CDMTCS Research Report Series

Computational Complementarity and Sofic Shifts

Cristian S. Calude
Marjo Lipponen
Department of Computer Science
University of Auckland
Auckland, New Zealand

CDMTCS-053
August 1997

Centre for Discrete Mathematics and
Theoretical Computer Science

Computational Complementarity and Sofic Shifts *

Cristian S. Calude[†] and **Marjo Lipponen**[‡]

Abstract

Finite automata (with outputs but no initial states) have been extensively used as models of computational complementarity, a property which mimics the physical complementarity. All this work was focussed on "frames", i.e., on fixed, static, local descriptions of the system behaviour. In this paper we are mainly interested in the asymptotical description of complementarity. To this aim we will study the asymptotical behaviour of two complementarity principles by associating to every incomplete deterministic automaton (with outputs, but no initial state) certain sofic shifts: automata having the same behaviour correspond to a unique sofic shift. In this way, a class of sofic shifts reflecting complementarity will be introduced and studied. We will prove that there is a strong relation between "local complementarity", as it is perceived at the level of "frames", and "asymptotical complementarity" as it is described by the sofic shift.

Key words: Complementarity principles, finite automata, sofic shifts.

1 Motivation

Physical systems are normally described by measurements. For example, a gas is described by the position and momentum of its molecules and a swinging pendulum is characterized by its angle from the vertical and its angular velocity. In the simplest case the set of possible values describing a system can be arranged in a sequence, a film which is infinite in both directions: each frame of the film—describing the system in a fixed interval of time—depends upon the previous one, usually in a continuous way.

The notion of measurement is strongly connected to physical complementarity: the observer either experiences one certain type of observation, (exclusive) or a different, complementary one. The "folklore" understanding of complementarity, in general, and of Heisenberg's uncertainty relation, in particular, is the existence of certain (complementary) features of quantum systems which cannot be measured and predicted simultaneously with arbitrary accuracy. In other words, any description of properties of microscopic objects in classical terms generates pairs of complementary variables; the accuracy in one member

*The first author was partially supported by AURC Grant A18/XXXXX/62090/F3414069. The second author is supported by Alfred Kordelin Foundation.

[†]Computer Science Department, The University of Auckland, Private Bag 92109, Auckland, New Zealand, e-mail: cristian@cs.auckland.ac.nz.

[‡]Computer Science Department, The University of Auckland, Private Bag 92109, Auckland, New Zealand; on leave from the Department of Mathematics, University of Turku, Finland; e-mail: marjo@cs.auckland.ac.nz.

of the pair cannot be improved without a corresponding loss in the accuracy of the other member.

Extensive work done by various authors (e.g. Moore [18], Ginsburg [12], Gill [11], Chaitin [6], Conway [7], Finkelstein and Finkelstein [8], Brauer [2], Grib and Zapatrin [14], Schaller and Svozil [20, 21], Svozil [22], Calude, Calude, Svozil, Yu [4], Calude, Calude and Khoussainov [3], Calude and Lipponen [5]) was devoted to modeling physical complementarity by computational complementarity, i.e., by means of complementarity properties displayed by various types of finite automata. All this quoted work was focussed on "frames", i.e., on fixed, static, local descriptions of the system behaviour. In this paper we take another view as we are mainly interested in the asymptotical description of complementarity. We will study the asymptotical behaviour of two complementarity principles—motivated by Moore's work [18] (see also Conway [7, p. 21] and Svozil [22]) and introduced by Calude, Calude, Svozil, Yu [4]—by associating to every incomplete deterministic automaton (with output, but no initial state)—studied in Calude and Lipponen [5]—certain sofic shifts. A class of sofic shifts reflecting complementarity will be introduced and studied. We will prove that there is a strong relation between "local complementarity", as it is perceived at the level of "frames", and "asymptotical complementarity" as it is described by the sofic shift, as automata having the same behaviour correspond to a unique sofic shift.

2 Notations

If S is a finite set, then $|S|$ denotes the cardinality of S. A **partial** function $f : A \stackrel{\circ}{\to} B$ is a function defined for some elements from A. In case f is not defined on $a \in A$ we write $f(a) = \infty$. Let $D(f) = \{a \in A \mid f(a) \neq \infty\}$ denote the domain of f. If $D(f) = A$, we say that f is **total**. Two partial functions f and g are equal, when $D(f) = D(g)$ and $f(a) = g(a)$, for every $a \in D(f)$. For any two sets A and B, we denote their symmetrical difference by $\triangle$, $A \triangle B = (A \setminus B) \cup (B \setminus A)$. If Σ is a finite set, called alphabet, then Σ^* stands for the set of all finite words over Σ and the empty word, denoted by λ, whereas $\Sigma^{\mathbb{Z}}$ is the set of all bi-infinite words over Σ. An element of $\Sigma^{\mathbb{Z}}$ is a sequence $x = (x_n)_{n\in\mathbb{Z}} = \ldots x_{-1}x_0x_1 \ldots$

Let Σ and O be two finite, nonempty alphabets; Σ is the set of **input** symbols, and O the set of **output** symbols. A **deterministic (finite) incomplete automaton** over the alphabets Σ and O is a system $A = (S_A, \Delta_A, F_A)$, where the **set of states** S_A is a finite, nonempty set, the **transition table** Δ_A is a partial function from $S_A \times \Sigma$ to the set of states S_A, and the **output function** F_A is a total mapping from the set of states S_A into output alphabet O.

