Machine Morphisms and Simulation

Jānis Buls

Abstract—This paper examines the concept of simulation from a modelling viewpoint. How can one Mealy machine simulate the other one? We create formalism for simulation of Mealy machines. The injective s–morphism of the machine semigroups induces the simulation of machines [1]. We present the example of s–morphism such that it is not a homomorphism of semigroups. The story for the surjective s–morphisms is quite different. These are homomorphisms of semigroups but there exists the surjective s–morphism such that it does not induce the simulation.

Keywords—Mealy machine, simulation, machine semigroup, injective s–morphism, surjective s–morphisms.

I. Introduction

We recall the classical approach to the representation of finite machines by semigroups (see, e.g., [4]). Let $V = \langle Q, A, B, \circ, *\rangle$ be a Mealy machine, where Q, A, B are finite, non-empty sets; $Q \times A \xrightarrow{\circ} Q$ is a function and $Q \times A \xrightarrow{*} B$ is a surjective function. Let $T(Q)$ denotes the semigroup of all transformations on the set Q and let $Fun(Q, B)$ denotes the set of all maps from Q to B. On the set $S(Q, B) = T(Q) \times Fun(Q, B)$ define the multiplication by

$$\begin{array}{rcl} (g_1, \psi_1)(g_2, \psi_2) & = & (g_1 g_2, g_1\psi_2); \\ g_1, g_2 \in T(Q), & & \psi_1, \psi_2 \in Fun(Q, B). \end{array}$$

Under this operation $S(Q, B)$ is easily seen to be a semigroup. Let $Q = \{q_1, q_2, \ldots, q_k\}$, $A = \{a_1, a_2, \ldots, a_m\}$, $B = \{b_1, b_2, \ldots, b_n\}$. Define two mappings $A \xrightarrow{\alpha} T(Q)$ and $A \xrightarrow{\beta} Fun(Q, B)$ as follows. For each $a_i \in A$ define $\alpha(a_i) \in T(Q)$ and $\beta(a_i) \in Fun(Q, B)$ by

$$\alpha(a_i) = \begin{pmatrix} q_1 & q_2 & \ldots & q_k \\ q'_1 & q'_2 & \ldots & q'_k \end{pmatrix},$$
$$\beta(a_i) = \begin{pmatrix} q_1 & q_2 & \ldots & q_k \\ b'_1 & b'_2 & \ldots & b'_k \end{pmatrix},$$

where $\forall s(q'_s = q_s \circ a_i \wedge b'_s = q_s * a_i)$. Now the representation $A \xrightarrow{\eta} S(Q, B)$ is defined by setting $\eta(a_i) = (\alpha(a_i), \beta(a_i))$. The semigroup $\langle V\rangle$ generated by $\eta(A)$ is called the *machine* V *semigroup.*

Simulation was first discussed by Hartmanis [2] more than forty years ago. This concept describes the possibility on abstract level in which one machine could be replaced by another one in applications, for example, cryptography, especially, cryptanalysis of cryptographic devices. If we like to treat as it is done till now the machines by semigroups and develop the theory not only as self-sufficient discipline the connections between simulation and semigroups should be considered from every point of view too. Thus we say that a transition from machines to semigroups through some representation is *successful* if it adequately characterizes the simulation.

II. Simulation

In this section we introduce some of the notation and terminology needed in the subsequent section. If C and $'C$ are alphabets any mapping $C \xrightarrow{h} {}'C$ can be extended in the usual way to a morphism denoted by h too from C^* to $'C^*$. Thus if $V = \langle Q, A, B, \circ, *\rangle$ we may extend the mappings $\circ$ and $*$ to $Q \times A^*$ by defining

$$\begin{array}{ll} q \circ \lambda = q, & q \circ (ux) = (q \circ u) \circ x\,, \\ q * \lambda = \lambda, & q * (ux) = (q * u)((q \circ u) * x)\,, \end{array}$$

for all $q \in Q$, $(u, x) \in A^* \times A$, and where λ is the empty word. Henceforth, we shall omit parentheses if there is no danger of confusion. So, for example, we will write $q \circ u * x$ instead of $(q \circ u) * x$.

