On some algebraic properties of automata*

András Ádám †

Abstract

Let $\mathcal{A}$ be a class of Moore automata. It is shown that $R(H(S(\mathcal{A})))$ is closed for the three operators S, H, R where S, H, R denote that the set of subautomata, of factor automata, of the automata obtained by input reduction (respectively) are formed.

Introduction

In the general theory of algebraic structures, the theorem of Tarski is one of the well-known results.[1] It concerns to how the narrowest class $V(\mathcal{A})$ can be produced from a class $\mathcal{A}$ of structures (all being of the same type) such that $V(\mathcal{A})$ is closed for the operators of forming direct products, subalgebras and factor algebras.

The present paper contains a variation on the theme of Tarski. We deal with automata (having output function) in the sense of Moore.[2] Our considerations concern to the operators of forming subautomata and factor automata, and to the operator of input reduction. (We study a weaker and a total version of the second and third of these operators.)

Let an arbitrary class $\mathcal{A}$ of finite Moore automata be considered. Let us denote by $K(\mathcal{A})$ the narrowest class which includes $\mathcal{A}$ and is closed for the three operators S, H, R mentioned above. Our main result expresses that $R(S(H(\mathcal{A})))$ exhausts the class $K(\mathcal{A})$. An auxiliary statement (Lemma 2) is now valid in a stronger form, than in the field of universal algebra (namely, equality can be asserted instead of set inclusion).

---

*Research partially supported by the Hungarian National Foundation for Scientific Research (OTKA) grant, no. T 026069.

†A. Rényi Mathematical Institute of the Hungarian Academy of Sciences, 1364 Budapest, P.O. Box 127, Hungary, email: tappancs@renyi.hu

[1] See [4] and Section 9 of Chapter 2 in [3].

[2] These automata cannot be regarded, in strict sense, to be algebraic structures. Although the transition function of an automaton may be viewed as a family consisting of $|X|$ unary operations, the output function is not an algebraic operation. In the field of automaton theory, direct products and substructures (we deal with the second of them only) have the same properties as familiar in algebra; the congruences and factor automata behave, however, somewhat curiously for an algebraist (cf. Sections 6–7 and Appendix 3 in [1]). The dissimilarity is continued when input reduction is considered; this operator does not preserve the type, in contrast to the usual algebraic operators which are type-preserving.

1 Basic terminology

By an *automaton* we mean a Moore-type automaton, written in form $\mathbf{A} = (A, X, Y, \delta, \lambda)$. (Here A, X, Y are nonempty finite sets.) The letter $\mathcal{A}$ is used for denoting a nonempty set consisting of automata. Isomorphic automata are regarded to be equal.

Some basic notions and facts of automaton theory are supposed to be known (see also Chapter 1 in [1]); including that there is a maximal congruence among the congruences of an automaton $\mathbf{A}$, and $a \equiv b \pmod{\pi_{\max}}$ precisely when the states a and b are indistinguishable (formally: when $\lambda(\delta(a,p)) = \lambda(\delta(b,p))$ for each input word p). We say that $\mathbf{A}$ is *simple* if $\pi_{\max}$ equals the trivial congruence of $\mathbf{A}$. Let π run through the congruences of $\mathbf{A}$, among the factor automata $\mathbf{A}/\pi$ solely $\mathbf{A}/\pi_{\max}$ is simple.

Let x_1, x_2 be input symbols, we say that x_1 and x_2 *act equally* (in $\mathbf{A}$) if $\delta(a, x_1) = \delta(a, x_2)$ for each $a (\in A)$. There is obviously a partition $\sigma_{\max}^{(A)}$ of the set X of input symbols such that the symbols being in a common partition class and only these act equally. $\mathbf{A}$ is called an *input-reduced* automaton if $\sigma_{\max}^{(A)}$ is the most refined partition of X (i.e., the partition whose index equals $|X|$). We can omit the superscript and write $\sigma_{\max}$ if there is no danger of confusion.