The transition diagram Δ_A is naturally extended to a partial function, $\Delta_A : S_A \times \Sigma^* \stackrel{\circ}{\to} S_A$ as follows: for every $s \in S_A$, $w \in \Sigma^*$ and $\sigma \in \Sigma$, $\Delta_A(s, \lambda) = s$, and $\Delta_A(s, \sigma w) = \Delta_A(\Delta_A(s, \sigma), w)$ if $\Delta_A(s, \sigma) \neq \infty$.

Furthermore, for all $p \in S_A$, the set $W_A(p) = \{w \in \Sigma^* \mid \Delta_A(p, w) \neq \infty\}$ consists of all words leading to complete computations on state p. Following Ginsburg [13], we say that a word u is **applicable to** the state p if $u \in W_A(p)$.

If Δ_A is a total function, we will say that the automaton A is **complete**, so every complete automaton is a special case of an incomplete automaton.

An automaton $A = (S_A, \Delta_A, F_A)$ is **strongly connected** if for every pair of states $p, q \in S_A$ there is a word $w \in W_A(p)$ such that $\Delta_A(p, w) = q$.

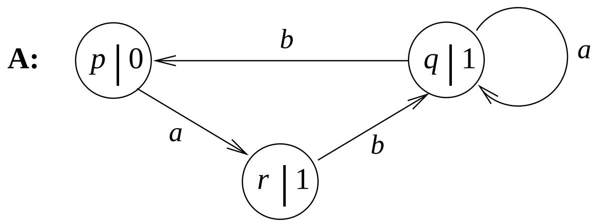
In this paper we will deal only with *strongly connected deterministic incomplete automata*, shortly automata, if not otherwise stated.

Following Calude and Lipponen [5], the **response** of an automaton $A = (S_A, \Delta_A, F_A)$ to an **input signal** is the partial function $R_A : S_A \times \Sigma^* \overset{\circ}{\to} O^*$ defined such that for every $s \in S_A$, $R_A(s, \lambda) = F_A(s)$, and

$$R_A(s, \sigma_1 \dots \sigma_n) = F_A(s)F_A(\Delta_A(s, \sigma_1))F_A(\Delta_A(s, \sigma_1\sigma_2)) \dots F_A(\Delta_A(s, \sigma_1 \dots \sigma_n)),$$

if $\sigma_1 \dots \sigma_n \in W_A(s)$, $\sigma_i \in \Sigma$, $n \geq 1$ and $1 \leq i \leq n$.

Example 2.1 Let $\Sigma = \{a, b\}$, $O = \{0, 1\}$, and consider the three-state automaton A presented below. The state p emits an output 0, $F_A(p) = 0$, and the states q and r emit



an output 1, $F_A(q) = F_A(r) = 1$. The responses to an input aba are $R_A(p, aba) = 0111$, $R_A(q, aba) = 1101$, and $R_A(r, aba) = \infty$.

Responses are used in Calude and Lipponen [5] to define the behavioral simulation (shortly β-simulation) of an automaton by another one, meaning that an automaton can perform all computations performed by another automaton. Formally, let $A = (S_A, \Delta_A, F_A)$ and $B = (S_B, \Delta_B, F_B)$ be two automata. Then A is **β-simulated** by B if there is a mapping $h : S_A \to S_B$ such that for all $s \in S_A$, $W_A(s) = W_B(h(s))$, and $R_A(s, w) = R_B(h(s), w)$, for all $w \in W_A(s)$. If A and B both β-simulate each other, we say that A and B are **β-equivalent**. If, moreover, the mapping $h : S_A \to S_B$ is one-to-one and onto, and for all $s \in S_A$ and $\sigma \in W_A(s) \cap \Sigma$, $h(\Delta_A(s, \sigma)) = \Delta_B(h(s), \sigma)$, then A and B are **isomorphic**. An automaton A is **minimal** if every automaton B which is β-equivalent to A has at least as many states as A, $|S_A| \leq |S_B|$.

3 Computational Complementarity

Following the study initiated in Moore [18], think of an automaton as a black box. Assume that we want to "distinguish" between two states p and q of the automaton A by means of a "measurable experiment", i.e. by the responses of the automaton to an input $w \in \Sigma^*$. Following Calude and Lipponen [5], we say that the experiment is *not relevant* if it is applicable to neither p nor q; hence, another experiment is required. On the other hand, if the experiment is *relevant* then we have three further possibilities: w is applicable to either p or q but not to both, or $R_A(p, w) \neq R_A(q, w)$, or $R_A(p, w) = R_A(q, w)$. In the first two cases w *distinguishes* between p and q, and in the third case w *does not distinguish* between p and q. To summarise, w distinguishes between p and q if $R_A(p,w) \neq R_A(q,w)$ (meaning that either w is applicable to both p and q and the responses are different or w is applicable to only one of the states). In the remaining cases, w may not distinguish or may not be relevant for distinguishing between p and q.

Consequently, two states $p, q \in S_A$ of an automaton $A = (S_A, \Delta_A, F_A)$ are **indistinguishable** iff

$$W_A(p) = W_A(q) \quad \text{and} \quad R_A(p,w) = R_A(q,w), \text{ for all } w \in W_A(p).$$

If the states p and q are not indistinguishable, we say that they are **distinguishable**, and every word from the set

$$\{w \in W_A(p) \cup W_A(q) \mid R_A(p,w) \neq R_A(q,w)\}$$

is said to **distinguish** between p and q. Hence a word w **cannot distinguish** between p and q if $R_A(p,w) = R_A(q,w)$ or $w \notin W_A(p) \cup W_A(q)$.

