ANDRÉ ARNOLD

A selection property of the boolean μ-calculus and some of its applications

Informatique théorique et applications, tome 31, nº 4 (1997), p. 371-384.

<http://www.numdam.org/item?id=ITA_1997__31_4_371_0>

Informatique théorique et Applications/Theoretical Informatics and Applications
(vol. 31, n° 4, 1997, pp. 371-384)

A SELECTION PROPERTY OF THE BOOLEAN μ-CALCULUS AND SOME OF ITS APPLICATIONS (*)

by André ARNOLD ([1])

Abstract. – *We prove that every closed Boolean μ-term τ has the same value as a μ-term τ' obtained by replacing any sum by one of its summand.*

1. INTRODUCTION

The μ-calculus, that is concerned with monotonic mappings between complete lattices, plays a central role in the study of the relations between logics and automata (see, for instance, [4] and [2]).

Depending on the complete lattices under consideration and the basic monotonic mappings that are used, one can define a lot of different μ-calculi. The most fundamental one, the Boolean μ-calculus, is based on the lattices $\mathbb{B}^I$, equipped with pointwise Boolean sum and product.

Although this calculus has been used for studying model-checking algorithms [3, 7, 1], it has not been studied "per se".

Indeed, it has a fundamental property, that we name "selection property" that has several interesting consequences. At the end of the paper, we mention three of these consequences:

• the fact that a McNaughton game with a chain (or parity) condition on any graph has a memoryless winning strategy [5, 8, 9],

• the fact that any satisfiable formula of the modal μ-calculus has a bounded-branching model [6],

• the Rabin's regularity theorem for parity automata.

(*) Received February 1997, accepted June 1997.
([1]) La BRI, Université Bordeaux-I, Unité de Recherche Associée au CNRS, URA 1304.

This property is an extension of the quite trivial property of the Boolean sum in $\mathbb{B}$: if $(b_i)_{i \in I}$ is any family of Boolean values, then there exists j in I such that $\sum_{i \in I} b_i = b_j$. Now, let us consider $f : \mathbb{B} \to \mathbb{B}$ be defined as $f(x) = \sum_{i \in I} f_i(x)$. Then there still exists $j \in I$ such that $\mu x . f(x) = \mu x . f_i(x)$. This is because $\mu x . f(x) = f(0)$ and we apply the selection property to $f(0) = \sum_{i \in I} f_i(0)$. Inductively, we can also prove that there exists $j \in I$ such that

$$\mu x . \nu y . \mu z ... \sum_{i \in I} f_i(x, y, z, ...) = \mu x . \nu y . \mu z ... f_j(x, y, z, ...).$$

What is far less trivial is that the same holds for *vectorial fixed points.* When there is one fixed point operator, say the least one, the selection property in the vectorial case reads as follows. Let I be a set of indices, let $\mathbf{x}$ be a family of variables indexed by I, and let $\mathbf{f}(\mathbf{x})$ be a family, indexed by I, of monotonic mappings from $\mathbb{B}^I$ to $\mathbb{B}$. For any i in I, let J_i be another set of indices and assume that $f_i(\mathbf{x})$, the component of $\mathbf{f}$ of index i, is equal to $\sum_{j \in J_i} f_{i,j}(\mathbf{x})$. Then for each i there exists an index j_i in J_i such that $\mu \mathbf{x} . \mathbf{f}(\mathbf{x}) = \mu \mathbf{x} . \mathbf{f}'(\mathbf{x})$ where $\mathbf{f}'(\mathbf{x})$ is the vector whose component of index i is $f_{i,j_i}(\mathbf{x})$. In other words, for each component f_i of $\mathbf{f}$, we can *select* only one summand $f_{i,j}$, and still have the same least fixed point.

It should be noted that this selection property can be easily obtained as a straightforward consequence of the determinacy property for games with a parity condition, mentioned above. However, it might be of some interest to have a purely Boolean algebraic proof of it.

2. THE BOOLEAN μ-CALCULUS

Let $\mathbb{B}$ be the classical Boole algebra with two elements, 0 and 1.

For any set I of indices, of arbitrary cardinality $\mathbb{B}^I$, is a complete lattice. We denote respectively by $\mathbf{0}$ and $\mathbf{1}$ the minimum and the maximum of this complete lattice, *i.e.,* the vectors, indexed by I, whose all components are 0 or 1.