Definition 1: Let $V = \langle Q, A, B\rangle$, $'V = \langle 'Q, 'A, 'B\rangle$ be machines. We say that $'V$ *simulates* V *by*

$$Q \xrightarrow{h_1} {}'Q, \quad A \xrightarrow{h_2} {}'A, \quad {}'B \xrightarrow{h_3} B$$

if the diagram

$$\begin{tikzcd} Q \arrow[d, "h_1"'] & \times & A^* \arrow[r, "*"] \arrow[d, "h_2"] & B^* \\ {}'Q & \times & {}'A^* \arrow[r, "*"] & {}'B^* \arrow[u, "h_3"'] \end{tikzcd}$$

commutes. That is, if

$$q * u = h_3(h_1(q) * h_2(u)) \qquad \text{for all} \qquad (q, u) \in Q \times A^*.$$

This concept corresponds to scheme E—$'\mathfrak{V}$—D (see Fig. 1) where E — an encoder, $'\mathfrak{V}$ — a device represents the machine $'V$, D — a decoder; $\mathfrak{V}$ — a device represents the machine V.

this scheme (Fig. 1) enables to extend the notion of simulation [5].

Definition 2: Let $V = \langle Q, A, B\rangle$, $'V = \langle 'Q, 'A, 'B\rangle$ be machines. We say that $'V$ *simulates* V *by*

$$Q \xrightarrow{h_1} {}'Q, \quad A \xrightarrow{h_2} {}'A^*, \quad {}'B^* \xrightarrow{h_3} B \qquad \textit{if}$$

$q \circ u * a = h_3(h_1(q) \circ h_2(u) * h_2(a))$ for all $(q, u, a) \in Q \times A^* \times A$.

Obviously now the upper tie from encoder to decoder is necessary. Otherwise the decoder is not able to decode the word $'v$ adequately. We write $'V \geq V(h_1, h_2, h_3)$ if $'V$ simulates V by h_1, h_2, h_3. We say $'V$ *simulates* V if there exist maps such that $'V \geq V(h_1, h_2, h_3)$. We write $'V \geq V$ if $'V$ simulates V.

The two machines V and $'V$ are *incomparable* if $V \not\geq {}'V$ and $'V \not\geq V$. If, on the other hand, $V \geq {}'V$ and $'V \geq V$ then we say that V *mutually simulates* $'V$ and we write $V \bowtie {}'V$.

Jānis Buls is with Department of Mathematics, University of Latvia, Raiņa bulvāris 19, Rīga, LV-1586 Latvia; e-mail: buls@fmf.lu.lv; web site: http://home.lanet.lv/˜buls

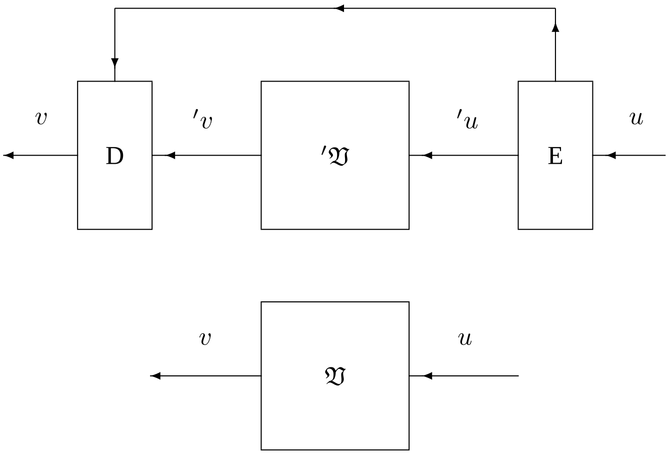

Fig. 1. Simulation.