Following the terminology of Calude, Calude, Svozil, Yu [4], we now define the properties **A**, **B**, **C** (for an automaton A) as follows:

A Every pair of the distinct states of A are distinguishable.

B For every state p of A there exists a word which distinguishes p from all the other states.

C There exists a word which distinguishes between any two distinct states of A.

(These properties are decidable, see Calude, Calude, Svozil, Yu [4] and Calude and Lipponen [5].)

According to Calude and Lipponen [5], an automaton is minimal iff it has property **A**, that is all its states are distinguishable. In fact, since indistinguishability is an equivalence relation, using equivalence classes of states we can construct a minimal automaton $M(A)$ for every automaton A: $M(A)$ is β-equivalent to A and has a minimal number of states.

Two complementarity principles can now be defined: CI means that an automaton has **A** but not **B** and CII means that an automaton has **B** but not **C**.

4 Shift Spaces

A subset X of $\Sigma^{\mathbb{Z}}$ is a **shift space** if it is topologically closed (with respect to the natural metric on $\Sigma^{\mathbb{Z}}$) and shift invariant, $\sigma(X) = X$, where $\sigma : \Sigma^{\mathbb{Z}} \to \Sigma^{\mathbb{Z}}$ is the **shift transformation** $\sigma(x)_i = x_{i+1}$. The set $\Sigma^{\mathbb{Z}}$ is called the **full shift**. The **language** of a shift X is the set $\mathcal{B}(X)$ of all subwords of sequences in X. Two shift spaces X and Y are **conjugate** if there is a one-to-one onto morphism $\phi : X \to Y$ which commutes with the shift transformation, $\phi \circ \sigma_X = \sigma_Y \circ \phi$. For more details, see Lind and Marcus [17].

To each automaton $A = (S_A, \Delta_A, F_A)$ we associate three shift spaces (of bi-infinite sequences):

1) the **automaton shift**,

$$\mathcal{S}_A = \{(q_i, a_i, x_i)_{i\in\mathbb{Z}} \mid q_i \in S_A, a_i \in \Sigma, x_i \in O, \Delta_A(q_i, a_i) = q_{i+1}, x_i = F_A(q_i)\},$$

2) the **label-output shift**,

$$\mathcal{S}_A^{\Sigma,O} = \{(a_i, x_i)_{i\in\mathbb{Z}} \mid (q_i, a_i, x_i) \in \mathcal{S}_A, \text{ for some } (q_i)\},$$

3) the **output shift**,

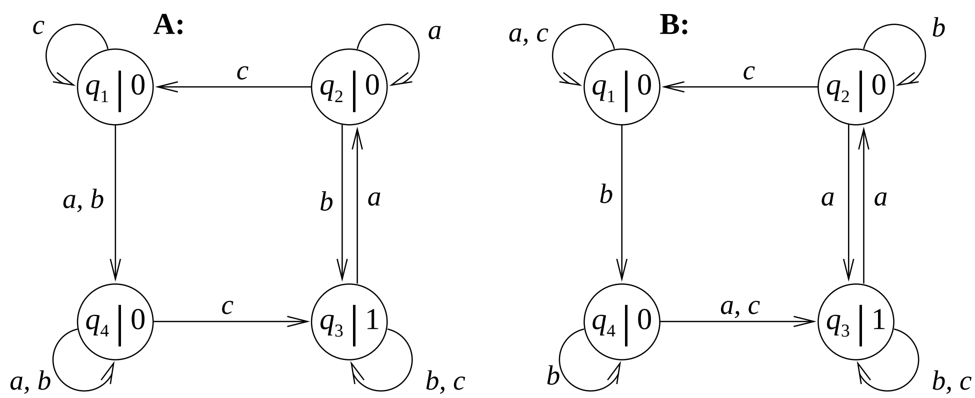
$$\mathcal{S}_A^{O} = \{(x_i)_{i\in\mathbb{Z}} \mid (q_i, a_i, x_i) \in \mathcal{S}_A, \text{ for some } (q_i) \text{ and } (a_i)\}.$$

Other relations between finite automata (with initial states) and sofic shifts were explored by various authors; see Béal and Perrin [1], Kůrka [15, 16] and Perrin [19].

In what follows we are mainly interested in expressing complementarity principles of automata in terms of their induced shifts. The first result proves that there is no such possibility for output shifts.

Proposition 4.1 *There exist two complete automata A and B such that A satisfies principle CI, B satisfies principle CII, and $\mathcal{S}_A^O = \mathcal{S}_B^O$.*

Proof. Consider the following automata. The output shift in both cases is the full shift $\{0,1\}^{\mathbb{Z}}$.



The automaton A has clearly property **A** since all its distinct states are distinguishable; for instance, $w = c$ distinguishes between q_2 and q_4 ($R_A(q_2, w) = 00 \neq 01 = R_A(q_4, w)$). But A does not have property **B**. If the experiment starts with a or b then it cannot distinguish between the states q_1 and q_4, and if the experiment starts with c then it cannot distinguish between q_1 and q_2. So there is no experiment which distinguishes q_1 from the other states.

In the same way we can prove that the automaton B has **B** but not **C**. □

The automaton shift completely describes the automaton, i.e., the shifts $\mathcal{S}_A$ and $\mathcal{S}_B$ are conjugate iff A and B are isomorphic. Accordingly, there is no real advantage in using $\mathcal{S}_A$ instead of A. It turns out that the label-output shift has the most interesting properties.