By Knaster-Tarski Theorem, any monotonic mapping $\mathbf{f} : \mathbb{B}^I \to \mathbb{B}^I$ has a least fixed point, denoted by $\mathbf{f}^\mu$, and a greatest fixed point, denoted by $\mathbf{f}^\nu$, both elements of $\mathbb{B}^I$.

It is well known that these fixed points can be characterized as follows:

1. $\mathbf{f}^\mu = \Pi \{\mathbf{b} \in \mathbb{B}^I | \mathbf{f}(\mathbf{b}) \leq \mathbf{b}\}$, $\mathbf{f}^\nu = \sum \{\mathbf{b} \in \mathbb{B}^I | \mathbf{b} \leq \mathbf{f}(\mathbf{b})\}$.

2. Let $(\mathbf{a}_\alpha)_\alpha$ and $(\mathbf{b}_\alpha)_\alpha$ be the sequences of elements of $\mathbb{B}^I$, indexed by ordinal numbers, defined by

$$\begin{array}{lll} \mathbf{a}_0 = \mathbf{0}, & \mathbf{b}_0 = \mathbf{1}, & \\ \mathbf{a}_{\alpha+1} = \mathbf{f}(\mathbf{a}_\alpha), & \mathbf{b}_{\alpha+1} = \mathbf{f}(\mathbf{b}_\alpha), & \text{for } \alpha+1 \text{ a successor ordinal,} \\ \mathbf{a}_\beta = \sum_{\alpha<\beta} \mathbf{a}_\alpha, & \mathbf{b}_\beta = \prod_{\alpha<\beta} \mathbf{b}_\alpha, & \text{for } \beta \text{ a limit ordinal.} \end{array}$$

Then there is an ordinal γ such that $\mathbf{f}^\mu = \mathbf{a}_\gamma$ and $\mathbf{f}^\nu = \mathbf{b}_\gamma$.

More generally, for any set E, if $\mathbf{f}(\mathbf{x}, y)$ is any mapping from $\mathbb{B}^I \times E$ into $\mathbb{B}^I$ that is monotonic in its first argument, we denote by $\mu\mathbf{x}\,.\,\mathbf{f}(\mathbf{x}, y)$ (resp. $\nu\mathbf{x}\,.\,\mathbf{f}(\mathbf{x}, y)$) the mapping from E into $\mathbb{B}^I$ defined by: for any $e \in E$, $\mu\mathbf{x}\,.\,\mathbf{f}(\mathbf{x}, e)$ (resp. $\nu\mathbf{x}\,.\,\mathbf{f}(\mathbf{x}, e)$) is the least (resp. greatest) fixed point of the mapping $\mathbf{f}(\mathbf{x}, e) : \mathbb{B}^I \to \mathbb{B}^I$.

If, moreover, E is an ordered set, and if $\mathbf{f}(\mathbf{x}, y)$ is monotonic in its second argument too, then $\mu\mathbf{x}\,.\,\mathbf{f}(\mathbf{x}, y)$ and $\nu\mathbf{x}\,.\,\mathbf{f}(\mathbf{x}, y)$ are also monotonic with respect to the argument y.

Therefore, if $\mathbf{f}(\mathbf{x}_1, ..., \mathbf{x}_n, y) : (\mathbb{B}^I)^n \times E \to \mathbb{B}^I$ is monotonic with respect to any $\mathbf{x}_i$, $\theta_1\,\mathbf{x}_1 ... \theta_n\,\mathbf{x}_n\,.\,\mathbf{f}(\mathbf{x}_1, ..., \mathbf{x}_n, y)$, where each θ_i is μ or ν, is a well-defined mapping from E into $\mathbb{B}^I$.

3. THE THEOREM

Let $\mathbf{f}(\mathbf{x}_1, ..., \mathbf{x}_n) : (\mathbb{B}^I)^n \to \mathbb{B}^I$ be monotonic in all its arguments, where I is a set of indices of arbitrary cardinality. For each $i \in I$ let $f_i(\mathbf{x}_1, ..., \mathbf{x}_n) : (\mathbb{B}^I)^n \to \mathbb{B}$ be the component of $\mathbf{f}$ of index i.