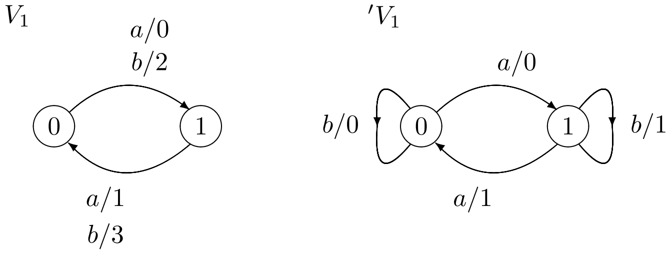

Fig. 2. $V_1 \bowtie {}'V_1$.

This definition has an interesting consequence.

***Example** 3:* $V_1 \bowtie {}'V_1$ (Fig. 2)

- $V_1 \geq {}'V_1(h_1', h_2', h_3')$, where

$$\begin{aligned} h_1' &: 0 \mapsto 0,\ 1 \mapsto 1; \\ h_2' &: a \mapsto a,\ b \mapsto a^2; \\ h_3' &: 0 \mapsto 0,\ 1 \mapsto 1,\ 01 \mapsto 0,\ 10 \mapsto 1. \end{aligned}$$

- ${}'V_1 \geq V_1(h_1, h_2, h_3)$, where

$$\begin{aligned} h_1 &: 0 \mapsto 0,\ 1 \mapsto 1; \\ h_2 &: a \mapsto a,\ b \mapsto a^3; \\ h_3 &: 0 \mapsto 0,\ 1 \mapsto 1,\ 010 \mapsto 2,\ 101 \mapsto 3. \end{aligned}$$

III. Morphisms

We generalize the concept of similar transformation semigroups (see, e.g., [3]) to machine semigroups as follows. Let $\sigma = (\alpha, \beta) \in S(Q, B)$ then we define a vector function of the machine

$$\bar{\sigma} : Q \longrightarrow Q \times B : q \mapsto (\alpha(q), \beta(q)).$$

The same denotation we use for a vector function ${}'Q \longrightarrow {}'Q \times {}'B$.

***Definition** 4:* Let $V = \langle Q, A, B, \circ, * \rangle$, ${}'V = \langle {}'Q, {}'A, {}'B, \acute{\circ}, \acute{*} \rangle$ be machines. We say that $\langle V \rangle \xrightarrow{\psi} \langle {}'V \rangle$ is the *s-morphism* of machine semigroup $\langle V \rangle$ to $\langle {}'V \rangle$ if there exist maps $Q \xrightarrow{g} {}'Q,\ B \xrightarrow{h} {}'B$ such that the diagram

$$\begin{tikzcd} Q \arrow[r, "\bar{\sigma}"] \arrow[d, "g"'] & Q \arrow[d, "g"'] & \times & B \arrow[d, "h"] \\ {}'Q \arrow[r, "\overline{\psi(\sigma)}"] & {}'Q & \times & {}'B \end{tikzcd}$$

commutes for every $\sigma \in \langle V \rangle$.

We adopt this notational convention henceforth.

If h is an injection the s-morphism is called the *injective s-morphism*. If g is a surjection the s-morphism is called the *surjective s-morphism*.

***Theorem** 5:* [1] Let $V = \langle Q, A, B, \circ, * \rangle$, ${}'V = \langle {}'Q, {}'A, {}'B, \acute{\circ}, \acute{*} \rangle$ be machines. If there exists the injective s-morphism $\langle V \rangle \xrightarrow{\psi} \langle {}'V \rangle$ then ${}'V$ simulates V.

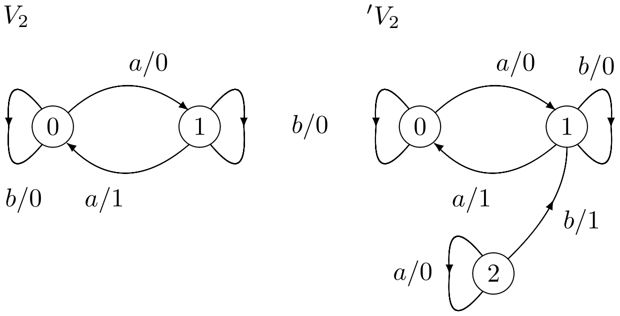

Fig. 3. ${}'V_2 \geq V_2$.