Theorem 4.2 *Let A and B be two automata. Then A is β-equivalent to B iff $\mathcal{S}_A^{\Sigma,O} = \mathcal{S}_B^{\Sigma,O}$.*

Proof. Assume first that A and B are β-equivalent and let $h_1 : S_A \to S_B$ and $h_2 : S_B \to S_A$ be the corresponding mappings. Consider all possible subwords of the sequences of $\mathcal{S}_A^{\Sigma,O}$ and $\mathcal{S}_B^{\Sigma,O}$. Then $\mathcal{B}(\mathcal{S}_A^{\Sigma,O}) = \mathcal{B}(\mathcal{S}_B^{\Sigma,O})$. Indeed, if $\omega = (a_1, x_1)\dots(a_m, x_m) \in \mathcal{B}(\mathcal{S}_A^{\Sigma,O})$, then there exist a state $p \in S_A$ and an output $x_{m+1} \in O$ such that $R_A(p, a_1 \dots a_m) = x_1 \dots x_m x_{m+1}$, hence $R_B(h_1(p), a_1 \dots a_m) = x_1 \dots x_m x_{m+1}$, so $\omega \in \mathcal{B}(\mathcal{S}_B^{\Sigma,O})$.

Conversely, let $M(A)$ and $M(B)$ be the minimal automata of A and B, respectively. We have

$$\mathcal{S}_{M(A)}^{\Sigma,O} = \mathcal{S}_A^{\Sigma,O} = \mathcal{S}_B^{\Sigma,O} = \mathcal{S}_{M(B)}^{\Sigma,O}.$$

In view of Corollary 6.7, $M(A)$ is isomorphic to $M(B)$, so in particular, they are β-equivalent, hence also A and B are β-equivalent. $\square$

By Calude and Lipponen [5], two minimal automata are β-equivalent iff they are isomorphic. The following result shows that for the label-output shifts, the minimal automaton presenting the shift is unique up to an isomorphism.

Corollary 4.3 *Let A and B be two minimal automata. Then A and B are isomorphic iff their label-output shifts $\mathcal{S}_A^{\Sigma,O}$ and $\mathcal{S}_B^{\Sigma,O}$ are equal.*

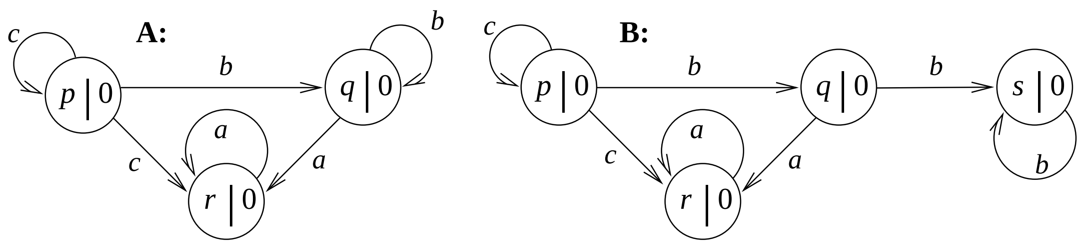
This result can be used to express complementarity principles in terms of properties of label-output shifts.

Corollary 4.4 *Let A and B be two automata. If A has CI and B has CII, then their label-output shifts are not equal.*

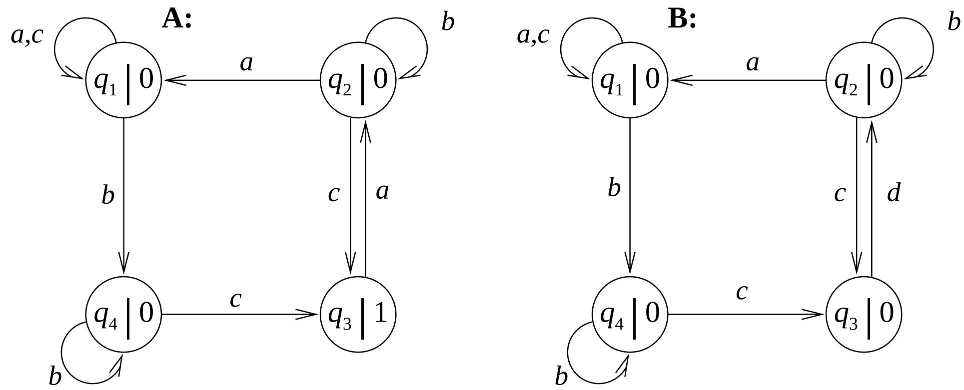
Corollary 4.5 *Let A and B be minimal automata such that their label-output shifts $\mathcal{S}_A^{\Sigma,O}$ and $\mathcal{S}_B^{\Sigma,O}$ are equal. If A has CI, then B has CI, and if A has CII, then B has CII.*

Notice that Theorem 4.2 is not valid for automata which are not strongly connected.

Example 4.6 The automata A and B below have the same label-output shifts but they are not β-equivalent. We also notice that A satisfies principle CII while B satisfies principle CI.



The following example shows that conjugacy cannot replace equality in Corollaries 4.4 and 4.5.



Example 4.7 Consider the automata A and B presented below. A has principle CII and B has principle CI; nevertheless, $X = \mathcal{S}_A^{\Sigma,O}$ and $Y = \mathcal{S}_B^{\Sigma,O}$ are conjugate via the extension of the morphism $\phi : \{a,b,c,d\} \times \{0,1\} \rightarrow \{a,b,c,d\} \times \{0,1\}$, $\phi((a,1)) = (d,0)$, $\phi((a,0)) = (a,0)$, $\phi((b,0)) = (b,0)$, $\phi((b,1)) = (b,1)$, $\phi((c,0)) = (c,0)$, $\phi((c,1)) = (c,1)$, $\phi((d,0) = (a,1)$, $\phi((d,1)) = (d,1)$. We will return to this example in Example 5.3.