Let a partition $\sigma (\leq \sigma_{\max}^{(A)})$ of X be chosen. We can form the automaton $\mathbf{A}\backslash\sigma$ in a natural manner, namely, by identifying the input symbols which are in a common class mod σ.

2 The five operators

Consider an arbitrary class $\mathcal{A}$ of automata. Five operators will be introduced; by applying any of them, we obtain another automaton class from $\mathcal{A}$.

Let $\mathbf{D} \in S(\mathcal{A})$ hold when there is an $\mathbf{A} (\in \mathcal{A})$ such that $\mathbf{D}$ is a subautomaton of $\mathbf{A}$.

Let $\mathbf{C} \in H(\mathcal{A})$ hold when there are an $\mathcal{A} (\in \mathcal{A})$ and a congruence π of $\mathbf{A}$ such that $\mathbf{C} = \mathbf{A}/\pi$.

Let $\mathbf{C}_1 \in H^{\Delta}(\mathcal{A})$ hold when $\mathbf{C}_1$ is simple and $\mathbf{C}_1 \in H(\mathcal{A})$.

Let $\mathbf{B} \in R(\mathcal{A})$ hold when there are an $\mathbf{A} (\in \mathcal{A})$ and a partition σ of the set X of input symbols or $\mathbf{A}$ such that ($\sigma \leq \sigma_{\max}^{(A)}$ and) $\mathbf{B} = \mathbf{A}\backslash\sigma$.

Let $\mathbf{B}_1 \in R^{\Delta}(\mathcal{A})$ hold when $\mathbf{B}_1$ is input-reduced and $\mathbf{B}_1 \in R(\mathcal{A})$.

In the final part of this section some evident consequences of the definitions above are listed.

Denote by Q any of $S, H, H^{\Delta}, R, R^{\Delta}$. The equality $Q(Q(\mathcal{A})) = Q(\mathcal{A})$ holds (i.e., the operators are idempotent), and

$$Q(\mathcal{A}) = \cup_{\mathbf{A} \in \mathcal{A}} Q(\mathbf{A}).$$

In case $|\mathcal{A}| = 1$ we write $Q(\mathbf{A})$ instead of $Q(\{\mathbf{A}\})$.

It is clear that the equalities

$$H^{\Delta}(H(\mathcal{A})) = H(H^{\Delta}(\mathcal{A})) = H^{\Delta}(\mathcal{A}) \tag{2.1}$$

and

$$R^{\Delta}(R(\mathcal{A})) = R(R^{\Delta}(\mathcal{A})) = R^{\Delta}(\mathcal{A}), \tag{2.2}$$

furthermore, the inclusions

$$S(\mathcal{A}) \supseteq \mathcal{A}, \;\; H(\mathcal{A}) \supseteq \mathcal{A}, \;\; R(\mathcal{A}) \supseteq \mathcal{A} \tag{2.3}$$

are valid. The membership relations $\mathbf{D} \in S(\mathbf{A})$ and $\mathbf{C} \in H(\mathbf{A})$ imply

$$\sigma_{\max}^{(A)} \leq \sigma_{\max}^{(D)}, \;\; \sigma_{\max}^{(A)} \leq \sigma_{\max}^{(C)}, \tag{2.4}$$

respectively.

3 The main result

Now we can expose the Tarski-type statements for automata.