***Example** 6:*

The direct calculations show (Fig. 3)

$$\langle V_2 \rangle = \{\eta(a), \eta(b), \eta(a^2), \eta(ab)\},$$

where

$$\eta(a) = \left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \right),$$

$$\eta(b) = \left(\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right);$$

$$\begin{aligned} \langle {}'V_2 \rangle = \{ & \eta'(a), \eta'(b), \eta'(a^2), \eta'(ab), \eta'(ba), \eta'(b^2), \\ & \eta'(aba), \eta'(ab^2), \eta'(ba^2), \\ & \eta'(bab), \eta'(aba^2), \eta'((ab)^2)\}, \end{aligned}$$

where

$$\begin{aligned} \eta'(a) &= \left(\begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 0 \end{pmatrix} \right), \\ \eta'(b) &= \left(\begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \right). \end{aligned}$$

Define $\psi : \langle V_2\rangle \longrightarrow \langle 'V_2\rangle$ by setting

$$\eta(a) \mapsto \eta'(a),\ \eta(b) \mapsto \eta'(b),$$

$$\eta(a^2) \mapsto \eta'(a^2),\ \eta(ab) \mapsto \eta'(ab).$$

If $g : Q \longrightarrow Q$ and $h : B \longrightarrow B$ are the identical maps then ψ is an injective s–morphism of $\langle V_2\rangle$ to $\langle 'V_2\rangle$. Nevertheless ψ is not a homomorphism of semigroups because

$$\psi(\eta(ab)\eta(a)) = \psi(\eta(aba)) = \psi(\eta(a^2)) = \eta'(a^2)$$

but

$$\psi(\eta(ab))\psi(\eta(a)) = \eta'(ab)\eta'(a) = \eta'(aba) \neq \eta'(a^2).$$

Thus we have

Corollary *7:* There exists an injective s–morphism such that it is not a homomorphism of semigroups.

The story for the surjective s–morphisms is quite different.

Lemma *8:* If $\sigma_1, \sigma_2 \in S(Q, B)$ then $\sigma_1 = \sigma_2$ iff $\bar{\sigma}_1 = \bar{\sigma}_2$.

Proof. Let $\sigma_i = (\alpha_i, \beta_i)$, $i \in \{1, 2\}$, then

$$\forall q \in Q \quad q\bar{\sigma}_i = (q\alpha_i, q\beta_i).$$

$\Rightarrow$ Assume $\sigma_1 = \sigma_2$ then $(\alpha_1, \beta_1) = \sigma_1 = \sigma_2 = (\alpha_2, \beta_2)$. Hence $\alpha_1 = \alpha_2$ and $\beta_1 = \beta_2$. Thus $q\alpha_1 = q\alpha_2$ and $q\beta_1 = q\beta_2$ for all $q \in Q$. Therefore $\bar{\sigma}_1 = \bar{\sigma}_2$.

$\Leftarrow$ Assume $\bar{\sigma}_1 = \bar{\sigma}_2$ then

$$\forall q \in Q \quad (q\alpha_1, q\beta_1) = q\bar{\sigma}_1 = q\bar{\sigma}_2 = (q\alpha_2, q\beta_2).$$

Hence

$$\sigma_1 = (\alpha_1, \beta_1) = (\alpha_2, \beta_2) = \sigma_2. \quad \square$$

Theorem *9:* Every sirjective s–morphism $\psi : \langle V\rangle \longrightarrow \langle 'V\rangle$ is a homomorphism of semigroups.

Proof. We take into consideration the previous lemma. Hence, we may prove

$$\overline{\psi(\sigma_1\sigma_2)} = \overline{\psi(\sigma_1)\psi(\sigma_2)}$$

for every $\sigma_1, \sigma_2 \in \langle V\rangle$.