5 Sofic Shifts

A **sofic shift** X is a subset of $\Sigma^{\mathbb{Z}}$ consisting of all bi-infinite walks on some graph G. Here G is a pair (S, Δ), where S is the set of **vertices** and the transition function $\Delta : S \times \Sigma \overset{\circ}{\rightarrow} S$ defines the labeled **edges** between the vertices; Σ is the underlying alphabet. We say that G is a **presentation** of X, and we write $X = X_G$.

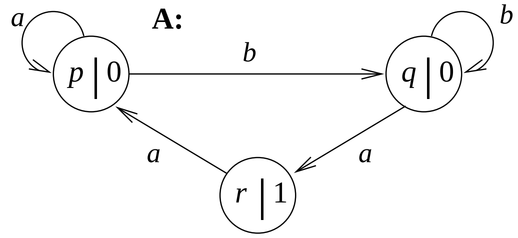
Notice that the graphs we consider are **right-resolving**, that is, for each vertex $p \in S$ the edges starting at p carry different labels. Such graphs have a "deterministic behaviour" in the sense that for every word $w \in \Sigma^*$ and every vertex p, there is at most one path labeled with w and starting from p. This property "reflects" the deterministic behaviour of the automata considered in this paper.

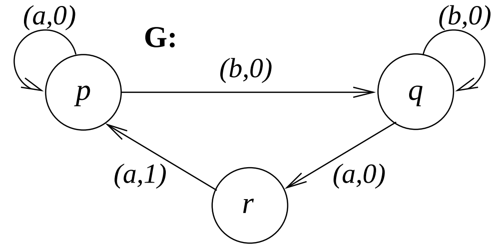
In what follows, we will consider mainly strongly connected graphs (a property which is defined in the same way as for automata). This property corresponds to irreducibility of the sofic shifts. Recall that a shift X having the property that for every words $u, v \in \mathcal{B}(X)$ there is a word $w \in \mathcal{B}(X)$ such that $uwv \in \mathcal{B}(X)$ is called **irreducible**. By Lind and Marcus [17], X_G is irreducible iff G is strongly connected.

We will now show that the label-output shifts are actually sofic shifts. The idea is to transform the underlying automaton A into a labeled graph G_A (over the alphabet $\Sigma \times O$) without affecting the represented shift.

Example 5.1 Consider the following automaton A and graph G. The label-output shift $\mathcal{S}_A^{\Sigma,O}$ is clearly the same as the sofic shift X_G.

Formally, let $A = (S_A, \Delta_A, F_A)$ be an automaton. The graph $G_A = (S_A, \Delta_{G_A})$ has the states of A as vertices and the transition table $\Delta_{G_A} : S_A \times \Sigma \times O \overset{\circ}{\rightarrow} S_A$ is defined by $\Delta_{G_A}(p, (a,x)) = \Delta_A(p,a)$ if $a \in W_A(p)$ and $x = F_A(p)$; otherwise, $\Delta_{G_A}(p,(a,x))$ is not defined. It follows immediately that $a \in W_A(p)$ iff $(a, F_A(p)) \in W_{G_A}(p)$, where $W_{G_A}(p)$

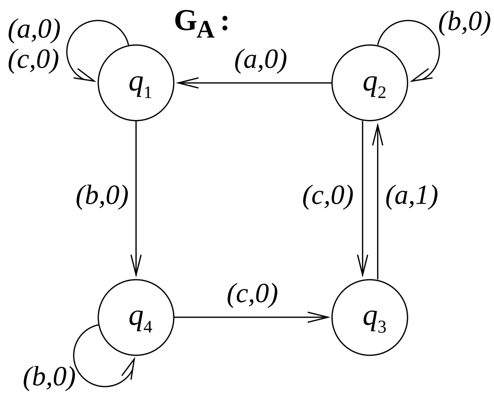


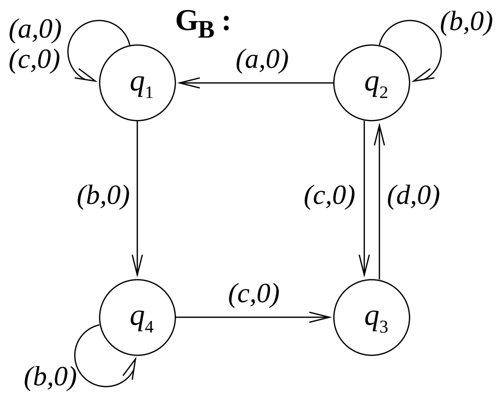


consists of words $\omega \in (\Sigma \times O)^*$ for which $\Delta_{G_A}(p, \omega) \neq \infty$. Consequently $\mathcal{S}_A^{\Sigma,O} = X_{G_A}$, so we have proved the following result:

Theorem 5.2 *Let A be an automaton. Then the label-output shift $\mathcal{S}_A^{\Sigma,O}$ is a sofic shift.*

Example 5.3 We will now return to Example 4.7. The graphs G_A and G_B below are represented by the automata A and B; it is easy to see that the sofic shifts X_{G_A} and X_{G_B} are conjugate via the extension of the mapping ϕ.

