INFORMATICA, 1999, Vol. 10, No. 4, 427–440

Decomposition Theorems for Probabilistic Automata over Infinite Objects

Robert D. REISZ
West University Timişoara, Romania
e-mail: reisz@info.uvt.ro

Received: October 1999

Abstract. A probabilistic Büchi automaton PBA is defined. The probabilistic language (L, p) as defined by the PBA is defined. A decomposition theorem similar to the classical Krohn-Rhodes theorem, but for PBA is proved.

Key words: probabilistic automata, Büchi automata, mathematical modelling, infinite processes.

The theory of classical (non stochastic) finite automata over infinite objects was fundamented as early as the 60s by such mathematicians as J.R. Büchi, R. McNaughton and M.O. Rabin (Büchi, 1960a, 1960b; McNaughton, 1966; Rabin, 1969). Their results gave birth to a theory that is now fundamental to those domains of theoretical computer science that deal with infinite processes or computations, and constitutes an adequate starting point for models in diverse domains of human knowledge.

The theory of stochastic automata, also named random automata relies, on the other hand, on another extension of Mealy's definition. The length of the input object is finite, but the evolution of the automaton is not simply non-deterministic, having a probabilistic character. The first definition of such an automaton is as old as 1963 and was put by J.W. Carlyle (1965). The denomination he used was that of stochastic sequential machine. During the same year, an article by M.O. Rabin gives a more complete form of the same object. The romanian mathematicians O. Onicescu and S. Guiaşu define in 1965 the random abstract finite automaton (Farcaş, 1987). Important results are presented in Paz (1970). A probabilistic Büchi automata, short PBA was defined by Reisz (1997) and studied in previous articles (Reisz, 1998; Reisz, 1999).

In the present article we will continue to investigate the properties of these automata, and in particular the possibility to separate their probabilistic and classical behaviour. A form of the classical Krohn-Rhosed theorem for PBA will be given.

1. Notations and Definitions

During this article, A is a finite set, named alphabet. The elements $x, y, \ldots \in A$, are named letters. We define as follows:

the empty word is ϵ and $A^0 = \{\epsilon\}$,

$$A^1 = A,$$
$$A^2 = AA = \{xy | x, y \in A\},$$
$$A^n = AA^{n-1}.$$

Let then $A^* = \bigcup_{n \geqslant 0} A^n$ be the set of finite words. A^ω is the set of ω-words (or ω-sequences) over A. An ω-word over A is by definition a sequence of the following form $\alpha = \alpha(0)\alpha(1)\alpha(2)\ldots$ where $\alpha(i) \in A$. Let $A^\infty = A^* \cup A^\omega$. Finite words will be denominated by the letters $u, v, w, \ldots$ and sets of finite words $U, V, W, \ldots$. Greek letters $\alpha, \beta, \ldots$ will be ω-words and $L, L_1, L_2, \ldots$ sets of ω-words (also named ω-languages). Reference to words in A^∞ will generally be made using $x, y, z, \ldots$. Segments of ω-words are denoted as:

$$\alpha(m, n) = \alpha(m)\ldots\alpha(n-1) \text{ where } m \leqslant n \text{ and}$$
$$\alpha(m, \omega) = \alpha(m)\alpha(m+1)\ldots$$

On A^∞ words we define an operation called concatenation: $\forall \alpha, \beta \in A^\infty$, where $\alpha = \alpha_0 \ldots \alpha_n$ and $\beta = \beta_0 \ldots \beta_n \ldots$, the concatenation $\alpha\beta = \alpha_0 \ldots \alpha_n \beta_0 \ldots \beta_n \ldots$. In this context ϵ proves to be neutral element of concatenation.

The usual logical conectors $\neg, \wedge, \vee, \forall, \exists, \rightarrow$ will be used. For the quantifiers "there exists an infinity of n" respectively "there exists a finite number of n" the notations "$\exists^\omega n$" and "$\exists^{<\omega} n$" will be used.

The operations defined on sets of finite words will also function for $W \subseteq A^\omega$. We will have as such the usual $\cup, \cap, \neg$ as well as the concatenation of sets ($L_1 L_2 = \{\alpha\beta | \alpha \in L_1, \ \beta \in L_2\}$. Let also:

$$\operatorname{pref} W = \{u \in A^* | \exists v \in A^\omega, \ uv \in W\},$$
$$W^\omega = \{\alpha \in A^\omega | \alpha = w_1 w_2 \ldots \text{ with } w_i \in W \text{ for } i \geqslant 0,$$
$$\vec{W} = \{\alpha \in A^\omega | \exists^\omega n, \ \alpha(0, n) \in W\}.$$

For $\vec{W}$ in the literature we can also find the notations $\lim W$ and W^δ. Finally, for the ω-sequence $\sigma = \sigma(0)\sigma(1)\ldots$ from S^ω the infinity set of σ is defined as being

$$\ln(\sigma) = \{s \in S | \exists^\omega n, \ \sigma(n) = s\}.$$

Büchi automata are non-deterministic finite automata that have a recognition condition fit to deal with ω-words. As such, an ω-word is accepted by a Büchi automaton if during the evolution of the automaton by reading the word from left to right the sequence of states of the automaton passes a certain state from a set of final states, an infinite number of times. The method is named Büchi acceptance.

