CDMTCS Research Report Series

Computational Complementarity for Mealy Automata

Cristian Calude
Elena Calude
Univeristy of Auckland

Cătălina Ştefănescu
Bucharest University

CDMTCS-083
May 1998

Centre for Discrete Mathematics and
Theoretical Computer Science

In Honour of D. Vaida's

65th Birthday

Computational Complementarity for Mealy Automata

Cristian S. Calude[*,†] **Elena Calude**[‡] **Cătălina Ştefănescu**[§]

Abstract

In this paper we extend (and study) two computational complementarity principles from Moore to Mealy automata which are finite machines possessing better "quantum-like" features. We conjecture that automata which are reversible according to Svozil do not satisfy any of these computational complementarity principles. This result is consistent with the embeddability of irreversible computations into reversible ones (via Bennett's method, for example). Mathematica experiments confirmed this hypothesis.

1 Introduction

Bohr's complementarity principle states the existence of certain (complementary) features of a quantum system which cannot be measured and predicted simultaneously with arbitrary accuracy. The most vivid illustration was announced recently in [1]: *wave-like behaviour (interference) occurs only when the different possible paths a particle can take are indistinguishable, even in principle.*[1]

Building on Moore's "Gedanken" experiments, in [14, 13] complementarity was modelled by means of finite automata. Two new computational complementarity principles have been introduced and studied in [3, 2, 8, 7, 6] using Moore's automata *without initial*

[*] Department of Computer Science, The University of Auckland, Private Bag 92019, Auckland, New Zealand; email: cristian@cs.auckland.ac.nz.

[†] Partially supported by AURC A18/XXXXX/62090/F3414075.

[‡] Department of Computer Science, The University of Auckland, Private Bag 92019, Auckland, New Zealand; email: elena@cs.auckland.ac.nz.

[§] Faculty of Mathematics, Bucharest University, Str. Academiei 14, Bucharest, Romania; email: cstef@colegiu.cs.unibuc.ro.

[1] In a double slit experiment with electrons scientists observed how the resultant interference pattern dissipates as the electrons go through the slits. The experiment involved for the first time fermions, spin-one-half particles. The "electrons particles" and "electron waves" slalom through a two-dimensional obstacle course, where they have to negotiate a pair of channels; one channel can "memorise" when an electron passed that way. The "electron wave" passes through both channels, but if it senses that it is being watched, the "electron particle" goes through only the one path, and as a result the interference diminishes.

states. We stress that we are dealing with a "classical measurement", that is one in which the measurement result can be copied (one-to-many) arbitrarily many times. This is very similar to the quantum measurement process, where also a classical apparatus is assumed. Thereby it is possible to maintain the measurement result "as well as" we develop the automaton backward.

Motivated by Svozil's analysis in [14] we extend the above mentioned computational complementarity principles for Mealy automata, a class of finite machines having better "quantum-like" features (see [14]). A special analysis will be devoted to the relation between "reversibility" and complementarity, mainly using Svozil's proposed definition of reversibility [15]. We conjecture that both computational complementarity principles are incompatible with reversibility; Mathematica experiments (we have used Mathematica 3.0 [17]) confirmed this hypothesis.

2 Moore and Mealy Automata

A finite deterministic automaton consists of a finite set of states and a set of transitions from state to state that occur on input symbols chosen from some fixed alphabet. For each symbol of the alphabet there is exactly one transition out of each state, possibly back to the state itself. So, formally, a *finite automaton* consists of a finite set Q of states, an input alphabet Σ, and a transition function $\delta : Q \times \Sigma \to Q$. Sometimes a fixed state is considered to be the *initial state*, and a subset F of Q denotes the set of *final states*. An automaton "reacts" by emitting an output from a finite set O. In what follows we are going to fix the alphabet Σ and concentrate almost exclusively on the case of automata for which O and Σ have the same cardinality, i.e., $\#(O) = \#(\Sigma)$.

A *Moore automaton* is a finite deterministic automaton having an *output function* $f : Q \to O$. At each time the automaton is in a given state q and is continually emitting the output $f(q)$. The automaton remains in state q until it receives an input signal σ, when it assumes the state $\delta(q, \sigma)$ and starts emitting $f(\delta(q, \sigma))$. So, a Moore automaton will be just a triple $\mathcal{A} = (Q, \delta, f)$.

Let Σ^* be the set of all finite sequences (words) over the alphabet Σ, including the empty word λ; by Σ^+ we denote $\Sigma^* \setminus \{\lambda\}$. The transition function δ can be extended to a function $\overline{\delta} : Q \times \Sigma^* \to Q$, as follows:[2]

$$\overline{\delta}(q, \lambda) = q,$$

$$\overline{\delta}(q, \sigma w) = \overline{\delta}(\delta(q, \sigma), w),$$

for all $q \in Q, \sigma \in \Sigma, w \in \Sigma^*$.