Theorem 1 *Let a class $\mathcal{A}$ of automata be considered. Denote by $\mathcal{K}$ the narrowest class such that $\mathcal{K} \supseteq \mathcal{A}$ and $\mathcal{K}$ is closed for the operators S, H, R.*

(I) *$\mathcal{K}$ equals $R(H(S(\mathcal{A})))$.*

(II) *The class of the simple automata belonging to $\mathcal{K}$ equals $R(H^{\Delta}(S(\mathcal{A})))$.*

(III) *The class of the input-reduced automata belonging to $\mathcal{K}$ equals $R^{\Delta}(H(S(\mathcal{A})))$.*

(IV) *The class of the input-reduced simple automata belonging to $\mathcal{K}$ equals $R^{\Delta}(H^{\Delta}(S(\mathcal{A})))$.* □

4 Proof of the main result

The following facts can be seen easily:

Lemma 1 *The operator R does not alter the distinguishability of states of an automaton. Hence the subsequent three conditions are equivalent for an automaton* $\mathbf{A}$:

(i) $\mathbf{A}$ *is simple.*

(ii) *$R(\mathbf{A})$ contains at least one simple automaton.*

(iii) *All the automata belonging to $R(\mathbf{A})$ are simple.*

□

Lemma 2 $S(H(\mathcal{A})) = H(S(\mathcal{A}))$.

Proof. Assume $\mathbf{A} \in \mathcal{A}$ and $\mathbf{D} \in S(H(\mathbf{A}))$. Then there exist an automaton $\mathbf{C}(\supseteq \mathbf{D})$ and a homomorphism χ such that χ maps $\mathbf{A}$ onto $\mathbf{C}$. The states a of $\mathbf{A}$ for which $\chi(a)$ belongs to the state set of $\mathbf{D}$ constitute a subautomaton $\mathbf{D}'$ of $\mathbf{A}$. It is obvious that $\mathbf{D}$ is the image of $\mathbf{D}'$ under the appropriate restriction of χ.

Conversely, suppose $\mathbf{A} \in \mathcal{A}$ and $\mathbf{C} \in H(S(\mathbf{A}))$. There exist a subautomaton $\mathbf{D}$ of $\mathbf{A}$ and a congruence π_1 of $\mathbf{D}$ such that $\mathbf{D}/\pi_1$ and $\mathbf{C}$ are isomorphic. Introduce a partition π_2 of the state set of $\mathbf{A}$ such that

(α) the restriction of π_2 to the state set of $\mathbf{D}$ coincides with π_1, and

(β) any state of $\mathbf{A}$ which is not contained in $\mathbf{D}$ forms a one-element class mod π_2.

It is evident that π_2 is a congruence of $\mathbf{A}$ and $\mathbf{D}/\pi_1$ is a subautomaton of $\mathbf{A}/\pi_2$. □

Lemma 3 $S(R(\mathcal{A})) \subseteq R(S(\mathcal{A}))$.

Proof. Suppose $\mathbf{A} \in \mathcal{A}$ and $\mathbf{D} \in S(R(\mathbf{A}))$. Then there exist a $\mathbf{B}(\supseteq \mathbf{D})$ and a partition σ of X such that $\mathbf{B} = \mathbf{A}\backslash\sigma$. We have clearly $\mathbf{D} = \mathbf{D}_1\backslash\sigma$ where $\mathbf{D}_1$ is a subautomaton of $\mathbf{A}$ such that the state sets of $\mathbf{D}_1$ and $\mathbf{D}$ coincide.

Lemma 4 $H(R(H(\mathcal{A}))) = R(H(\mathcal{A}))$.

Proof. The inclusion $\supseteq$ holds by (2.3). It suffices to show the relation $\subseteq$ when $\mathcal{A} = \{\mathbf{A}\}$.

Assume $\mathbf{C}_1 \in H(R(H(\mathbf{A})))$. This supposition means the existence of two automata $\mathbf{C}_2, \mathbf{B}$, a partition σ of X, two homomorphisms χ_1, χ_2 such that

$$\mathbf{B} \in R(H(\mathbf{A})), \;\; \mathbf{C}_2 \in H(\mathbf{A}), \;\; \mathbf{B} = \mathbf{C}_2\backslash\sigma,$$

moreover, χ_1 maps $\mathbf{B}$ onto $\mathbf{C}_1$ and χ_2 maps $\mathbf{A}$ onto $\mathbf{C}_2$. The state sets of $\mathbf{C}_2$ and $\mathbf{B}$ are equal.