Let Q be a finite set, $q_0 \in Q$, $\Delta \subseteq Q \times A \times Q$ and $F \subseteq Q$, then

DEFINITION (Thomas, 1990). A Büchi automaton over an alphabet A has the form $\mathcal{A} = (Q, q_0, \Delta, F)$ where Q will be denoted as the set of states, q_0 the inital state, Δ the transition relation and F the set of final states.

DEFINITION (Thomas, 1990). A run of the automaton $\mathcal{A}$ over an ω-word $\alpha = \alpha(1)\alpha(2)\ldots \in A^\omega$ is by definition a sequence $\sigma = \sigma(0)\sigma(1)\ldots \in Q^\omega$ so that $\sigma(0) = q_0$ and $(\sigma(i), \alpha(i), \sigma(i+1)) \in \Delta$ for $i \geqslant 0$.

DEFINITION (Thomas, 1990). A word $\alpha \in A^\omega$ is being recognised (or accepted) by $\mathcal{A}$ if $\ln(\sigma) \cap F \neq \emptyset$ that is, if a certain state from F is repeated an infinite number of times during the run.

DEFINITION (Thomas, 1990). The ω-language recognised by the automaton $\mathcal{A}$ is $L(\mathcal{A}) = \{\alpha \in A^\omega | \mathcal{A} \text{ acceptes } \alpha\}$.

DEFINITION (Thomas, 1990). Let $L \subseteq A^\omega$ then if $\exists \mathcal{A}$ such that $L = L(\mathcal{A})$ then L is *Büchi recognisable* (or simply a Büchi language).

The random automata is a finite automata that reads finite words from an input device but whose evolution is determined by a probability function that gives to all actions possible to be made at a certain moment a random character instead of the usually non-deterministic character.

A simple form of the finite random automaton concentrated on its acceptance function is the p-model. In this case the output alphabet is formed by only two values, coded 0 and 1 (Thathachar, 1990). A definition equivalent to the p-model will be used in which the output alphabet is skipped and the languages recognised by the random automata will be studied. As such, the output produced by the automaton at reading a word will be the recognition or non-recognition of the respective word, that is the membership or non-membership of the word in the language recognised by the automaton. In essence we will deal with a binary response.

Let Q be a finite set, $q_0 \in Q$, P a probability function defined $P : Q \times A \times Q \to [0, 1]$ and $F \subseteq Q$, then

DEFINITION (Thathachar, 1990). A simple random automaton over an alphabet A has the form: $\mathcal{A}_{SR} = (Q, q_0, P, F)$ where Q is the set of states, q_0 the initial state (or start state), P the transition probability function and F the set of final states. The function P has the property:

$$\forall x \in A, \quad \sum_{q' \in Q} P(q, x, q') = 1.$$

The definition above was used in a series of papers and is relatively close to the definition of the Büchi automaton previously given. It is evident that based on the definition above we can compute the probability that the state reached at the end of the evolution

of the random automaton over a given word is in the set of final states F. The language recognised by the random automaton will as such also have a random character, the membership of any word to this language being characterised by a probability value. Such a language is generally named a probabilistic language (by Suppes, Ellis, etc.) as in (Suppes, 1990), and is formed by a pair (L, p) where $L \subseteq A^*$ and $p : \ L \to [0, 1]$ is a probability with which an element of L is a member of the language.

DEFINITION (Thathachar, 1990). The probability $p(q, q')$ with which the automaton evolves between $q \in Q$ and $q' \in Q$ is:

$$p(q, q') = \max_{u_0 \ldots u_n \in A^*} \max_{q_1, \ldots q_n \in Q} P(q, u_0, q_1) \ldots P(q_n, u_n, q').$$

Given $u \in A^*$, the definition above delimites the functions $p_u : \ Q \times Q \to [0, 1]$ having the form

$$p_u(q, q') = \max_{q_1, \ldots q_n \in Q} P(q, u_0, q_1) \ldots P(q_n, u_n, q'), \ \text{ where } \ u = u_0 \ldots u_n.$$