The output produced by an experiment executed on the Moore automaton A in state q with input sequence $w \in \Sigma^*$ is described by $R_{\mathcal{A}}(q, w)$, where $R_{\mathcal{A}} : Q \times \Sigma^* \longrightarrow O^*$ is *Moore's response function* defined as follows (see[8]):

$$R_{\mathcal{A}}(q, \lambda) = f(q),$$

$$R_{\mathcal{A}}(q, \sigma w) = f(q)\ R_{\mathcal{A}}(\delta(q, \sigma), w),$$

for all $q \in Q, \sigma \in \Sigma, w \in \Sigma^*$.

[2] For brevity we will write δ instead of $\overline{\delta}$.

A *Mealy automaton* is a finite automaton with the *output function* μ defined on $Q \times \Sigma$ instead of just Q, i.e., $\mu : Q \times \Sigma \to O$. So, a Mealy automaton is a triple $\mathcal{A} = (Q, \delta, \mu)$. The *response of the Mealy automaton* $\mathcal{A}$ is the function $\mu_{\mathcal{A}} : Q \times \Sigma^* \to O^*$ defined by

$$\mu_{\mathcal{A}}(q, \lambda) = \lambda,$$

$$\mu_{\mathcal{A}}(q, \sigma w) = \mu(q, \sigma)\ \mu_{\mathcal{A}}(\delta(q, \sigma), w),$$

for all $q \in Q, \sigma \in \Sigma, w \in \Sigma^*$.

Let $\mathcal{A} = (Q, \delta, f)$ be a Moore automaton and consider it as a Mealy automaton $\mathcal{A} = (Q, \delta, \mu)$, with the output function defined by $\mu(q, \sigma) = f(q)$, for all $q \in Q,\ \sigma \in \Sigma$. Then, there is an 1-shift translation between Moore and Mealy responses of $\mathcal{A}$:

$$R_{\mathcal{A}}(q, w) = \mu_{\mathcal{A}}(q, w\sigma), \tag{1}$$

for all $q \in Q, w \in \Sigma^*, \sigma \in \Sigma$. Indeed, $\mu_{\mathcal{A}}(q, \sigma) = \mu(q, \sigma) = f(q) = R_{\mathcal{A}}(q, \lambda)$, and assuming that the equation (1) is valid, for all $\varepsilon \in \Sigma$ we get:

$$\begin{aligned} \mu_{\mathcal{A}}(q, \varepsilon w \sigma) &= \mu(q, \varepsilon)\ \mu_{\mathcal{A}}(\delta(q, \varepsilon), w\sigma) \\ &= \mu_{\mathcal{A}}(q, \varepsilon)\ R_{\mathcal{A}}(\delta(q, \varepsilon), w) \\ &= R_{\mathcal{A}}(q, \lambda)\ R_{\mathcal{A}}(\delta(q, \varepsilon), w) \\ &= R_{\mathcal{A}}(q, \varepsilon w). \end{aligned}$$

3 Computational Complementarity

Let $\mathcal{A}$ be a Mealy automaton. Two states $p, q \in Q$ are *distinguishable* in case there exists a word $w \in \Sigma^*$ such that $\mu_{\mathcal{A}}(q, w) \neq \mu_{\mathcal{A}}(p, w)$. Following [8] we say that:

- The automaton $\mathcal{A}$ has property **A** if every pair of distinct states $q, q' \in Q$ is distinguishable.
- The automaton $\mathcal{A}$ has property **B** if for every state $q \in Q$ there exists a word $w \in \Sigma^*$ which distinguishes q from all states $q' \neq q$.
- The automaton $\mathcal{A}$ has property **C** if there exists a word $w \in \Sigma^*$ which distinguishes every distinct states q, q'.

Intuitively, $\mathcal{A}$ has property **A** if any two states have distinct behaviours; $\mathcal{A}$ has property **B** if for every state q there exists a word depending upon q which distinguishes between q and all other states. Finally, $\mathcal{A}$ has property **C** if there exists a word which globally distinguishes between any two states.

Example 1 *Let $\mathcal{A}$ be the Mealy automaton with $Q = \{1, 2, 3\}$, $\Sigma = \{a, b\}$, and $O = \{0, 1\}$, whose transition and output are given by the following tables:*

δ	a	b
1	2	3
2	1	3
3	2	3

μ	a	b
1	1	0
2	0	1
3	1	1

Figure 1.

Then, $\mathcal{A}$ has ***A*** *but not* ***B***.