We assume that for each index $i \in I$ there exists a set J_i of indices, also of arbitrary cardinality, such that

$$f_i(\mathbf{x}_1, ..., \mathbf{x}_n) = \sum_{j \in J} f_{i,j}(\mathbf{x}_1, ..., \mathbf{x}_n).$$

A *selector* is a mapping σ that associates, with each i in I, an element $\sigma(i)$ of J_i. Given a selector σ, we define $\mathbf{f}_\sigma(\mathbf{x}_1, ..., \mathbf{x}_n) : (\mathbb{B}^I)^n \to \mathbb{B}^I$ as the mapping whose the i-th component is $f_{i,\sigma(i)}(\mathbf{x}_1, ..., \mathbf{x}_n) : (\mathbb{B}^I)^n \to \mathbb{B}$.

THEOREM 1: *Let* $\mathbf{f}$ *be defined as above and let*

$$\mathbf{a} = \theta_1\,\mathbf{x}_1 ... \theta_n\,\mathbf{x}_n\,.\,\mathbf{f}(\mathbf{x}_1, ..., \mathbf{x}_n) \in \mathbb{B}^I.$$

Then there exists a selector σ *such that* $\mathbf{a} = \theta_1\,\mathbf{x}_1 ... \theta_n\,\mathbf{x}_n\,.\,\mathbf{f}_\sigma(\mathbf{x}_1, ..., \mathbf{x}_n)$.

In order to keep notations simple enough, we first prove this theorem in the case where each set J_i has only two elements (dyadic case). Then we explain how to extend this proof in the general case where each J_i has any cardinality.

3.1. The dyadic case

Let us assume that each component f_i of $\mathbf{f}$ is written $f_{i,1} + f_{i,2}$. Let $\mathbf{y}$ and $\mathbf{z}$ be two families of variables, indexed by I. We consider the mapping

$$\mathbf{g}(\mathbf{y}, \mathbf{z}, \mathbf{x}_1, \ldots, \mathbf{x}_n) : (\mathbb{B}^I)^{n+2} \to \mathbb{B}^I$$

whose the i-th component is $y_i \cdot f_{i,1} + z_i \cdot f_{i,2}$. It is clear that

$$\mathbf{f}(\mathbf{x}_1, \ldots, \mathbf{x}_n) = \mathbf{g}(\mathbf{1}, \mathbf{1}, \mathbf{x}_1, \ldots, \mathbf{x}_n).$$

Moreover, with each selector σ we associate the element $\mathbf{u}_\sigma$ of $\mathbb{B}^I$ whose the i-th component is 0 if $\sigma(i) = 2$, 1 if $\sigma(i) = 1$. It follows that $\mathbf{f}_\sigma(\mathbf{x}_1, \ldots, \mathbf{x}_n) = \mathbf{g}(\mathbf{u}_\sigma, \overline{\mathbf{u}}_\sigma, \mathbf{x}_1, \ldots, \mathbf{x}_n)$, where $\overline{\mathbf{u}}_\sigma$ is the complement of $\mathbf{u}_\sigma$ in the Boolean algebra $\mathbb{B}^I$.

Since the correspondence between σ and $\mathbf{u}_\sigma$ is bijective, the theorem can be stated:

There exists $\mathbf{u} \in \mathbb{B}^I$ such that

$$\theta_1 \mathbf{x}_1 \ldots \theta_n \mathbf{x}_n \,.\, \mathbf{g}(\mathbf{1}, \mathbf{1}, \mathbf{x}_1, \ldots, \mathbf{x}_n) = \theta_1 \mathbf{x}_1 \ldots \theta_n \mathbf{x}_n \,.\, \mathbf{g}(\mathbf{u}, \overline{\mathbf{u}}, \mathbf{x}_1, \ldots, \mathbf{x}_n).$$

To prove this theorem we need a definition.

DEFINITION 1: We say that a monotonic mapping $\mathbf{f}(\mathbf{y}, \mathbf{z}, \mathbf{x}) : \mathbb{B}^I \times \mathbb{B}^I \times (\mathbb{B}^I)^m \to \mathbb{B}^I$ *has property* S if $\forall \mathbf{u}, \mathbf{u}', \mathbf{v}, \mathbf{v}' \in \mathbb{B}^I$ such that $\mathbf{u} \leq \mathbf{v}$ and $\mathbf{u}' \leq \mathbf{v}'$, $\forall \mathbf{e}_1, \mathbf{e}_2 \in (\mathbb{B}^I)^m$ such that $\mathbf{e}_1 \leq \mathbf{e}_2$, if $\mathbf{u} + \mathbf{u}' \leq \mathbf{f}(\mathbf{u}, \mathbf{u}', \mathbf{e}_1)$ then there exist $\mathbf{w}, \mathbf{w}' \in \mathbb{B}^I$ such that