Properties

The function $p : \ Q \times Q \to R$ has the properties

1. $0 \leqslant p(q, q') \leqslant 1, \quad \forall q \in Q.$
2. $q = q' \leftrightarrow p(q, q') = 1.$
3. $\exists \mathcal{A}_A, \ \exists q \neq q', \ \ p(q, q') = 1.$
4. $\exists \mathcal{A}_A, \ \exists q, q', \ \ p(q, q') \neq p(q', q).$

DEFINITION. The language recognised by a random automaton is

$$(A^*, p) \ \text{ where } \ \forall u \in A^*, \ \ p(u) = \max_{q \in F} p_u(q_0, q).$$

Another definition is (L, p) where $L \subseteq A^*$ and L contains all words $u \in A^*$ for which $p(u) > 0$, p having the same definition as above. Actually one has to consider in the (L, p) situation, $p(u) = 0$ for all $u \notin L$ even if $p(u) = 0$ could also be allowed for certain $u \in L$. The (L, p) form will be used in the present article.

Over the class of such languages of pairs one can easily extend the set operations $\cup, \cap, \neg$. Next to these the concatenation of two pairs is defined as follows:

$$(u, p_1)(v, p_2) = (uv, p_1 p_2),$$

where uv is the usual operation of concatenation of words, while $p_1 p_2$ is the product of real numbers. The operation is, similar to the classic one, associative, having a neutral element, without simetry and noncomutative. The operation above can be extended as usual over sets. Based upon this operation a Kleene-type closure can also be defined.

2. The Probabilistic Büchi Automaton

A structure combining characteristics of both the above defined automata was defined in (Reisz, 1997) as follows:

Let Q be a finite set, $q_0 \in Q$, P a probability function defined $P:\ Q\times A\times Q \to [0,1]$ and $F \subseteq Q$, then

DEFINITION. A probabilistic Büchi automata over an alphabet A has the form $PBA = (Q, q_0, P, F)$ where Q denotes the set of states, q_0 the initial state (or start state), P the transition probability function and F the set of final states. The function P has the property:

$$\forall q \in Q,\ \ \forall x \in A,\ \ \sum_{q' \in Q} P(q, x, q') = 1.$$

The recognition condition will be a Büchi type condition. As such an ω-word will be a member of the language recognised by PBA with a probability depending on the probability with which states from F are visited infinitely many times during an evolution. While in the case of finite words the probability that the evolution reaches a final state is the acceptability criterion, in this case the probability that the evolution visites a final state infinitely many times is the corresponding criterion.

To define the language, recognised by PBA's , some more considerations are necesary.

DEFINITION. The probability $p(q, q')$ with which a PBA evolves from $q \in Q$ to $q' \in Q$ is defined as:

$$p(q, q') = \max_{u=u_0\dots u_n \in A^*} \sum_{q_1,\dots q_n \in Q} P(q, u_0, q_1)\dots P(q_n, u_n, q').$$

Observation. The formula is different from the one used for stochastic automata over finite words. The change from max to sum had to be made in order to expand the set of BP languages.

DEFINITION. For any $u = u_0u_1\dots u_n\dots$, a string of states $q_0, q_1, \dots, q_n, \dots$ where $\forall i \geqslant 0,\ P(q_i, u_i, q_{i+1}) > 0$ is named a possible evolution for u. The set of possible evolutions for a certain u will be denoted by $Ev(u)$. The evolutions themselves will be denoted by Greek letters.

DEFINITION. Given $u \in A^\omega$, the probability of an evolution α of the PBA over u is:

$$\forall \alpha \in Ev(u),\ \ \alpha = q_0, q_1, \dots,$$
$$P(\alpha) = P(q_0, u_0, q_1)P(q_1, u_1, q_2)\dots .$$

Properties

Forall $u \in A^\omega$ and $\alpha \in Ev(u)$ the following properties hold:

1. $0 \leqslant P(\alpha) \leqslant 1$.
2. Given $u = u_0 \dots u_n \dots$ and $\alpha = q_0 \dots q_n \dots \in Ev(u)$ then if $\forall i \in N, P(q_i, u_i, q_{i+1}) \leqslant P(q_{i-1}, u_{i-1}, q_i)$ and $P(q_0, u_0, q_1) < 1$ or if $\forall i \in N, P(q_i, u_i, q_{i+1}) < P(q_{i-1}, u_{i-1}, q_i)$ then $P(\alpha) \to 0$.
3. $\exists PBA,\ \exists u \in A^\omega,\ \exists \alpha \in Ev(u)$ such that $0 < P(\alpha) < 1$.

Proof.