Denote the kernels of χ_2 and χ_1 by π_2 and π_1, respectively. (π_2 is a congruence of $\mathbf{A}, \pi_1$ is a congruence of $\mathbf{B}$ as well as of $\mathbf{C}_2(= \mathbf{A}/\pi_2)$.) Introduce a partition π_1' of the state set A of $\mathbf{A}$ by

$$a \equiv b \pmod{\pi_1'} \Leftrightarrow \chi_2(a) \equiv \chi_2(b) \pmod{\pi_1}.$$

π_1' is a congruence of $\mathbf{A}$ (since π_1, π_2 are congruences), and

$$\mathbf{C}_1 = (\mathbf{A}/\pi_1')\backslash\sigma.$$

This representation of $\mathbf{C}_1$ assures $\mathbf{C}_1 \in R(H(\mathbf{A}))$. □

Lemma 5 $H^{\Delta}(R(\mathcal{A})) \subseteq R(H^{\Delta}(\mathcal{A}))$.

Proof. As in the preceding proof, we deal with the case $\mathcal{A} = \{\mathbf{A}\}$. Let $\mathbf{C}$ belong to $H^{\Delta}(R(\mathbf{A}))$. There exists a $\sigma(\leq \sigma_{\max}^{(A)})$ such that, with the maximal congruence π of $\mathbf{B} = \mathbf{A}\backslash\sigma$, we have $\mathbf{C} = \mathbf{B}/\pi$. The first sentence of Lemma 1 guarantees that the state partition π is the maximal congruence of A also, thus $\mathbf{C}_1 = \mathbf{A}/\pi$ is a simple automaton. There exists the automaton $\mathbf{C}_1\backslash\sigma$ (since $\sigma \leq \sigma_{\max}^{(C_1)}$ by (2.4)), and

$$\mathbf{C} = \mathbf{C}_1\backslash\sigma \in R(H^{\Delta}(\mathbf{A}))$$

is evident. □

Lemma 6 $H^{\Delta}(R(H(\mathcal{A}))) = R(H^{\Delta}(\mathcal{A}))$.

Proof. Assume $\mathbf{C}_2 \in R(H^{\Delta}(\mathcal{A}))$. The automaton $\mathbf{C}_2$ is simple (by the second sentence of Lemma 1), consequently

$$\{\mathbf{C}_2\} = H^{\Delta}(\mathbf{C}_2) \subseteq$$

$$\subseteq H^{\Delta}(R(H^{\Delta}(\mathcal{A}))) \subseteq H^{\Delta}(R(H(\mathcal{A}))).$$

Thus $\supseteq$ has been verified. The inclusion $\subseteq$ follows from Lemma 5 and (2.1):

$$H^{\Delta}(R(H(\mathcal{A}))) \subseteq R(H^{\Delta}(H(\mathcal{A}))) = R(H^{\Delta}(\mathcal{A})).$$

□

Proof of Theorem 1. For verifying (I), first we observe

$$(\mathcal{A} \subseteq) R(H(S(\mathcal{A}))) \subseteq \mathcal{K}.$$

Conversely, suppose $\mathbf{B} \in \mathcal{K}$. There exist a positive integer t and t automata $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_t$ such that $\mathbf{A}_1 \in \mathcal{A}, \mathbf{A}_t = \mathbf{B}$, and, for any i (where $2 \leq i \leq t$), $\mathbf{B}_i$ can be obtained from $\mathbf{B}_{i-1}$ either by R or by H or by S.

Our next aim is to show the implication

$$\mathbf{A}_{i-1} \in R(H(S(\mathbf{A}_1))) \Rightarrow \mathbf{A}_i \in R(H(S(\mathbf{A}_1))). \tag{4.1}$$

If $\mathbf{A}_i \in R(\mathbf{A}_{i-1})$ or $\mathbf{A}_i \in H(\mathbf{A}_{i-1})$, then (4.1) holds by the idempotency of R or by Lemma 4, respectively. When $\mathbf{A}_i \in S(\mathbf{A}_{i-1})$, then (4.1) follows from Lemmas 2, 3 and the idempotency of S.