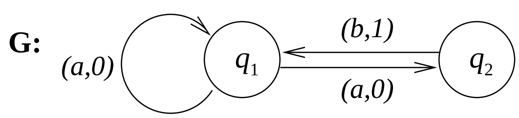




Notice that the graph G_A is strongly connected and right-resolving iff the automaton A is strongly connected and deterministic. The graph G_A has also the following property: *For any vertex p, all outgoing edges (a, x) must have the same second label x* (the output emitted by the state p). This property is essential in proving that not all sofic shifts are label-output shifts.

Theorem 5.4 *There exists a sofic shift which is not a label-output shift.*

Proof. For the graph G below there is no automaton A such that the shift space X_G is equal to the label-output shift $\mathcal{S}_A^{\Sigma,O}$.



Indeed, a typical word in $\mathcal{B}(X_G)$ is of the form

$$(a,0)^{i_1}(b,1)(a,0)^{i_2}(b,1)\ldots(a,0)^{i_k}(b,1)(a,0)^{i_{k+1}},$$

where $k, i_1, i_2, \ldots, i_k > 0$ and $i_{k+1} \geq 0$. Assume, for the sake of a contradiction, that X_G is conjugate to some $\mathcal{S}_A^{\Sigma,O}$. As k and the exponents i_j may have arbitrarily large values, it follows that there is a state $q \in S_A$ such that $\Delta_{G_A}(q, (a,0)) = q$, and

a) $\Delta_{G_A}(q, (a,0)) = q' \neq q$ for some state q', or

b) $\Delta_{G_A}(q, (b,1)) \neq \infty$.

The first case is impossible as A is deterministic (and hence G_A must be right-resolving); the second variant is also impossible as it contradicts the specific property of G_A mentioned above. □

The following results show two more specific properties of label-output shifts.

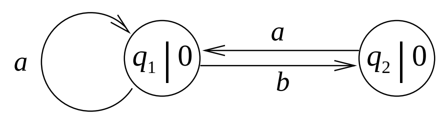
Corollary 5.5

1. *There is a shift of finite type which is not a label-output shift.*

2. *The class of label-output shifts is not invariant under conjugacy.*

Proof. Consider the shift X_G in the proof of Theorem 5.4 which cannot be a label-output shift for any automaton A. Thus the first claim follows from the fact that X_G is of finite type, as the set of forbidden subwords of X_G is finite: $\{(b,1)(b,1), (a,1), (b,0)\}$. The second statement is proved by considering the same shift X_G and the conjugacy induced by the morphism $\phi : \{a,b\} \times \{0,1\} \to \{a,b\} \times \{0,1\}$, $\phi((b,1)) = (b,0)$, $\phi((a,0)) = (a,0)$, $\phi((a,1)) = (a,1)$, $\phi((b,0)) = (b,1)$. Then X_G and $\mathcal{S}_A^{\Sigma,O}$ presented by the automaton A below are conjugate.

A:



□

Comment. By a well-known result (presented in Lind and Marcus [17]), every sofic shift has a right-resolving presentation, i.e., the graph G is right-resolving. However, the proof of Theorem 5.4 shows that X_G, in spite of being deterministic (as a graph), has an intrinsic nondeterministic behaviour which cannot be described by any deterministic automaton A.

6 More About Complementarity and Sofic Shifts

By Corollaries 4.4 and 4.5 we already know that the complementarity principles CI and CII are properties of the label-output shifts $\mathcal{S}_A^{\Sigma,O}$. In this section we will approach this fact from another point of view.

The **follower set** $\mathcal{F}_G(p)$ of a vertex p in the graph G is the collection of labels of paths starting at p. In the case of G_A, the follower set of p coincides with the set of words applicable to the state p, $\mathcal{F}_{G_A}(p) = W_{G_A}(p)$.

It turns out that the follower sets are closely related to indistinguishability. To prove this we first need to prove the following lemma.

Lemma 6.1 *For an automaton A, $(a_1,x_1)(a_2,x_2)\dots(a_k,x_k) \in W_{G_A}(p)$ iff $a_1\dots a_k \in W_A(p)$ and $R_A(p,a_1\dots a_{k-1}) = x_1\dots x_k$, where $p \in S_A$, $a_i \in \Sigma$, $x_i \in O$.*

Proof. We will use the induction. By definition, $(a,x) \in W_{G_A}(p)$ iff $a \in W_A(p)$ and $F_A(p) = x$. Assume now that the result holds for all words of length at most $k-1$. Let $\omega = (a_1,x_1)\dots(a_k,x_k)$ be a word from the set $W_{G_A}(p)$ for some p. By induction hypothesis, $a_1\dots a_{k-1} \in W_A(p)$ and $R_A(p,a_1\dots a_{k-2}) = x_1\dots x_{k-1}$. Let $q = \Delta_{G_A}(p,(a_1,x_1)\dots(a_{k-1},x_{k-1}))$. By definition, $\Delta_A(p,a_1\dots a_{k-1}) = q$ and since $(a_k,x_k) \in \Delta_{G_A}(q)$, we have $a_k \in W_A(q)$ and $F_A(q) = x_k$. But now

$$\begin{aligned} R_A(p,a_1\dots a_{k-1}) &= R_A(p,a_1\dots a_{k-2})F_A(\Delta_A(p,a_1\dots a_{k-1})) \\ &= x_1\dots x_{k-1}F_A(q) = x_1\dots x_k. \end{aligned}$$

This is clearly the case also for the converse implication. □

Theorem 6.2 *Two states $p,q \in S_A$ are indistinguishable iff $\mathcal{F}_{G_A}(p) = \mathcal{F}_{G_A}(q)$.*