Proof. We have $\mu_{\mathcal{A}}(1,a) = 1 \neq 0 = \mu_{\mathcal{A}}(2,a)$, $\mu_{\mathcal{A}}(1,b) = 0 \neq 1 = \mu_{\mathcal{A}}(3,b)$ and $\mu_{\mathcal{A}}(2,a) = 0 \neq 1 = \mu_{\mathcal{A}}(3,a)$, hence every pair of distinct states are distinguishable. Therefore $\mathcal{A}$ has property **A**. Let $w \in \Sigma^+$. If $w = aw'$ with $w' \in \Sigma^*$, then $\mu_{\mathcal{A}}(3,w) = \mu(3,a)\mu_{\mathcal{A}}(2,w') = 1\mu_{\mathcal{A}}(2,w') = \mu(1,a)\mu_{\mathcal{A}}(2,w') = \mu_{\mathcal{A}}(1,w)$. If $w = bw'$ with $w' \in \Sigma^*$, then $\mu_{\mathcal{A}}(3,w) = \mu(3,b)\mu_{\mathcal{A}}(3,w') = 1\mu_{\mathcal{A}}(3,w') = \mu(2,b)\mu_{\mathcal{A}}(3,w') = \mu_{\mathcal{A}}(2,w)$. So, there is no word $w \in \Sigma^+$ such that $\mu_{\mathcal{A}}(3,w) \neq \mu_{\mathcal{A}}(1,w)$ and $\mu_{\mathcal{A}}(3,w) \neq \mu_{\mathcal{A}}(2,w)$, therefore the automaton $\mathcal{A}$ has not property **B**. □

Example 1 shows a first type of complementarity, property **A** but not property **B**: any two distinct states of the automaton can be distinguished, but there is at least one state which cannot be distinguished from all the others by any single input word. Measurement of the hypothesis that “the automaton is in state 1” makes impossible the measurement of the hypotheses “the automaton is in state 2” and “the automaton is in state 3”. This is the first principle of complementarity, *CI*: it mimics Heisenberg’s uncertainty (cf. [3]).

Example 2 *Let* $\mathcal{A}$ *be the Mealy automaton with* $Q = \{1,2,3,4\}$, $\Sigma = \{a,b\}$, *and* $O = \{0,1\}$, *whose transition and output are given by the following tables:*

δ	a	b
1	1	1
2	1	4
3	4	2
4	3	2

μ	a	b
1	0	0
2	0	1
3	0	1
4	1	1

Figure 2.

Then, $\mathcal{A}$ has ***B*** *but not* ***C***.

Proof. Let $w_1 = b$, $w_2 = ba$, $w_3 = ab$ and $w_4 = a$. It can be easily verified that $\mu_{\mathcal{A}}(i,w_i) \neq \mu_{\mathcal{A}}(j,w_i)$ for all $i,j \in Q$, $j \neq i$, therefore $\mathcal{A}$ has property **B**.

Let $w \in \Sigma^+$. If $w = aw'$ with $w' \in \Sigma^*$, then $\mu_{\mathcal{A}}(1,w) = \mu(1,a)\mu_{\mathcal{A}}(1,w') = 0\mu_{\mathcal{A}}(1,w') = \mu(2,a)\mu_{\mathcal{A}}(1,w') = \mu_{\mathcal{A}}(2,w)$. If $w = bw'$ with $w' \in \Sigma^*$, then $\mu_{\mathcal{A}}(3,w) = \mu(3,b)\mu_{\mathcal{A}}(2,w') = 1\mu_{\mathcal{A}}(2,w') = \mu(4,b)\mu_{\mathcal{A}}(2,w') = \mu_{\mathcal{A}}(4,w)$. Hence there is no word $w \in \Sigma^+$ which globally distinguishes between every two distinct states, so the automaton $\mathcal{A}$ has not the property **C**. □

Example 2 shows a second type of complementarity: property **B** but not property **C**. Any state of the automaton can be distinguished from the others by a single input word, but there is no unique input word which globally distinguishes between any two distinct states. This is the complementarity principle *CII*: each experiment "generates" a pair of distinct states which exercise a mutual influence, namely they cannot be separated by the experiment w; this influence mimics, in a sense, the state of *quantum entanglement,* and may be conceived as a *toy model* for the *EPR effect* (see [9, 11, 12]), as well as for the *Zou-Wang-Mandel effect* [16]. Under *CII*, for each experiment w we have at least two states q, q' (as distant as we like) which interact via the experiment w: any measurement of q affects q' and, conversely, any measurement of q' affects q.

We present below an automaton having property **C**.

Example 3 *Let $\mathcal{A}$ be the Mealy automaton with $Q = \{1, 2, 3\}$, $\Sigma = \{a, b\}$, and $O = \{0, 1\}$, whose transition and output are given by the following tables:*

δ	a	b
1	2	3
2	1	2
3	2	3

μ	a	b
1	1	0
2	0	1
3	1	1

Figure 3.

Then, $\mathcal{A}$ has ***C***.

Proof. We have $\mu_{\mathcal{A}}(1, ba) = 01$, $\mu_{\mathcal{A}}(2, ba) = 10$ and $\mu_{\mathcal{A}}(3, ba) = 11$, therefore the word ba globally distinguishes between any two distinct states. Hence $\mathcal{A}$ has property **C**. □

The coherence between the definition of properties **A**, **B**, **C** for Moore and Mealy automata is stated in the following proposition.