Let $\sigma_i = (\alpha_i, \beta_i)$ and $\psi(\sigma_i) = (\acute{\alpha}_i, \acute{\beta}_i)$, $i \in \{1, 2\}$, then

$$\forall \acute{q} \in {}'Q \quad \acute{q}\overline{\psi(\sigma_1)\psi(\sigma_2)} = (\acute{q}\acute{\alpha}_1\acute{\alpha}_2, \acute{q}\acute{\alpha}_1\acute{\beta}_2).$$

Let

$$\psi(\sigma_1\sigma_2) = (\acute{\alpha}_3, \acute{\beta}_3)$$

then

$$\acute{q}\overline{\psi(\sigma_1\sigma_2)} = (\acute{q}\acute{\alpha}_3, \acute{q}\acute{\beta}_3).$$

Since $g : Q \longrightarrow {}'Q$ is surjective then $\exists q \in Q \ \ qg = \acute{q}$. Hence, we must prove

$$(qg\acute{\alpha}_3, qg\acute{\beta}_3) = (qg\acute{\alpha}_1\acute{\alpha}_2, qg\acute{\alpha}_1\acute{\beta}_2). \tag{1}$$

Since diagram commutes (see Definition 4) then for every $i \in \{1, 2\}$

$$(qg\acute{\alpha}_i, qg\acute{\beta}_i) = ((qg)\acute{\alpha}_i, (qg)\acute{\beta}_i) = qg\overline{\psi(\sigma_i)} = (q\alpha_i g, q\beta_i h).$$

Hence

$$\begin{aligned} (qg\acute{\alpha}_1\acute{\alpha}_2, qg\acute{\alpha}_1\acute{\beta}_2) &= ((qg\acute{\alpha}_1)\acute{\alpha}_2, (qg\acute{\alpha}_1)\acute{\beta}_2) \\ &= ((q\alpha_1 g)\acute{\alpha}_2, (q\alpha_1 g)\acute{\beta}_2) \\ &= ((q\alpha_1)g\acute{\alpha}_2, (q\alpha_1)g\acute{\beta}_2) \\ &= ((q\alpha_1)\alpha_2 g, (q\alpha_1)\beta_2 h) \\ &= (q\alpha_1\alpha_2 g, q\alpha_1\beta_2 h) \end{aligned} \tag{2}$$

We have $\sigma_1\sigma_2 = (\alpha_1\alpha_2, \alpha_1\beta_2)$, therefore

$$\begin{aligned} (qg\acute{\alpha}_3, qg\acute{\beta}_3) &= qg\overline{\psi(\sigma_1\sigma_2)} \\ &= (q(\alpha_1\alpha_2)g, q(\alpha_1\beta_2)h) \\ &= (q\alpha_1\alpha_2 g, q\alpha_1\beta_2 h) \end{aligned} \tag{3}$$

Now (2) and (3) yield (1). $\square$

Example *10:*

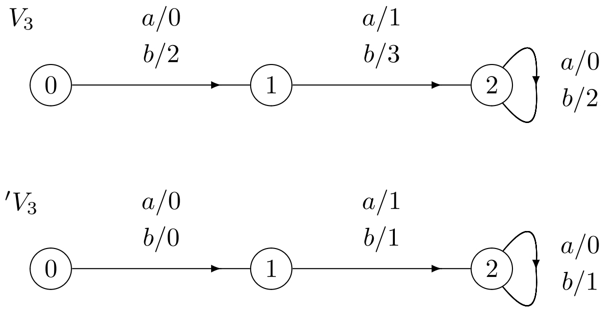

Fig. 4. Machines $'V_3$ and V_3 are incomparable.

The direct calculations show (Fig. 4)

$$\langle V_3\rangle = \{\eta(a), \eta(b), \eta(a^2), \eta(b^2), \eta(a^3), \eta(b^3)\},$$

where

$$\eta(a) = \left(\begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 0 \end{pmatrix} \right),$$

$$\eta(b) = \left(\begin{pmatrix} 0 & 1 & 2 \\ 0 & 2 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 \\ 2 & 3 & 2 \end{pmatrix} \right);$$

$$\langle 'V_3\rangle = \{\eta'(a), \eta'(b), \eta'(a^2), \eta'(b^2), \eta'(a^3)\},$$

where $\eta'(a) = \eta(a)$,

$$\eta'(b) = \left(\begin{pmatrix} 0 & 1 & 2 \\ 0 & 2 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 1 \end{pmatrix} \right).$$