- $\mathbf{u} \leq \mathbf{w} \leq \mathbf{v}$ and $\mathbf{u}' \leq \mathbf{w}' \leq \mathbf{v}'$
- $\mathbf{u} \,.\, \mathbf{u}' = \mathbf{w} \,.\, \mathbf{w}'$,
- $\mathbf{w} + \mathbf{w}' = \mathbf{f}(\mathbf{w}, \mathbf{w}', \mathbf{e}_2) = \mathbf{f}(\mathbf{v}, \mathbf{v}', \mathbf{e}_2)$,

where $\mathbf{u} + \mathbf{u}'$ and $\mathbf{u} \,.\, \mathbf{u}'$ are the pointwise extensions to $\mathbb{B}^I$ of the sum and product of $\mathbb{B}$.

LEMMA 2: *If* $\mathbf{f}(\mathbf{y}, \mathbf{z}, \mathbf{x})$ *is such that* $f_i = y_i \cdot f_{i,1}(\mathbf{x}) + z_i \cdot f_{i,2}(\mathbf{x})$, *then it has property* S.

Proof: It is sufficient to show that $f(y, z, \mathbf{x}) = y \,.\, g_1(\mathbf{x}) + z \,.\, g_2(\mathbf{x})$ has property S in the following restricted sense: $\forall u, u', v, v' \in \mathbb{B}$ such that $u \leq v$ and $u' \leq v'$, $\forall \mathbf{e}_1, \mathbf{e}_2 \in (\mathbb{B}^I)^m$ such that $\mathbf{e}_1 \leq \mathbf{e}_2$, if $u + u' \leq f(u, u', \mathbf{e}_1)$ then there exist $w, w' \in \mathbb{B}$ such that

- $u \leq w \leq v$ and $u' \leq w' \leq v'$,
- $u \,.\, u' = w \,.\, w'$,
- $w + w' = f(w, w', \mathbf{e}_2) = f(v, v', \mathbf{e}_2)$.

Let us remark that $u + u' \leq f(u, u', \mathbf{e}_1) \leq f(u, u', \mathbf{e}_2) \leq f(v, v', \mathbf{e}_2)$.

If $u + u' = 1$, we have $1 = f(u, u', \mathbf{e}_2) = f(v, v', \mathbf{e}_2) = u + u'$ and we take $w = u$, $w' = u'$. If $f(v, v', \mathbf{e}_2) = 0$ then we have $0 = u + u' = f(u, u', \mathbf{e}_2) = f(v, v', \mathbf{e}_2) = u + u'$ and, again, we take $w = u$, $w' = u'$.

It remains to consider the case $u + u' = 0$ (hence, $u = u' = u \,.\, u' = 0$) and $f(v, v', \mathbf{e}_2) = 1$. We cannot have $v + v' = 0$, because $f(0, 0, \mathbf{e}) = 0$ for any $\mathbf{e}$. If $v \,.\, v' = 0$ we can take $w = v$, $w' = v'$ since $f(v, v', \mathbf{e}_2) = v + v' = 1$. If $v \,.\, v' = 1$, (*i.e.*, $v = v' = 1$), then $f(v, v', \mathbf{e}_2) = f(1, 1, \mathbf{e}_2) = g_1(\mathbf{e}_2) + g_2(\mathbf{e}_2) = 1$. Thus $g_i(\mathbf{e}_2) = 1$ for some $i \in \{1, 2\}$ and we take $w = 1$, $w' = 0$ or $w = 0$, $w' = 1$ according to the value of i. □

LEMMA 3: *Let us assume that* $\mathbf{f}(\mathbf{y}, \mathbf{z}, \mathbf{x}, \mathbf{x}') : \mathbb{B}^I \times \mathbb{B}^I \times (\mathbb{B}^I)^{m+1} \to \mathbb{B}^I$ *has property* S. *Then* $\theta \mathbf{x} \,.\, \mathbf{f}(\mathbf{y}, \mathbf{z}, \mathbf{x}, \mathbf{x}') : \mathbb{B}^I \times \mathbb{B}^I \times (\mathbb{B}^I)^m \to \mathbb{B}^I$ *has property* S.