1. $\forall u \in A,\ q, q' \in Q, P(q, u, q') \in [0,1] \Rightarrow P(\alpha) \geqslant \lim\limits_{n\to\infty} 0^n = 0$ and $P(\alpha) \leqslant \lim\limits_{n\to\infty} 1^n = 1$.
2. If for $u = u_0 \dots u_n \dots$ and $\alpha = q_0 \dots q_n \dots \in Ev(u)$ $\forall i \in N, P(q_i, u_i, q_{i+1}) \leqslant P(q_{i-1}, u_{i-1}, q_i)$ and $P(q_0, u_0, q_1) < 1$ then $P(\alpha) = P(q_0, u_0, q_1) \dots P(q_i, u_i, q_{i+1}) \dots \leqslant \lim\limits_{n\to\infty} P(q_0, u_0, q_1)^n = 0$. If for $u = u_0 \dots u_n \dots$ and $\alpha = q_0 \dots q_n \dots \in Ev(u)$ $\forall i \in N, P(q_i, u_i, q_{i+1}) < P(q_{i-1}, u_{i-1}, q_i)$ and $P(q_0, u_0, q_1) = 1$ then $P(\alpha) = P(q_0, u_0, q_1) \dots P(q_i, u_i, q_{i+1}) \dots \leqslant \lim\limits_{n\to\infty} P(q_1, u_1, q_2)^n = 0$.
3. Such a case results from the product: $P(\alpha) = (1 - \frac{1}{2^2})(1 - \frac{1}{3^2}) \dots (1 - \frac{1}{n^2}) \dots$ that has the value $\frac{1}{2}$.

DEFINITION. The infinity set associated to an ω-word $u \in A^\omega$ for a PBA automaton is:

$$In_{PBA}(u) = \Big\{(q,p), q \in Q, p \in [0,1] | \exists \alpha \in Ev(u) \exists^\omega q' \in \alpha, \\ q = q';\ p = \max_\alpha P(\alpha)\Big\}.$$

In other words, a state is in the infinity set of a certain word if there exists a possible evolution on the respective word in which the state is visited an infinity of times. The probability related to the state will be the sum of probabilities of evolutions on which the state is visited an infinity of times. This will avoid that a state q appears in the infinity set more then once (i.e., for different values of the probability).

The union of the first projection of the pairs in $In_{PBA}(u)$ will be denoted by $In^Q_{PBA}(u)$, while the second component with $In^p_{PBA}(u)$.

DEFINITION. Let us use the notation $FIn_{PBA}(u) \subseteq In(PBA)(u)$ such that $FIn^Q_{PBA}(u) = In^Q_{PBA}(u) \cap F$. The language recognised by a probabilistic Büchi automaton is then

$$(A^\omega, p) \text{ where } \forall u \in A^\omega, p(u) = \max_{(q,p) \in FIn_{PBA}(u)} p.$$

The following form will also be used:

$$L(ABP) = \{(u, p(u)) \in (A^\omega, p) | FIn_{PBA}(u) \neq \emptyset\}.$$

The class of languages recognised by probabilistic Büchi automata will be denominated as the class of probabilistic Büchi languages or BP.

In the definition above p represents the second component of the pair $In_{PBA}(u)$ for which the maximum is achieved. In words, the language recognised by the PBA will be formed by all the words for which there exist evolutions in which a final state is visited an infinity of times. The probability of membership in this language of a certain word will actually be the maximum of probabilities of the evolutions on which the final state is visited an infinity of times.

3. Decomposition Theorems

In the present section we will refer to the transition system concept. The object of this section is the presentation of decomposition theorems for classical as well as probabilistic transition systems and the prove of a decomposition result for probabilistic Büchi automata. If the decomposition theorems for classical transitions systems presented here have a relatively long history, being discussed in depth in (Arbib, 1968a, 1968b) we will also present a recent result for the decomposition of a probabilistic transition system (Maler, 1995).

The transition system concept was defined in reference works (Arbib, 1968a, 1968b; Ginsburg, 1962; Paz, 1970) in more or less different ways and having different names. The more often used denominations are state-output automaton, abstract automaton or abstract machine. The following definition only partly corresponds to the initial one given by Mealy.

DEFINITION (Transition systems). A transition system (TS) is a structure $\mathcal{A} = (X, Q, Y, \delta, \beta)$ where X is the input alphabet, Q is the set of states, Y is the output alphabet. $\delta : \ Q \times X \rightarrow Q$ is the state transition function and $\beta : \ Q \rightarrow Y$ the output function.

The intuitive interpretation is the following: The system is at any moment t in time in a state $q \in Q$ and receives an input character $x \in X$ that determines the evolution of the system in a state $\delta(q, x)$ and the output of a character $\beta(q)$.