Proposition 4 *Let $\mathcal{A} = (Q, \delta, f)$ be a Moore automaton and consider it as a Mealy automaton $\mathcal{A}' = (Q, \delta, \mu)$, where $\mu(q, \sigma) = f(q)$, for all $q \in Q$, $\sigma \in \Sigma$. Then, $\mathcal{A}$ has **A** (respectively, **B**, **C**) if and only if $\mathcal{A}'$ has **A** (respectively, **B**, **C**).*

Proof. In view of (1), for every states $p, q \in Q$, p and q are distinguishable in $\mathcal{A}$ if and only if $R_{\mathcal{A}}(p, w) \neq R_{\mathcal{A}}(q, w)$, for some $w \in \Sigma^*$ if and only if $\mu_{\mathcal{A}}(p, w\sigma) \neq \mu_{\mathcal{A}}(q, w\sigma)$, for some $w \in \Sigma^*$ and $\sigma \in \Sigma$ if and only if p and q are distinguishable in $\mathcal{A}'$. □

A morphism between the automata $\mathcal{A} = (Q, \delta, \mu)$ and $\mathcal{A}' = (Q', \delta', \mu')$ is a function $h : Q \to Q'$ such that

$$h(\delta(q, \sigma)) = \delta'(h(q), \sigma), \quad \text{for all } q \in Q, \sigma \in \Sigma,$$

$$\mu(q, \sigma) = \mu'(h(q), \sigma), \quad \text{for all } q \in Q, \sigma \in \Sigma.$$

Two Mealy automata $\mathcal{A}$ and $\mathcal{A}'$ are isomorphic in case there exists a bijective morphism $h : \mathcal{A} \to \mathcal{A}'$.

Proposition 5 *If $\mathcal{A}$ and $\mathcal{A}'$ are two Mealy automata, $\mathcal{A}$ has property* ***A*** *and $h : \mathcal{A} \to \mathcal{A}'$ is a morphism, then h is injective.*

Proof. Suppose $h(q) = h(q')$ with $q, q' \in Q$ and $q \neq q'$. Then $\mu(q, \sigma) = \mu'(h(q), \sigma) = \mu'(h(q'), \sigma) = \mu(q', \sigma)$ for all $\sigma \in \Sigma$ and $h(\delta(q, \sigma)) = \delta'(h(q), \sigma) = \delta'(h(q'), \sigma) = h(\delta(q', \sigma))$, for all $\sigma \in \Sigma$ as h is a morphism.

Since $\mathcal{A}$ has property **A**, there exists $w = \sigma_1 \ldots \sigma_n \in \Sigma^*$ such that $\mu_{\mathcal{A}}(q, w) \neq \mu_{\mathcal{A}}(q', w)$. Let $q_1 = \delta(q, \sigma_1)$ and $q'_1 = \delta(q', \sigma_1)$. Then $h(q_1) = h(\delta(q, \sigma_1)) = h(\delta(q', \sigma_1)) = h(q'_1)$. Inductively define $q_i = \delta(q_{i-1}, \sigma_i)$ and $q'_i = \delta(q'_{i-1}, \sigma_i)$, for $i = 2, \ldots, n$. We then deduce that

$$
\begin{aligned}
\mu_{\mathcal{A}}(q, w) &= \mu_{\mathcal{A}}(q, \sigma_1 \ldots \sigma_n) \\
&= \mu(q, \sigma_1)\mu_{\mathcal{A}}(q_1, \sigma_2 \ldots \sigma_n) \\
&= \mu(q, \sigma_1)\mu(q_1, \sigma_2) \ldots \mu(q_{n-1}, \sigma_n) \\
&= \mu(q', \sigma_1)\mu(q'_1, \sigma_2) \ldots \mu(q'_{n-1}, \sigma_n) \\
&= \mu_{\mathcal{A}}(q', w),
\end{aligned}
$$

which contradicts the relation $\mu_{\mathcal{A}}(q, w) \neq \mu_{\mathcal{A}}(q', w)$. Therefore $q = q'$, so h is injective. □

Lemma 6 *If h is a morphism between the Mealy automata $\mathcal{A} = (Q, \delta, \mu)$ and $\mathcal{A}' = (Q', \delta', \mu')$, then the following relation holds for all $q \in Q, w \in \Sigma^*$:*

$$\mu_{\mathcal{A}}(q, w) = \mu_{\mathcal{A}'}(h(q), w).$$

Proof. The proof follows by induction on w. □

Corollary 7 *If two Mealy automata are isomorphic and one of them has* ***A*** *(**B** or **C**), then the other has the same property.*

Proof. We use Lemma 6 to show that if two states p and q are distinguishable in $\mathcal{A}$ by the input w and h is the isomorphism between $\mathcal{A}$ and $\mathcal{A}'$, then w distinguishes $h(p)$ and $h(q)$ in $\mathcal{A}'$. □

4 When Computational Complementarity Disappears?

It is obvious that **C** implies **B** and **B** implies **A**. A natural question is: when are the properties **A**, **B** and **C** equivalent, i.e., when both computational complementarity principles disappear? We shall partially answer this question using an algebraic approach.