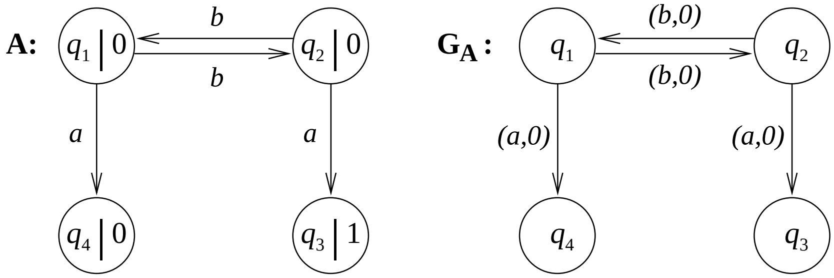
Proof. If the states p,q in A are indistinguishable then $W_A(p) = W_A(q)$ and $R_A(p,w) = R_A(q,w)$ for all $w \in W_A(p)$. We want to prove that $W_{G_A}(p) = W_{G_A}(q)$. Take any word $\omega = (a_1,x_1)\dots(a_k,x_k) \in W_{G_A}(p)$. By Lemma 6.1, $w = a_1\dots a_k \in W_A(p)$ and $R_A(p,a_1\dots a_{k-1}) = x_1\dots x_k$. In view of the hypothesis, $w \in W_A(q)$ and $R_A(q,a_1\dots a_{k-1}) = x_1\dots x_k$. Hence, applying Lemma 6.1 again, the word ω belongs to the set $W_{G_A}(q)$, too. Changing the places of p and q in the above proof, we obtain the equality $W_{G_A}(p) = W_{G_A}(q)$.

Assume now that $\mathcal{F}_{G_A}(p) = \mathcal{F}_{G_A}(q)$, in other words $W_{G_A}(p) = W_{G_A}(q)$. We want to prove that $W_A(p) = W_A(q)$ and $R_A(p,w) = R_A(q,w)$ for any word $w \in W_A(p)$. So assume that $w = a_1\dots a_k \in W_A(p)$, and let $R_A(p,w) = x_1\dots x_{k+1}$. Since A is strongly connected, there has to be a letter, say a_{k+1}, such that $\Delta_A(p,wa_{k+1})$ is defined and $R_A(p,wa_{k+1}) = x_1\dots x_{k+1}x_{k+2}$. By Lemma 6.1, $\omega = (a_1,x_1)\dots(a_k,x_k)(a_{k+1},x_{k+1}) \in W_{G_A}(p)$. By hypothesis, $\omega \in W_{G_A}(q)$ which again by Lemma 6.1 implies that $a_1\dots a_{k+1} \in W_A(q)$, consequently, $a_1\dots a_k \in W_A(q)$ and $R_A(q,a_1\dots a_k) = x_1\dots x_k x_{k+1}$. Thus the states p and q are indistinguishable in A. □

The following example shows that Theorem 6.2 does not hold if the automaton A is not strongly connected.

Example 6.3 In the automaton A below the states q_1 and q_2 are distinguishable by $w = a$; however, in G_A the follower sets $\mathcal{F}_{G_A}(p)$ and $\mathcal{F}_{G_A}(q)$ are equal. Notice that the shift $\mathcal{S}_A^{\Sigma,O}$ is still the same as the sofic shift X_{G_A}.

For an incomplete automaton $A = (S_A, \Delta_A, F_A)$ the length of the shortest words to check whether two states $p,q \in S_A$ are distinguishable is $|S_A|-1$ (see Calude and Lipponen [5]) whereas for complete automata the bound is $|S_A|-2$ (see Calude, Calude, Svozil and Yu [4]). We can prove that for incomplete automata the bound $|S_A|-1$ is needed only when all outputs of states of A are the same, and moreover, the word w which distinguishes between p and q belongs to $W_A(p)\Delta W_A(q)$. With this in mind we are able to improve the bound presented in Lind and Marcus [17] for output-label shifts.



Proposition 6.4 *Let G_A be a graph corresponding to an automaton A and $p, q \in S_A$. Then $\mathcal{F}_{G_A}(p) \neq \mathcal{F}_{G_A}(q)$ iff there is a word ω of length $|S_A| - 1$ which belongs to $\mathcal{F}_{G_A}(p) \triangle \mathcal{F}_{G_A}(q)$.*

Proof. Assume first that the follower sets of the states p, q are different. Then by Lemma 6.2 the states $p, q \in S_A$ are distinguishable. Let $w = a_1 \ldots a_k$, $a_i \in \Sigma$, be the shortest word which distinguishes these two states. We have two possibilities: If $w \in W_A(p) \triangle W_A(q)$ then $|w| \leq |S_A| - 1$. Hence the word $\omega = (a_1, x_1)(a_2, x_2) \ldots (a_k, x_k)$ which is of the same length belongs to either $\mathcal{F}_{G_A}(p)$ or $\mathcal{F}_{G_A}(q)$ but not to both. On the other hand, if $w \in W_A(p) \cap W_A(q)$ then $R_A(p, w) \neq R_A(q, w)$ and $|w| \leq |S_A| - 2$. If $R_A(p, w) = x_1 x_2 \ldots x_k x_{k+1}$ then there is a letter $a_{k+1} \in \Sigma$ (A is strongly connected) such that the word $\omega = (a_1, x_1)(a_2, x_2) \ldots (a_k, x_k)(a_{k+1}, x_{k+1})$ belongs to the set $\mathcal{F}_{G_A}(p) \triangle \mathcal{F}_{G_A}(q)$.