Let in the following the set X^* be the set of all finite sequences of symbols from X including Λ the empty string formed with 0 characters as well. X^* is a semigrup with unity raported to the concatenation operation, the concatenation being associative and having as neutral element Λ. We can extend than $\delta : \ Q \times X^* \rightarrow Q$ applying repeatedly:

$$\delta(q, \lambda) = q,$$
$$\delta(q, x'x") = \delta(\delta(q, x'), x").$$

To every state q of the TS we can associate the way it prroduces output depending on input. Let this be the function $M_q : \ X^* \rightarrow Y$ where $M_q(x) = \lambda(q, x)$ and $\lambda(q, x) =$

$\beta(\delta(q,x))$. Evidently the behavior of the TS is identic for two states having equal input-output functions, that is $M_{q_1}(x) = M_{q_2}(x)$ for any input string x. If our interest lies in the external behavior of the transition system we can replace the M_q functions with the reduced set of distinct M_q functions constructing as such a new TS having only those states that have distinct M_q functions. Let than the ST in the state q, having the input-output function f and q' an *accesible* state meaning that there exists $x \in X^*$ such that $\delta(q,x) = q'$. Than q' has the function:

$$M'_q(x') = M_\delta(q,x)(x') = \lambda(\delta(q,x),x') = \lambda(q,xx') = f(xx') = fL_x(x'),$$

where $L_x : X^* \to X^*$ is "left multiplication with x" function. L_x is not an homomorfism. In the reduced form of the TS we will replace any accesible state q with the input-output function fL_x and the reduced form will have a finite number of states if there exists a finit number of distinct functions fL_x (such that an infinite number of strings $x \in X^*$ should correspond to the same fl_x). Than our interest will be reduced to a TS of the form:

$$\mathcal{A}(f) = (X, Q, Y, \delta_f, \beta_f),$$

where is the function that maps X^* in Y and:

$$\begin{aligned} &Q_f = \{g : X^* \to Y | g = fL_x \quad \text{for} \quad x \in X^*\},\\ &\delta_f(g,x) = gL_x,\\ &\beta_f(g) = g(\Lambda). \end{aligned}$$

We will specially refer to the case in which f is such that Q_f is a finite set. We will refer in the following to the TS by its f function.

DEFINITION. For any TS $\mathcal{A}(f)$ the associated semigroup f^S is defined as being formed by all the transformations of the set of states Q_f inducted by input strings for $\mathcal{A}(f)$, that is:

$$f^S = \{s : Q_f \to Q_f | \exists x \in X^* \text{ such that } s(q) = \delta(q,x) \text{ for any } q \in Q\}.$$

DEFINITION (State homomorfisms). Being given two TS $\mathcal{A}_1 = (X, Q_1, Y, \delta_1, \beta_1)$ and $\mathcal{A}_2 = (X, Q_2, Y, \delta_2, \beta_2)$ a homomorfisms of states from $\mathcal{A}_1$ to $\mathcal{A}_2$ is a surjective function $\phi : Q_1 \to Q_2$ such that for any $q \in Q_1$ and $x \in X$ there is:

$$\phi(\delta_1(q,x)) = \delta_2(\phi(q),x).$$

We will denote $\mathcal{A}_1 \leqslant_\phi \mathcal{A}_2$. Two TS are isomorfous if ϕ is bijective.

DEFINITION (Cascade product). Being given two TS $\mathcal{A}_1 = (X, Q_1, Z, \delta_1, \beta_1)$ and $\mathcal{A}_2 = (Z, Q_2, Y, \delta_2, \beta_2)$ we define their cascade product as a transition system $\mathcal{A}_1 \circ \mathcal{A}_2 =$

(X, Q, Y, δ, β) such that, $Q = Q_1 \times Q_2$ and for all $(q_1, q_2), (q_1', q_2') \in Q$, $x \in x$ and $y \in Y$ there is:

$$\delta((q_1, q_2), x) = (q_1', q_2') \text{ and}$$
$$\beta((q_1, q_2)) = y,$$
$$\text{if and only if there exists } z \in Z \text{ such that :}$$
$$\delta_1(q_1, x) = q_1' \text{ and}$$
$$\beta_1(q_1) = z,$$
$$\delta_2(q_2, z) = q_2' \text{ and}$$
$$\beta_2(q_2) = y.$$

The definition can be evidently extended to any finite number of TS where the output alphabet of a given $\mathcal{A}_i$ corresponds to the input alphabet of $\mathcal{A}_{i+1}$.

To be able to present the decomnposition theorems we will have to introduce first some particular cases of transition systems.

DEFINITION (Reset automaton). A transition system that transfers any state in the same new state is named reset automaton. The reset state r is than a right zero the semigroup associated to the automaton, that is, if S is the associated semigroup and "." the operation, than $sr = r$ for any $s \in S$.