Let us consider the Mealy automaton $\mathcal{A} = (Q, \delta, \mu)$ and the operators $(T_w)_{w \in \Sigma^*}$ defined by

$$T_w : Q \to Q, \quad T_w(q) = \delta(q, w), \quad \text{for all } q \in Q.$$

Since $T_u \circ T_v = T_{uv}$, for all $u, v \in \Sigma^*$ and T_λ is neutral element for the composition law, the class of operators $(T_w)_{w\in\Sigma^*}$ is a finite monoid called the transition monoid of the automaton $\mathcal{A}$.

The proof of the following result was given in [3] for the case of Moore automata; it can be easily extended to Mealy automata as well.

Proposition 8 *If the transition monoid of the Mealy automaton $\mathcal{A}$ is a group, then properties **A**, **B** and **C** are equivalent for $\mathcal{A}$.*

In fact, for Moore automata a stronger result is valid:

Theorem 9 *If the transition semigroup $(T_w)_{w\in\Sigma^+}$ of the Moore automaton $\mathcal{A} = (Q, \delta, f)$ is a group, then properties **A**, **B** and **C** are equivalent.*

Proof. Let T_τ be the neutral element of the group $(T_u)_{u\in\Sigma^+}$, with $\tau \in \Sigma^+$. Then for all $u \in \Sigma^+$ we have $T_{u\tau} = T_{\tau u} = T_u$ and there exists $\bar{u} \in \Sigma^+$ such that $T_{u\bar{u}} = T_{\bar{u}u} = T_\tau$. If the automaton $\mathcal{A}$ has **A**, then for each pair of states $q_1 \neq q_2$ there exists a word $w_{q_1,q_2} \in \Sigma^+$ such that $\mu_\mathcal{A}(q_1, w_{q_1,q_2}) \neq \mu_\mathcal{A}(q_2, w_{q_1,q_2})$. We concatenate all words $w_{q_1,q_2}\overline{w_{q_1,q_2}}$ with $q_1 \neq q_2$ and we get a word $w \in \Sigma^+$. We shall prove that $\mu_\mathcal{A}(q_1, w) \neq \mu_\mathcal{A}(q_2, w)$, for all distinct states q_1 and q_2.

There are two cases to consider depending on whether the equality $T_\tau(q_1) = T_\tau(q_2)$ is valid or not.

If $T_\tau(q_1) = T_\tau(q_2)$ then for all $\sigma \in \Sigma$ we have

$$T_\sigma(q_1) = T_{\sigma\tau}(q_1) = T_\sigma(T_\tau(q_1)) = T_\sigma(T_\tau(q_2)) = T_{\sigma\tau}(q_2) = T_\sigma(q_2).$$

Therefore $\delta(q_1, \sigma) = \delta(q_2, \sigma)$, for all $\sigma \in \Sigma$. But $R_\mathcal{A}(q_1, w_{q_1,q_2}) \neq R_\mathcal{A}(q_2, w_{q_1,q_2})$, hence $f(q_1) \neq f(q_2)$. Then obviously $R_\mathcal{A}(q_1, w) \neq R_\mathcal{A}(q_2, w)$ (because their first letters are different).

If $T_\tau(q_1) \neq T_\tau(q_2)$, let $q_1' = T_\tau(q_1)$ and $q_2' = T_\tau(q_2)$. Since $q_1' \neq q_2'$ and $\mathcal{A}$ has **A**, there exists a word $w_{q_1',q_2'} \in \Sigma^+$ such that $R_\mathcal{A}(q_1', w_{q_1',q_2'}) \neq R_\mathcal{A}(q_2', w_{q_1',q_2'})$. Let $w = w_1 w_{q_1',q_2'}\overline{w_{q_1',q_2'}}w_2$, with $w_1, w_2 \in \Sigma^+$. The prefix w_1 and the suffix w_2 have the same form as w, since they are obtained by the concatenation of some $w_{q_i,q_j}\overline{w_{q_i,q_j}}$ with $q_i \neq q_j$.

We shall first prove that $\delta(q_1, w_1) = T_\tau(q_1) = q_1'$ and $\delta(q_2, w_1) = T_\tau(q_2) = q_2'$. Suppose that $w_1 = w_{q_{i_1},q_{j_1}}\overline{w_{q_{i_1},q_{j_1}}} \dots w_{q_{i_k},q_{j_k}}\overline{w_{q_{i_k},q_{j_k}}}$, where $q_{i_1} \neq q_{j_1}, \dots, q_{i_k} \neq q_{j_k}$. We have

$$T_{w_{q_{i_1},q_{j_1}}\overline{w_{q_{i_1},q_{j_1}}}}(q_1) = T_\tau(q_1) = q_1',$$