Proof: Let $\mathbf{g}(\mathbf{y}, \mathbf{z}, \mathbf{x}') = \theta \mathbf{x} \,.\, \mathbf{f}(\mathbf{y}, \mathbf{z}, \mathbf{x}, \mathbf{x}')$. Let $\mathbf{u}, \mathbf{u}', \mathbf{v}, \mathbf{v}' \in \mathbb{B}^I$ such that $\mathbf{u} \leq \mathbf{v}$ and $\mathbf{u}' \leq \mathbf{v}'$, let $\mathbf{e}_1, \mathbf{e}_2 \in (\mathbb{B}^I)^m$ such that $\mathbf{e}_1 \leq \mathbf{e}_2$, and let us assume that $\mathbf{u} + \mathbf{u}' \leq \mathbf{g}(\mathbf{u}, \mathbf{u}', \mathbf{e}_1)$. We have to show that there exist $\mathbf{w}, \mathbf{w}' \in \mathbb{B}^I$ such that

- $\mathbf{u} \leq \mathbf{w} \leq \mathbf{v}$ and $\mathbf{u}' \leq \mathbf{w}' \leq \mathbf{v}'$,
- $\mathbf{u} \,.\, \mathbf{u}' = \mathbf{w} \,.\, \mathbf{w}'$,
- $\mathbf{w} + \mathbf{w}' = \mathbf{g}(\mathbf{w}, \mathbf{w}', \mathbf{e}_2) = \mathbf{g}(\mathbf{v}, \mathbf{v}', \mathbf{e}_2)$.

Let $\mathbf{a} = \mathbf{g}(\mathbf{u}, \mathbf{u}', \mathbf{e}_1)$ and $\mathbf{b} = \mathbf{g}(\mathbf{v}, \mathbf{v}', \mathbf{e}_2)$. Obviously,

$$\mathbf{a} = \mathbf{f}(\mathbf{u}, \mathbf{u}', \mathbf{a}, \mathbf{e}_1) \leq \mathbf{b} = \mathbf{f}(\mathbf{v}, \mathbf{v}', \mathbf{b}, \mathbf{e}_2).$$

We have two different proofs according to $\theta = \mu$ or $\theta = \nu$.

Case $\theta = \mu$. Let us consider the sequence $\mathbf{b}_\beta$ of elements of $\mathbb{B}^I$, indexed by ordinal numbers, and defined by $\mathbf{b}_0 = \mathbf{a}$, $\mathbf{b}_{\alpha+1} = \mathbf{f}(\mathbf{v}, \mathbf{v}', \mathbf{b}_\alpha, \mathbf{e}_2)$, $\mathbf{b}_\beta = \sum_{\alpha<\beta} \mathbf{b}_\alpha$.

This sequence is increasing, since $\mathbf{f}$ is monotonic and

$$\mathbf{b}_0 = \mathbf{a} = \mathbf{f}(\mathbf{u}, \mathbf{u}', \mathbf{a}, \mathbf{e}_1) \leq \mathbf{f}(\mathbf{v}, \mathbf{v}', \mathbf{b}_0, \mathbf{e}_2) = \mathbf{b}_1.$$

Moreover, it is easy to see that $\mathbf{b} = \mathbf{b}_\gamma = \mathbf{b}_{\gamma+1}$ for some ordinal γ.

Now, we construct, inductively, two increasing sequences $\mathbf{w}_\alpha$ and $\mathbf{w}'_\alpha$, for $0 \leq \alpha \leq \gamma + 1$, that satisfy

- $\forall \alpha \leq \gamma + 1$, $\mathbf{u} \leq \mathbf{w}_\alpha \leq \mathbf{v}$, $\mathbf{u}' \leq \mathbf{w}'_\alpha \leq \mathbf{v}'$,
- $\forall \alpha \leq \gamma + 1$, $\mathbf{u} \,.\, \mathbf{u}' = \mathbf{w}_\alpha \,.\, \mathbf{w}'_\alpha$,
- $\forall \alpha : 1 \leq \alpha \leq \gamma + 1$, $\mathbf{w}_\alpha + \mathbf{w}'_\alpha = \mathbf{b}_\alpha \leq \mathbf{f}(\mathbf{w}_\alpha, \mathbf{w}'_\alpha, \mathbf{b}_\alpha, \mathbf{e}_2)$,
- $\forall \alpha \leq \gamma$, $\mathbf{b}_{\alpha+1} = \mathbf{f}(\mathbf{w}_{\alpha+1}, \mathbf{w}'_{\alpha+1}, \mathbf{b}_\alpha, \mathbf{e}_2)$.