DEFINITION (Permutation automaton). A transition system in which any state is transfered in a single state is named permutation automaton. The semigroup associated to a permutation automaton is a group.

A transition system that has a reset or permutation type mapping is named permutation-reset automaton. Such an automaton will have an associated semigroup resulted from the union of group G and a set of resets R.

Theorem 1 (Krohn Rhodes decomposition theorem). *Any determinist transtion system $\mathcal{A}$ is backwards homomorfous to a cascade product of permutation and reset automata.*

We will not give the proof of this classical result, more forms of it can be found in (Arbib, 1968b).

Additional information to this theorem can be found in (Arbib, 1968b; Eilenberg, 1976; Ginzburg, 1968; Maler, Pnueli, 1990).

Let us follow with the presentation of the probabilistic case.

As in the case with the TS the definition of probabilistic transtion system (PTS) is not new and can be found in different papers under different names (e.g., Arbib, 1968a; Paz, 1970; Starke, 1972).

DEFINITION (Probabilistic transition systems). A probabilistic transition system (PTS) is a structure $\mathcal{A} = (X, Q, Y, p)$ where X is the input alphabet, Q the set of states, Y the

output alphabet and $p: Q \times X \times Q \times Y \to [0,1]$ the input-output transition probability function, satisfying for any $q \in Q, x \in X$, the condition:

$$\sum_{(q',y)\in Q\times Y} p(q,x,q',y) = 1.$$

The intuitive sense of the definition is the following: given $\mathcal{A}$ in a state q, the system reads the input symbol x, passes in a new state q' and writes the output symbol y with a probability $p(q,x,q',y)$. Diverse similar known models can be considered as degenerate variants of PTS, where either X or Q are single element sets, or $|Y| \leqslant |Q|$ or other additional restrictions are imposed to the form of p. Let us mention Markov chains, deterministic transition systems and Bernoulli processes as such examples.

As in the determinist case, one of the important concepts related to probabilistic transition systems are homomorfisms. A system $\mathcal{A}_1$ is homomorfous with $\mathcal{A}_2$ if, in some conditions, $\mathcal{A}_1$ aproximates $\mathcal{A}_1$.

DEFINITION (Homomorfisms of PTS). Given two PTS $\mathcal{A}_1 = (X, Q_1, Y, p_1)$ and $\mathcal{A}_2 = (X, Q_2, Y, p_2)$ a homomorfism (of states) from $\mathcal{A}_1$ to $\mathcal{A}_2$ is a surjective function $\phi : Q_1 \to Q_2$ such that $\forall (q_2, x, q_2', y) \in Q_2 \times X \times Q_2 \times Y$ and $\forall q_1 \in \phi^{-1}(q_2)$ there is

$$p(q_2,x,q_2',y) = \sum_{q_1'\in\phi^{-1}(q_2')} p_1(q_1,x,q_1',y).$$

We will note as in the determinist case $\mathcal{A}_1 \leqslant_\phi \mathcal{A}_2$. Two systems are isomorfous if ϕ is bijective.

This definition can be intuitively explicited by the fapt that $\mathcal{A}_2$ can be constructed by the partitioning of Q_2 in blocks such that the transition probabilities between blocks are consistent with the transition probabilities between elements. It can than be observed that in the case of $0-1$ probabilities this corresponds to the familiar concept of automata homomorfism, that is $\phi(\delta(q,x)) = \delta'(\phi(q),x)$. It can be proven that that the PTS homorfism is transitive, that is, $\mathcal{A}_2 \leqslant_\phi \mathcal{A}_1$ and $\mathcal{A}_3 \leqslant_\psi \mathcal{A}_2$ lead to $\mathcal{A}_3 \leqslant_\theta \mathcal{A}_1$ where $\theta = \psi\phi$.

Two PTS can be conected such that the input of the second PTS is the output of the first PTS.

DEFINITION (Cascade product). Given two PTS $\mathcal{A}_1 = (X, Q_1, Z, p_1)$ and $\mathcal{A}_2 = (Z, Q_2, Y, p_2)$, their cascade product is $\mathcal{A}_1 \circ \mathcal{A}_2 = (X, Q, Y, p)$ where $Q = Q_1 \times Q_2$ and for any $(q_1,q_2),(q_1',q_2') \in Q, x \in X$ and $y \in Y$:

$$p((q_1,q_2),x,(q_1',q_2',y) = \sum_{z\in Z} p_1(q_1,x,q_1',z)\cdot p_2(q_2,z,q_2',y).$$

This definition can be extended to the family $\mathcal{A}_1, \ldots \mathcal{A}_k$ of PTS, such that the input aphabet of $\mathcal{A}_{i+1}$ should be the output alphabet of $\mathcal{A}_i$. It can in fact also be reduced to the familiat notion of cascade product between deterministic systems if $Z = X \times Q_1$ and

$Y = Q_2$. In that case we can use the known result that specifies that any finite automaton can be decomposed in simpler parts.