since T_τ is the neutral element of the group $(T_u)_{u\in\Sigma^+}$. Also,

$$T_{w_{q_{i_2},q_{j_2}}\overline{w_{q_{i_2},q_{j_2}}}}(q_1') = \cdots = T_{w_{q_{i_k},q_{j_k}}\overline{w_{q_{i_k},q_{j_k}}}}(q_1') = T_\tau(q_1') = q_1',$$

since $T_\tau(q_1') = T_\tau(T_\tau(q_1)) = T_{\tau\tau}(q_1) = T_\tau(q_1) = q_1'$. Then $\delta(q_1, w_1) = T_{w_1}(q_1) = T_\tau^k(q_1) = T_\tau^{k-1}(T_\tau(q_1)) = T_\tau^{k-1}(q_1') = q_1'$. In the same manner it follows that $\delta(q_2, w_1) = T_\tau(q_2) = q_2'$.

Then

$$\begin{aligned} R_\mathcal{A}(q_1, w) &= R_\mathcal{A}(q_1, w_1 w_{q_1',q_2'}\overline{w_{q_1',q_2'}}w_2) \\ &= f(q_1)w_1' R_\mathcal{A}(\delta(q_1, w_1), w_{q_1',q_2'}\overline{w_{q_1',q_2'}}w_2) \\ &= f(q_1)w_1' R_\mathcal{A}(q_1', w_{q_1',q_2'}\overline{w_{q_1',q_2'}}w_2). \end{aligned}$$

Similarly,

$$R_{\mathcal{A}}(q_2, w) = f(q_2)w_2' R_{\mathcal{A}}(q_2', w_{q_1',q_2'}\overline{w_{q_1',q_2'}}w_2),$$

with $|f(q_1)w_1'| = |f(q_2)w_2'| = |w_1|+1$. If $f(q_1)w_1' \neq f(q_2)w_2'$, then $R_{\mathcal{A}}(q_1, w) \neq R_{\mathcal{A}}(q_2, w)$. If $f(q_1)w_1' = f(q_2)w_2'$, since $R_{\mathcal{A}}(q_1', w_{q_1',q_2'}) \neq R_{\mathcal{A}}(q_2', w_{q_1',q_2'})$, it follows again that $R_{\mathcal{A}}(q_1, w) \neq R_{\mathcal{A}}(q_2, w)$.

We have proved that the word w globally distinguishes between any two distinct states, therefore M has property C. □

Remark. Theorem 9 is stronger than the corresponding Proposition 8 for Moore automata. Indeed, if the transition monoid is a group, then the transition semigroup $(T_w)_{w\in\Sigma^+}$ is also a group, but the converse implication fails to be true (see Example 10). If the transition monoid is a group, then every operator T_σ ($\sigma \in \Sigma$) is a permutation (see [3]), so there is a word $u \in \Sigma^+$ such that T_u is the identity, which shows that the transition semigroup is also a group.

Theorem 9 is no longer true for all Mealy automata, as the following counterexample shows.

Example 10 *The automaton with* $Q = \{1, 2, 3, 4\}$, $\Sigma = \{a, b\}$ *and* $O = \{0, 1\}$, *with transitions and outputs given by:*

δ	a	b
1	1	3
2	3	1
3	3	1
4	1	3

μ	a	b
1	1	0
2	0	1
3	1	1
4	1	1

Figure 4.

has a group transition $(T_w)_{w\in\Sigma^+}$, *but it has* ***B*** *and not* ***C***.

Proof. Let $w_1 = b$, $w_2 = a$, $w_3 = ab$ and $w_4 = bb$. It can be easily verified that $\mu_{\mathcal{A}}(i, w_i) \neq \mu_{\mathcal{A}}(j, w_i)$ for all $i, j \in Q$, $j \neq i$, therefore $\mathcal{A}$ has property **B**.

Let $w \in \Sigma^+$. If $w = aw'$ with $w' \in \Sigma^*$, then $\mu_{\mathcal{A}}(4, w) = \mu(4, a)\mu_{\mathcal{A}}(1, w') = 1\mu_{\mathcal{A}}(1, w') = \mu(1, a)\mu_{\mathcal{A}}(1, w') = \mu_{\mathcal{A}}(1, w)$. If $w = bw'$ with $w' \in \Sigma^*$, then $\mu_{\mathcal{A}}(2, w) = \mu(2, b)\mu_{\mathcal{A}}(1, w') = 1\mu_{\mathcal{A}}(1, w') = \mu(3, b)\mu_{\mathcal{A}}(1, w') = \mu_{\mathcal{A}}(3, w)$. It follows that there is no word $w \in \Sigma^+$ which globally distinguishes between every two distinct states, so the automaton $\mathcal{A}$ has not **C**.