Define $\psi : \langle V_3\rangle \longrightarrow \langle 'V_3\rangle$ by setting

$$\eta(a) \mapsto \eta'(a), \quad \eta(a^2) \mapsto \eta'(a^2), \quad \eta(a^3) \mapsto \eta'(a^3),$$
$$\eta(b) \mapsto \eta'(a), \quad \eta(b^2) \mapsto \eta'(a^2), \quad \eta(b^3) \mapsto \eta'(a^3).$$

If $g : \{0, 1, 2\} \longrightarrow \{0, 1, 2\}$ is the identical map and

$$h : \{0, 1, 2, 3\} \longrightarrow \{0, 1\} \quad : \quad 0 \mapsto 0,\ 1 \mapsto 1; 2 \mapsto 0,\ 3 \mapsto 1$$

then ψ is a surjective s–morphism of $\langle V_3\rangle$ to $\langle 'V_3\rangle$.

Nevertheless $'V_3$ cannot simulate the machine V_3. Suppose that $'V_3 \geq V_3(h_1, h_2, h_3)$ then $h_2(a) \neq h_2(b)$. Hence whether $h_2(a) \neq a$ or $h_2(b) \neq a$.

(i) Suppose $w = h_2(a) \neq a$ and observe (see Definition 2)

$$\begin{array}{rcl} 0 * a & = & h_3(h_1(0)\acute{*}w) = 0, \\ 0 \circ a * a & = & h_3(h_1(0)\acute{\circ}w\acute{*}w) = 1, \\ 0 \circ a^2 * a & = & h_3(h_1(0)\acute{\circ}w^2\acute{*}w) = 0, \\ 0 \circ a^3 * a & = & h_3(h_1(0)\acute{\circ}w^3\acute{*}w) = 0. \end{array}$$

Hence $h_1(0), h_1(0)\acute{\circ}w, h_1(0)\acute{\circ}w^2$ are distinct states. Therefore, there is only one possibility, namely, $h_1 : 0 \mapsto 0$ and

$$h_1(0)\acute{\circ}w = 1, \quad h_1(0)\acute{\circ}w^2 = 2.$$

So we are forced: $w = b$. Now we have

$$h_1(0)\acute{\circ}w\acute{*}w = 1\acute{*}b = 1 = 2\acute{*}b = h_1(0)\acute{\circ}w^2\acute{*}w.$$

Contradiction.

(ii) The same happens if we suppose $w = h_2(b) \neq a$.

Thus we have

Corollary *11:* There exists the surjective s–morphism such that it does not induce the simulation.

Acknowledgment

This work was supported by the European Social Fund within the project

Nr. 2009/0223/1DP/1.1.1.2.0/09/APIA/VIAA/008.

References

[1] J.Buls, I.Zandere. *Injective Morphisms of the Machine Semigroups.* Contributions to General Algebra **14**, Proceedings of the Olomouc Conference 2002 (AAA64) and the Potsdam Conference 2003 (AAA65). Verlag Johannes Heyn, Klagenfurt, P. 15–19, 2004.

[2] Hartmanis J. On the State Assignment Problem for Sequential Machines I. *IRE Transactions on Electronic Computers.* Vol. EC–**10**, No.**2**(June), pp.157–165, 1961.

[3] Lallement G. Semigroups and Combinatorial Applications. John Wlley & Sons, New York, Chichester, Brisbane, Toronto, 1979.

[4] Plotkin B. I., Greenglaz I. Ja., Gvaramija A. A. Algebraic Structures in Automata and Databases Theory. World Scientific, Singapore, New Jersey, London, Hong Kong, 1992.

[5] Я.А. Булс. *Оценка длины слова при моделировании конечных детерминированных автоматов.* Теория алгоритмов и программ. Рига: ЛГУ им. П. Стучки, С. 50–63, 1986. (Russian)