DEFINITION (Probability of a transformation). Given a set $Q = \{q_1, \ldots, q_n\}$, we will note by $M = Q^Q$ the set of all n^n transformations over Q. M with the composition operation forms a semigroup. For any Markov chain[1] $\mathcal{A} = (\{x^*\}, Q, Q, p)$ we will consider $\pi : M \to [0, 1]$ where:

$$\pi(m) = \prod_{i=1}^{n} p(q_i, m(q_i)),$$

PROPOSITION 1. $\sum_{m \in M} \pi(m) = 1.$

PROPOSITION 2. Any Markov chain $\mathcal{A} = (\{x^*\}, Q, Q, p)$ having $|Q| = n$ is isomorfous with a cascade product between a Bernoulli generator with at most n^n outputs and a determinist finite automaton with n states.

To use well this decomposition and to connect it with the Krohn-Rhodes decomposition theorem we will need a weak variant of the following proposition (Maler, 1995):

PROPOSITION 3. Given the PTS $\mathcal{B} = (X, Q, Z, p)$, $\mathcal{A}_1 = (Z, R, Y, p_1)$ and $\mathcal{A}_2 = (Z, S, Y, p_2)$. If $\mathcal{A}_2 \leqslant \mathcal{A}_1$ than $\mathcal{B} \circ \mathcal{A}_2 \leqslant \mathcal{B} \circ \mathcal{A}_1$.

COROLLARY 1. Any Markov chain is the backwards image through an homomorfism of a cascade product between a Bernoulli process and a string of deterministic reset and permutation automata.

COROLLARY 2. Any non-deterministic automata is the backwards image through an homomorfism of a cascade product between a non-deterministic transition system with a single state and a deterministic automata.

Let us return now to the probabilistic Büchi automata.

Theorem 2. *For any* PBA *there exists a* PTS *with binary output that is equivalent to it.*

Proof. Let $ABP = ((Q, q_0, P, F)$ be a probabilistic Büchi automaton where Q is the set of states, q_0 the start (or initial) state, P the probability function defined as $P : Q \times A \times Q \to [0, 1]$ and F the set of final states. The function P will have the property:

$$\forall q \in Q, \forall x \in A, \sum_{q' \in Q} P(q, x, q') = 1.$$

[1] We omit the input (one single element) and the output of the system (equal with the state) from the definition of p.

We define than a PTS $\mathcal{A} = (A, Q, 0, 1, p)$ where A is the input alphabet, Q the space of states, $\{0, 1\}$ the output alphabet (such a TS is named a binary output TS). $p : Q \times A \times Q \times \{0, 1\} \to [0, 1]$ is the input/output transition probability function, defined as follows:

$\forall q, q' \in Q, x \in A$ if $q' \in F$ than $p(q, x, q', 1) = P(q, x, q')$ and $p(q, x, q', 0) = 0$ otherwise $p(q, x, q', 0) = P(q, x, q')$ and $p(q, x, q', 1) = 0$

The verification of the fact that the function p satisfies for all $q \in Q, x \in A$, the condition:

$$\sum_{(q',y)\in Q\times\{0,1\}} p(q, x, q', y) = 1$$

is immediate and results from the way the PTS is defined and from the similar condition that exists at PBAs.

As usually two automata are equivalent if they recognise the same language.

To prove that the two systems are equivalent we will have to define the acceptance method of the PTS. We will as such say that $a \in A^*$ is accepted by the PTS with the probability p if after the input of a the output will have an infinity of appearances of 1. The acceptance probability is $p = \max_{m\in M} \pi(m)$.

Proving the equivalence is than narrowed to the equality $L(ABP) = L(\mathcal{A})$.

Let $(a, p) \in L(ABP)$ where $a \in A^*$ and $p \in [0, 1]$. Than according to the definition of the language recognised by the PBA we will have:

$$p(a) = \max_{q\in In^Q_{ABP}(a)\cap F} p.$$

In the upper definition p represents the second component of the pair from $In_{ABP}(u)$ for which the maximum is achieved.