However, $T_{ab} = T_{ba} = T_b$ and $T_{aa} = T_{bb} = T_a$, so that the transition semigroup $(T_w)_{w\in\Sigma^+}$ is a group. □

5 Decidability of Properties A, B and C

In this paragraph we are going to work with Moore automata with initial and final states, as our main aim is to represent properties **A**, **B** and **C** in terms of regular languages. Let $\mathcal{A} = (Q, \delta, \mu)$ be a Mealy automaton and let $\natural$ be a symbol which does not belong to Q. We consider the class of finite deterministic automata $(\mathcal{A}_q)_{q \in Q}$ given by

$$\mathcal{A}_q = (Q \cup \{\natural\}, \Sigma \times \Sigma,\ q, \delta', Q),$$

with final states Q, initial state q and the transition function

$$\delta'(p, (\sigma, \tau)) = \begin{cases} \delta(p, \sigma), & \text{if } \mu(p, \sigma) = \tau, \\ \natural, & \text{otherwise,} \end{cases} \qquad \text{for all } p \in Q, \sigma, \tau \in \Sigma.$$

Extending a result from [3] it can be easily shown that every distinct states p and q from Q are distinguishable if and only if the languages accepted by the automata $\mathcal{A}_p$ and $\mathcal{A}_q$ are different, i.e., $L(\mathcal{A}_p) \neq L(\mathcal{A}_q)$.

Proposition 11 *Properties **A**, **B** and **C** are algorithmically decidable for Mealy automata.*

Proof. From the construction of automata $(\mathcal{A}_q)_{q \in Q}$ it follows that **A** is true if and only if

$$(L(\mathcal{A}_q) \setminus L(\mathcal{A}_p)) \cup (L(\mathcal{A}_p) \setminus L(\mathcal{A}_q)) \neq \emptyset, \quad \text{for all } p, q \in Q,\ p \neq q,$$

B is true if and only if

$$\left(L(\mathcal{A}_q) \setminus \bigcup_{p \neq q} L(\mathcal{A}_p) \right) \bigcup \left(\bigcap_{p \neq q} L(\mathcal{A}_p) \setminus L(\mathcal{A}_q) \right) \neq \emptyset, \quad \text{for all } q \in Q,$$

and **C** is true if and only if

$$\bigcap_{p \neq q} (L(\mathcal{A}_q) \setminus L(\mathcal{A}_p)) \cup (L(\mathcal{A}_p) \setminus L(\mathcal{A}_q)) \neq \emptyset.$$

Since $L(\mathcal{A}_q)$ is a regular language for all $q \in Q$, the class of regular languages is closed under difference, union and intersection and the emptiness property of a regular language is decidable, we deduce that properties **A**, **B** and **C** are algorithmically decidable. □

6 Reversibility and Computational Complementarity

An operation is reversible if can be undone; it is simply determinism looking backwards in time. Conventional computers are irreversible, and constantly discard information about their states. Since the laws of physics are reversible at a microscopic level (a given microstate can only be reached by a single path) it follows that irreversible operations and the accompanying production of entropy are in principle not necessary.[3] The world's first fully adiabatic and reversible universal computer was presented by Frank, Vieri, Ammer, Love, Margolus, Knight [10, 5]: working with a parallel and scalable architecture, ignoring leakage and power supply issues one can show that the machine can perform any computation using arbitrarily little energy per operation.

As a consequence the lesson taught by quantum mechanics is reinforced: we have to restrict ourselves to one-to-one computational operations and exclude one-to-many ones (e.g., copying). Following Svozil [15] we are going to be interested in Mealy automata $\mathcal{A} = (Q, \delta, \mu)$ for which the function $\Gamma : Q \times \Sigma \to Q \times O$ defined by $\Gamma(q, \sigma) = (\delta(q, \sigma), \mu(q, \sigma))$ is bijective.[4] This is Svozil's definition of "reversibility" for Mealy automata.

First notice that there exist $(m \cdot n)!$ reversible Mealy automata with n states working on an alphabet with m symbols. However, it may be the case that for some pair Σ, Q no Moore automaton (Q, δ, f) is Svozil reversible.

Proposition 12 *A necessary and sufficient condition for the existence of a Svozil reversible Moore automaton is that the automaton has an even number of states.*

Proof. For simplicity assume that $\Sigma = \{a, b\}$, $O = \{0, 1\}$. If $Q = \{1, 2, \ldots, 2k\}$, then the Moore automaton corresponding to the function Γ defined by $\Gamma(1, a) = (1, 0)$, $\Gamma(2, a) = (2, 0), \ldots, \Gamma(k, a) = (k, 0)$, $\Gamma(k+1, a) = (1, 1), \ldots, \Gamma(2k, a) = (k, 1)$, $\Gamma(1, b) = (k+1, 0), \ldots, \Gamma(k, b) = (2k, 0), \Gamma(k+1, b) = (k+1, 1), \ldots, \Gamma(2k, b) = (2k, 1)$ is Svozil reversible.