Our inference can be summarized as follows:

$$\mathbf{B} \in \{\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_t\} \subseteq R(H(S(\mathbf{A}_1))) \subseteq R(H(S(\mathcal{A}))).$$

Now we turn to showing (II) and (III). Lemma 6 and (2.2) imply the equalities

$$H^{\Delta}(R(H(S(\mathcal{A})))) = R(H^{\Delta}(S(\mathcal{A}))) \tag{4.2}$$

and

$$R^{\Delta}(R(H(S(\mathcal{A})))) = R^{\Delta}(H(S(\mathcal{A}))), \tag{4.3}$$

respectively. Since the statement (I) is true, (4.2) expresses (II) and (4.3) expresses (III).

Finally, we prove (IV). Consider an arbitrary input-reduced simple automaton $\mathbf{B}'$which is contained in $\mathcal{K}$. We have

$$\{\mathbf{B}'\} = R^\Delta(H^\Delta(\mathbf{B}')) \subseteq R^\Delta(H^\Delta(\mathcal{K})).$$

This means that $R^\Delta(H^\Delta(\mathcal{K}))$ exhausts the class of input-reduced simple automata which belong to $\mathcal{K}$. The deduction

$$R^\Delta(H^\Delta(\mathcal{K})) = R^\Delta(H^\Delta(R(H(S(\mathcal{A}))))) =$$

$$= R^\Delta(R(H^\Delta(S(\mathcal{A})))) = R^\Delta(H^\Delta(S(\mathcal{A})))$$

is valid by (I), Lemma 6 and (2.2). □

5 Final remarks

Some statements, related to lemmas in the preceding section, can be proved by similar ideas; for example, the equalities

$$H^\Delta(S(H(\mathcal{A}))) = S(H^\Delta(\mathcal{A}))$$

and

$$H^\Delta(R^\Delta(H^\Delta(\mathcal{A}))) = R^\Delta(H^\Delta(\mathcal{A})). \tag{5.1}$$

I have become acquainted with facts belonging to the present topics when H. Andréka and Zs. Baranyai showed that (5.1) holds (in case $|\mathcal{A}| = 1$) but

$$R^\Delta(H^\Delta(R^\Delta(\mathcal{A}))) = H^\Delta(R^\Delta(\mathcal{A}))$$

is not valid in general [2].

We have stated *equality* in Lemma 2 for automata, in the general theory of algebraic structures only the *inclusion* $S(H(\mathcal{A})) \subseteq H(S(\mathcal{A}))$ is valid. In addition, it follows from Lemma 2 that

$$S(H^\Delta(\mathcal{A})) = H^\Delta(S(H(\mathcal{A}))) = H^\Delta(H(S(\mathcal{A}))) = H^\Delta(S(\mathcal{A})) \tag{5.2}$$

in the field studied here. Consequently, the formulae in the statements (I)–(IV) of Theorem 1 can equivalently be replaced by

$$R(S(H(\mathcal{A}))), \quad R(S(H^\Delta(\mathcal{A}))),$$

$$R^\Delta(S(H(\mathcal{A}))), \quad R^\Delta(S(H^\Delta(\mathcal{A}))),$$

respectively.

a	$\delta(a, x_1)$	$\delta(a, x_2)$
1	2	3
2	3	3
3	2	2

Table 1

e	$\delta(e, x_1)$	$\delta(e, x_2)$	$\lambda(e)$
1	2	4	y_1
2	3	3	y_2
3	1	1	y_3
4	3	3	y_2

(a)

c	$\delta(c, x_1)$	$\delta(c, x_2)$	$\lambda(c)$
1	2	2	y_1
2	3	3	y_2
3	1	1	y_3

(b)

d	$\delta(d, x)$	$\lambda(d)$
1	2	y_1
2	3	y_2
3	1	y_3

(c)