The definition is as follows: $\mathbf{w}_0 = \mathbf{u}$, $\mathbf{w}'_0 = \mathbf{u}'$. Since

$$\mathbf{w}_0 + \mathbf{w}'_0 = \mathbf{u} + \mathbf{u}' \leq \mathbf{a} \leq \mathbf{b}_1 = \mathbf{f}(\mathbf{v}, \mathbf{v}', \mathbf{b}_0, \mathbf{e}_2),$$

and since $\mathbf{f}$ has property S, there exists $\mathbf{w}_1$ and $\mathbf{w}'_1$ such that

$$\mathbf{w}_1 \,.\, \mathbf{w}'_1 = \mathbf{w}_0 \,.\, \mathbf{w}'_0,$$

$$\mathbf{w}_1 + \mathbf{w}'_1 = \mathbf{b}_1 = \mathbf{f}(\mathbf{w}_1, \mathbf{w}'_1, \mathbf{b}_0, \mathbf{e}_2) \leq \mathbf{f}(\mathbf{w}_1, \mathbf{w}'_1, \mathbf{b}_1, \mathbf{e}_2).$$

Similarly, if $\mathbf{w}_\alpha + \mathbf{w}'_\alpha = \mathbf{b}_\alpha \leq \mathbf{f}(\mathbf{w}_\alpha, \mathbf{w}'_\alpha, \mathbf{b}_\alpha, \mathbf{e}_2)$, we can find $\mathbf{w}_{\alpha+1}$ and $\mathbf{w}'_{\alpha+1}$ such that

$$\mathbf{w}_{\alpha+1} \,.\, \mathbf{w}'_{\alpha+1} = \mathbf{w}_\alpha \,.\, \mathbf{w}'_\alpha = \mathbf{u} \,.\, \mathbf{u}',$$

$$\begin{aligned}\mathbf{b}_{\alpha+1} = \mathbf{w}_{\alpha+1} + \mathbf{w}'_{\alpha+1} &= \mathbf{f}(\mathbf{w}_{\alpha+1}, \mathbf{w}'_{\alpha+1}, \mathbf{b}_\alpha, \mathbf{e}_2) \\ &\leq \mathbf{f}(\mathbf{w}_{\alpha+1}, \mathbf{w}'_{\alpha+1}, \mathbf{b}_{\alpha+1}, \mathbf{e}_2).\end{aligned}$$

For limit ordinals, we set $\mathbf{w}_\beta = \sum_{\alpha<\beta} \mathbf{w}_\alpha$ and $\mathbf{w}'_\beta = \sum_{\alpha<\beta} \mathbf{w}'_\alpha$. Since $\mathbf{w}_\alpha \leq \mathbf{w}_\beta$ and $\mathbf{w}'_\alpha \leq \mathbf{w}'_\beta$, we get $\mathbf{u} \,.\, \mathbf{u}' = \mathbf{w}_\alpha \,.\, \mathbf{w}'_\alpha \leq \mathbf{w}_\beta \,.\, \mathbf{w}'_\beta$. Assume that this inequality is strict, that is, for some component i, $(\mathbf{u} \,.\, \mathbf{u}')_i = 0$ and $(\mathbf{w}_\beta \,.\, \mathbf{w}'_\beta)_i = 1$. The last equality implies $(\mathbf{w}_\beta)_i = (\mathbf{w}'_\beta)_i = 1$, thus there exists α_1 and α_2 such that $(\mathbf{w}_{\alpha_1})_i = (\mathbf{w}'_{\alpha_2})_i = 1$. For $\alpha = \bigvee(\alpha_1, \alpha_2)$ we get $(\mathbf{w}_\alpha)_i = (\mathbf{w}'_\alpha)_i = 1$, thus $(\mathbf{u} \,.\, \mathbf{u}')_i = 1$, a contradiction. We also have, for $\alpha < \beta$, $\mathbf{b}_\alpha \leq \mathbf{f}(\mathbf{w}_\alpha, \mathbf{w}'_\alpha, \mathbf{b}_\alpha, \mathbf{e}_2) \leq \mathbf{f}(\mathbf{w}_\beta, \mathbf{w}'_\beta, \mathbf{b}_\beta, \mathbf{e}_2)$. Hence, $\mathbf{b}_\beta \leq \mathbf{f}(\mathbf{w}_\beta, \mathbf{w}'_\beta, \mathbf{b}_\beta, \mathbf{e}_2)$. It remains to prove that $\mathbf{b}_\beta = \mathbf{w}_\beta + \mathbf{w}'_\beta$. Again, $\mathbf{b}_\alpha = \mathbf{w}_\alpha + \mathbf{w}'_\alpha \leq \mathbf{w}_\beta + \mathbf{w}'_\beta$, hence $\mathbf{b}_\beta \leq \mathbf{w}_\beta + \mathbf{w}'_\beta$. Assume that this inequality is strict, *i.e.*, for some component i, $(\mathbf{b}_\beta)_i = 0$ and $(\mathbf{w}_\beta)_i + (\mathbf{w}'_\beta)_i = 1$. Since $(\mathbf{b}_\beta)_i = 0$, for all $\alpha < \beta$, $(\mathbf{b}_\alpha)_i = 0$, hence, since $\mathbf{b}_\alpha = \mathbf{w}_\alpha + \mathbf{w}'_\alpha$, $(\mathbf{w}_\alpha)_i + (\mathbf{w}'_\alpha)_i = 0 = (\mathbf{w}_\alpha)_i = (\mathbf{w}'_\alpha)_i$. If follows that $(\mathbf{w}_\beta)_i = (\mathbf{w}'_\beta)_i = 0$, a contradiction.