From the form of $p(a)$ it can be seen that this non-nil only if there exists a final state in the infinity set $In^Q_{ABP}(a)$. By construction if such a state exists on the output of $\mathcal{A}$ there will be a 1 on the output for every occurence of the respective final state, that is an infinity of 1s. More, the formula below is than true:

$$p(a) = \max_{q\in In^Q_{ABP}(a)\cap F} p = \max_{m\in M} \pi(m) = p.$$

The proof of the reverse implication is based on the finiteness of the set F of the PBA. Let $(a, p) \in L(\mathcal{A})$ than for the input of a on the output we will get an infinity of appearances of 1 with the probability p. Than, according to the construction there exists an evolution of the PBA with a probability p on which final states are reached an infinity of times. We know that $F \subseteq Q$ and Q is finite, from where it results that F is finite, so there $\exists q_f \in F$ such that $q_f \in In^Q_{ABP}(a) \cap F$. This leads to the fact that a is recognised by the PBA. The recognition probability is equal with the acceptance probability of the $\mathcal{A}$ being the probability of the evolution on which the infinity of appearances of 1 occurs.

Observation. The converse of the theorem is not true.

Theorem 3. *Any* PBA *is the backwards image of a cascade product between a Bernoulli generator and a deterministic Büchi automaton through an homomorfism.*

Proof. Let us consider the PTS equivalent with a given PBA (according to Theorem 2). Than according to the decomposition theorem (the remark to Proposition 2) this is the backwards image through an homomorfism of a cascade product between a Bernoulli generator and a deterministic automaton. Given the necesity of the evolution of the product over infinite objects, the deterministic automaton will have to be equipped with the Büchi acceptance method. This leads to the theorem.

References

Arbib, M.A. (1968). *Theories of Abstract Authomata*. Prentice Hall, Englewood Cliffs, NJ.

Arbib, M.A. (1968). *Algebraic Theory of Machines, Languages and Semigroups*. Academic Press, New York.

Büchi, J.R. (1960). Weak second order arithmetic and finite automata. *Z. Math. Logik Grundlag. Math.*, **6**.

Büchi, J.R. (1960). On a decision method in restricted second order arithmetic. In E. Nagel e.a. *Proc. Internat. Congr. on Logic, Methodology, and Philosophy of Science*. Stanford Univ, Press, Stanford.

Carlyle, J.W. (1965). State-calculable stochastic sequential machines, equivalences and events. *IEEE Symposium on Foundations of Computer Science*, **7**.

Eilenberg, S. (1976). *Authomata, Languages and Machines*, Vol. B. Academic Press, New York.

Farcaş, D.D. (1987). *Automate Aleatoare cu utilităti*, Editura Ştiinţifică şi Enciclopedică, Bucureşti.

Ginsburg, S. (1962). *An Introduction to Mathematical Machine Theory*. Addis on-Wesley Publishing, Reading.

Ginzburg, A. (1968). *Algebraic Theory of Authomata*. Academic Press, New York.

McNaughton, R. (1966). Testing and generating infinite sequences by a finite automaton. *Inform. and Control*, **9**.

Maler, O., A. Pnueli (1990). On a cascaded decomposition of authomata, its complexity and its application to logic. *Proc. 31st Ann. Symp. on Foundation of Computer Sciences*, IEEE Press.

Maler, O. (1995). A decomposition theorem for probabilistic transition systems. *Theoretical Computer Science*, **145**.

Paz, A. (1970). *Introduction to Probabilistic Authomata*. Academic Press, New York.

Rabin, M.O. (1969). Decidability of second order theories and automata on infinite trees. *Trans. Amer. Math. Soc.*, **141**.

Reisz, R.D. (1997). A decomposition theorem for probabilistic Büchi automata. *Zilele Academice Timişene Conference* Timişoara.

Reisz, R.D. (1998). Probabilistic Automata over infinite objects – a characterisation theorem. *50 de ani de la Înfiinţarea Facultăţii de Matematică*, Conference Timişoara.

Reisz, R.D. (1999). Probabilistic Automata over infinite objects. *Analele Universităţii din Timişoara*, Timişoara.

Starke, P.H. (1972). *Abstract Authomata*. North-Holland, Amsterdam.

Suppes, P. (1990). *Metafizica Probabilistă*. Humanitas, Bucureşti.

Thathachar, M.A.L. (1990). *Stochastic automata and learning systems*. Sadhana, Academy Proceedings in Engineering Sciences, India.

Thomas, W. (1990). Automata on infinite objects. In J.van Leeuwen (Ed.), *Handbook of Theoretical Computer Science*. North Holland, Amsterdam.

R.D. Reisz is a lecturer at the University of the West of Timisoara in Romania, Faculty of Mathematics Department of Computer Science, and a Ph.D. candidate in the theory of probabilities. His work is mainly concerned with social statistics and mathematical models for the social sciences.

Tikimybinių automatų dekompozicijos teoremos neribotiems objektams

Robert D. REISZ

Apibrežtas tikimybinis Buchi automatas PBA, pasinaudojant specialia tikimybine kalba. Įrodyta PBA liečianti teorema, panaši į klasikinę Krohn-Rhodes teoremą.