgroup $\{\rho|_{T_p} \mid \rho \in G(\mathcal{A})\}$ of $G(\mathcal{C})$.

Theorem 7 ([6]) Let $G$ be a subgroup of $G(\mathcal{C})$ and let $\{\mathcal{B}, \mathcal{C}\}$ be the decomposition of an automaton $\mathcal{A}$. If there exists a homomorphism $\beta$ of $G(\mathcal{B})$ onto $G$, then there exists a composition $\mathcal{A}'$ of $\mathcal{B}$ and $\mathcal{C}$ such that $G = \{\rho|_{T_p} \mid \rho \in G(\mathcal{A}')\}$.

References

[1] J. Černý, Poznámka k homogénym experimentom s konečinými automatami, Matematicko-fysikalny Časopis SAV 14 (1964), 208-215.

[2] A.C. Fleck, Isomorphism groups of automata, J. ACM 9 (1962), 469-476.

[3] J.E. Hopcroft and J.D. Ullman, *Introduction to Automata Theory, Languages and Computation*, Addison-Wesley, Reading MA, 1979.

[4] M. Ito, A representation of strongly connected automata and its applications, Journal of Computer and Systems Science 17 (1978), 65-80.

[5] M. Ito, *Algebraic Theory of Automata and Languages*, World Scientific, Singapore, 2004.

[6] M. Ito, Algebraic structures of automata, Theoretical Computer Science 429 (2012), 164-168.

[7] M. Katsura, Automorphism groups and factor automata of strongly connected automata, Journal of Computer and Systems Science 36 (1988), 25-65.

[8] G.P. Weeg, The structure of an automaton and its operation preserving transformation group, J. ACM 9 (1962), 345-349.