The other implication is obvious. $\square$

We say that a graph G is **follower-separated** if all distinct vertices have distinct follower sets. By Theorem 6.2, we easily obtain the following result:

Theorem 6.5 *The automaton A has property* **A** *iff G_A is follower-separated.*

A graph H is a **merged graph** from G if the vertex set of H consists of disjoint equivalence classes of vertices of G, where two vertices are **equivalent** if they have the same follower sets. Hence by definition, the merged graph is always follower-separated.

Corollary 6.6 *The automaton A is minimal iff G_A is merged.*

Corollary 6.7 *If A and B are minimal automata satisfying the condition $\mathcal{S}_A^{\Sigma,O} = \mathcal{S}_B^{\Sigma,O}$, then they are isomorphic.*

Proof. The proof will be essentially based on two results by Fischer [10, 9] which will be quoted in the form given by Lind and Marcus [17]. Consider the graphs G_A and G_B and notice that

$$X = X_{G_A} = \mathcal{S}_A^{\Sigma,O} = \mathcal{S}_B^{\Sigma,O} = X_{G_B}.$$

As A and B are minimal and strongly connected then G_A and G_B are merged and strongly connected, so X is irreducible. By Corollary 3.3.20 (Lind and Marcus [17, p. 83]) it follows that G_A and G_B are minimal presentations of X. Finally by Theorem 3.3.18 (Lind and Marcus [17, p. 82]), G_A and G_B are isomorphic graphs which assures that A and B are isomorphic automata. $\square$

Comment. From the above analysis it follows that one can define the analogues of CI and CII for label-output shifts. These are properties of label-output shifts, i.e., they do not depend on specific representations of label-output shifts. Further on, if $X = \mathcal{S}_A^{\Sigma,O}$ and has CI (resp. CII) then A has CI (resp. CII) if it is minimal.

References

[1] Béal, M.-P., and Perrin, D. Symbolic dynamics and finite automata. In *Handbook of Formal Languages, Vol. 2*, G. Rozenberg and A. Salomaa, Eds. Springer-Verlag, Heidelberg, 1997, pp. 463–506.

[2] Brauer, W. *Automatentheorie.* Teubner, Stuttgart, 1984.

[3] Calude, C., Calude, E., and Khoussainov, B. Deterministic automata: simulation, universality and minimality. *Annals of Pure and Applied Logic* (1997). in press.

[4] Calude, C., Calude, E., Svozil, K., and Yu, S. Physical versus computational complementarity I. *International Journal of Theoretical Physics* (1997). in press.

[5] Calude, E., and Lipponen, M. Deterministic incomplete automata: simulation, universality and complementarity. *Research Report CDMTCS 39* (1997).

[6] Chaitin, G. J. An improvement on a theorem by E. F. Moore. *IEEE Transactions on Electronic Computers EC-14* (1965), 466–467.

[7] Conway, J. H. *Regular Algebra and Finite Machines.* Chapman and Hall Ltd., London, 1971.

[8] Finkelstein, D., and Finkelstein, S. R. Computational complementarity. *International Journal of Theoretical Physics 22*, 8 (1983), 753–779.

[9] Fischer, R. Graphs and symbolic dynamics. *Mathematische Annalen 16* (1975), 229–243.

[10] Fischer, R. Sofic systems and graphs. *Monatshefte für Mathematik 80*, 3 (1975), 179–186.

[11] Gill, A. State-identification experiments in finite automata. *Information and Control 4* (1961), 132–154.

[12] Ginsburg, S. On the length of the smallest uniform experiment which distinguishes the terminal states of the machine. *Journal of the Association for Computing Machinery 5* (1958), 266–280.

[13] Ginsburg, S. *An Introduction to Mathematical Machine Theory.* Addison Wesley, Reading Massachusetts, 1962.

[14] Grib, A. A., and Zapatrin, R. R. Automata simulating quantum logics. *International Journal of Theoretical Physics 29*, 2 (1990), 113–123.

[15] KŮRKA, P. One-dimensional dynamics and factors of finite automata. *Acta Universitatis Carolinae. Mathematica et Physica 34* (1993), 83–95.

[16] KŮRKA, P. Simplicity criteria for dynamical systems. In *Analysis of Dynamical and Cognitive Systems (Stockholm, 1993)*, S. I. Andersson, Ed. Lecture Notes in Comput. Sci., 888, Springer-Verlag, Berlin, 1995, pp. 189–225.

[17] LIND, D., AND MARCUS, B. *Symbolic Dynamics and Coding.* Cambdridge University Press, Cambdridge, 1995.

[18] MOORE, E. F. Gedanken-experiments on sequential machines. In *Automata Studies*, C. E. Shannon and J. McCarthy, Eds. Princeton University Press, Princeton, 1956.

[19] PERRIN, D. Symbolic dynamics and finite automata. In *Proc. 20th International Symposium MFCS'95*, J. Wiedermann and P. Hájek, Eds. Springer-Verlag, Heidelberg, 1995, pp. 94–104.

[20] SCHALLER, M., AND SVOZIL, K. Partition logics of automata. *Il Nuovo Cimento 109B* (1994), 167–176.

[21] SCHALLER, M., AND SVOZIL, K. Automaton logic. *International Journal of Theoretical Physics 35*, 5 (May 1996), 911–940.

[22] SVOZIL, K. *Randomness & Undecidability in Physics.* World Scientific, Singapore, 1993.