Conversely, if a Moore automaton (Q, δ, f) is Svozil reversible and $\#(Q) = 2k+1$, then $\#(\Gamma(Q \times \Sigma)) < \#(Q \times \Sigma)$ which shows that Γ is not bijective. Indeed, take $Q_0 = \{q \in Q \mid f(q) = 0\}$ and notice that $\max\{\#(Q_0), \#(Q \setminus Q_0)\} \geq k+1$. Assume that $\#(Q_0) \geq k+1$. The restriction of Γ to $Q_0 \times \Sigma$ produces always pairs $(p, 0)$. Consequently, $\#\Gamma(Q_0 \times \Sigma) \geq 2k+2$, and $\{\Gamma(q, \sigma) \mid q \in Q_0, \sigma \in \Sigma\} \subset \{(p, 0) \mid p \in Q\}$. We have reached a contradiction, as the set in the left-hand side has at least $2k+2$ elements while the set on the right-hand side has $2k+1$ elements. □

What is the relation between Svozil reversibility and computational complementarity principles *CI, CII*? Svozil's analysis in [15] suggests the following conjecture: *no Mealy automaton satisfying CI or CII is Svozil reversible.* Using Mathematica 3.0 ([17]) we have tested this conjecture for Mealy automata defined on a binary alphabet Σ and having 3 and 4 states; we also performed random tests for automata with 5 and 6 states. All these experiments confirmed our conjecture.

---

[3] Karl Svozil, in an email sent to C.S. Calude on 29 April 1998, comments: "In an uniformly reversible environment (also the measurement apparatus is reversible), my suspicion is that there is no such "free lunch" scenario: one has to decide either to swallow the measurement result (exclusive) or develop the automaton backward. But I have no proof of that."

[4] This can be realised in case Σ and O have the same number of elements. If we require only injectivity we need to make sure that O has at least as many elements as Σ.

Acknowledgement

We thank R. Nicolescu and K. Svozil for comments and bibliographical suggestions.

References

[1] Buks, E., Schuster, R., Heiblum, M., Mahalu, D., and Umansky, V. Dephasing in electron interference by a 'which-path' detector. *Nature* 391 (1998), 871–874.

[2] Calude, C., Calude, E., and Khoussainov, B. Deterministic automata: simulation, universality and minimality. *Annals of Pure and Applied Logic 90, 1-3* (1997), 263–276.

[3] Calude, C., Calude, E., Svozil, K., and Yu, S. Physical versus computational complementarity I. *International Journal of Theoretical Physics 36* (1997), 1495–1523.

[4] Calude, C. S., Casti, J., and Dinneen, M. J. *Unconventional Methods of Computation*. Springer, Singapore, 1998.

[5] Calude, C. S., and Casti, J. L. Parallel thinking. *Nature 392* (1998), 549–551.

[6] Calude, C. S., and Lipponen, M. Computational complementarity and sofic shifts. In *Theory of Computing 98, Proceedings of the 4th Australasian Theory Symposium, CATS'98* (Perth, 1998), X. Lin, Ed., Springer, Singapore, 1998, pp. 277–290.

[7] Calude, E., and Lipponen, M. Minimal deterministic incomplete automata. *J. UCS 11* (1997), 1180–1193.

[8] Calude, E., and Lipponen, M. Deterministic incomplete automata: Simulation, universality and complementarity. In *Unconventional Models of Computation* (Auckland, 1998), C. S. Calude, J. Casti, and M. J. Dinneen, Eds., Springer, Singapore, 1998, pp. 131–149.

[9] Einstein, A., Podolsky, B., and Rosen, N. Can quantum-mechanical description of physical reality be considered complete? *Physical Review 47* (1935), 777–780.

[10] Frank, M., Vieri, C., Ammer, M. A., Love, N., Margolus, N. H., Knight, T. F. A scalable reversible computer in silicon. In *Unconventional Models of Computation* (Auckland, 1998), C. S. Calude, J. Casti, and M. J. Dinneen, Eds., Springer, Singapore, 1998, pp. 183–200.

[11] Penrose, R. *The Emperor's New Mind: Concerning Computers, Minds, and the Laws of Physics*. Oxford University Press, Oxford, 1990.

[12] Penrose, R. *Shadows of the Minds, A Search for the Missing Science of Consciousness*. Oxford University Press, Oxford, 1994.

[13] Schaller, M., and Svozil, K. Automaton partition logic versus quantum logic. *International Journal of Theoretical Physics 34*, 8 (August 1995), 1741–1750.

[14] Svozil, K. *Randomness & Undecidability in Physics*. World Scientific, Singapore, 1993.

[15] Svozil, K. The Church-Turing Thesis as a guiding principle. In *Unconventional Models of Computation* (Auckland, 1998), C. S. Calude, J. Casti, and M. J. Dinneen, Eds., Springer, Singapore, 1998, pp. 371–385.

[16] Wang, L. J., Zou, X. Y., and Mandel, L. Induced coherence without induced emission. *Physical Review A44* (1991), 4614–4622.

[17] Wolfram, S. *Mathematica, A System for Doing Mathematics by Computer*, third edition, Cambridge University Press, Cambridge, 1996.