Table 2

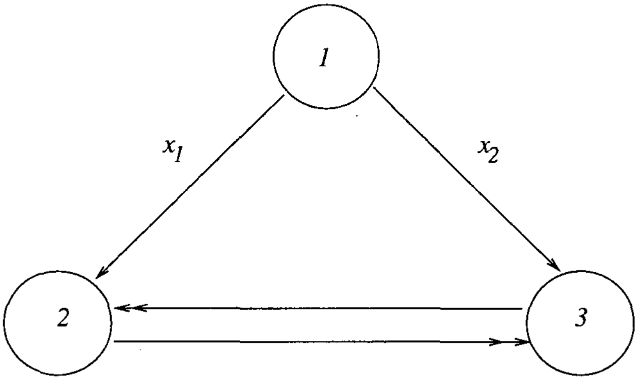

Figure 1

Is Lemma 3 true with equality (instead of $\subseteq$)? The next example shows that the answer is negative (in general). Consider the automaton **A** determined by Table 1 (the output function is indifferent), see also Figure 1. Let **B** be the autonomous automaton having two states in which $\delta(b_1, x) = b_2$ and $\delta(b_2, x) = b_1$. This **B** is contained in $R(S(\mathbf{A}))$, it does not belong to $S(R(\mathbf{A}))$.

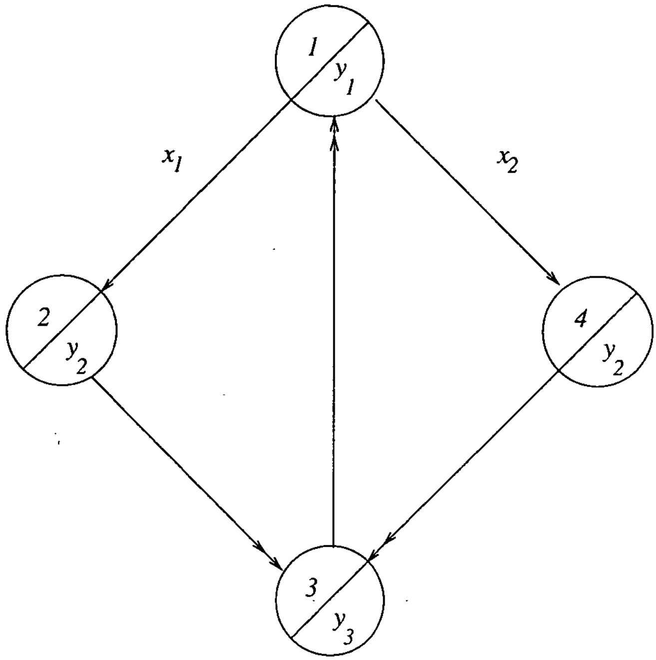

Figure 2

Analogously, Lemma 5 loses its validity if inclusion is replaced by equality. Indeed, let $\mathbf{E}, \mathbf{C}, \mathbf{D}$ be the Moore automata determined by Tables 2/a, 2/b, 2/c, respectively; see also Figure 2 for $\mathbf{E}$. Then $R(H^{\Delta}(\mathbf{E})) = \{\mathbf{C}, \mathbf{D}\}$ and $H^{\Delta}(R(\mathbf{E})) = \{\mathbf{D}\}$.

References

[1] Ádám, A., *The behaviour and simplicity of finite Moore automata*, Akadémiai Kiadó, Budapest, 1996.

[2] Andréka, H. and Baranyai, Zs., Personal communication (in the late 1960's).

[3] Burris, S. and Sankappanavar, H. P., *A course in Universal Algebra*, Springer, New York, 1981. (Hungarian translation: Tankönyvkiadó, Budapest, 1988.)

[4] Tarski, A., A remark on functionally free algebras, *Annals of Math.* 47 (1946), 163-165.

Received September, 2000