Now, we have

$$\mathbf{b} = \mathbf{b}_{\gamma+1} = \mathbf{f}(\mathbf{w}_{\gamma+1}, \mathbf{w}'_{\gamma+1}, \mathbf{b}_\gamma, \mathbf{e}_2) = \mathbf{f}(\mathbf{w}_{\gamma+1}, \mathbf{w}'_{\gamma+1}, \mathbf{b}, \mathbf{e}_2).$$

We take $\mathbf{w} = \mathbf{w}_{\gamma+1}$, $\mathbf{w}' = \mathbf{w}'_{\gamma+1}$. Since $\mathbf{b} = \mathbf{f}(\mathbf{w}, \mathbf{w}', \mathbf{b}, \mathbf{e}_2)$, we have

$$\mathbf{b} \geq \mu\mathbf{x}.\mathbf{f}(\mathbf{w}, \mathbf{w}', \mathbf{x}, \mathbf{e}_2) = \mathbf{g}(\mathbf{w}, \mathbf{w}', \mathbf{e}_2).$$

It remains to prove the reverse inequality.

Let $\mathbf{c}$ be any element of $\mathbb{B}^I$ such that $\mathbf{c} = \mathbf{f}(\mathbf{w}, \mathbf{w}', \mathbf{c}, \mathbf{e}_2)$. We prove by induction that $\mathbf{b}_\alpha \leq \mathbf{c}$. Firstly,

$$\mathbf{b}_0 = \mathbf{a} = \mu\mathbf{x}.\mathbf{f}(\mathbf{u}, \mathbf{u}', \mathbf{x}, \mathbf{e}_1) \leq \mu\mathbf{x}.\mathbf{f}(\mathbf{w}, \mathbf{w}', \mathbf{x}, \mathbf{e}_2) \leq \mathbf{c}.$$

If $\mathbf{b}_\alpha \leq \mathbf{c}$ then $\mathbf{b}_{\alpha+1} = \mathbf{f}(\mathbf{w}_{\alpha+1}, \mathbf{w}'_{\alpha+1}, \mathbf{b}_\alpha, \mathbf{e}_2) \leq \mathbf{f}(\mathbf{w}, \mathbf{w}', \mathbf{c}, \mathbf{e}_2) = \mathbf{c}$ and $\mathbf{b}_\beta = \sum_{\alpha<\beta} \mathbf{b}_\alpha \leq \mathbf{c}$.

Case $\theta = \nu$ Since $\mathbf{f}$ has property S, there exist $\mathbf{w}_0$ and $\mathbf{w}'_0$ such that $\mathbf{u} \leq \mathbf{w}_0 \leq \mathbf{v}$ and

$$\mathbf{u}' \leq \mathbf{w}'_0 \leq \mathbf{v}', \ \mathbf{w}_0 . \mathbf{w}'_0 = \mathbf{u}.\mathbf{u}', \ \mathbf{w}_0 + \mathbf{w}'_0 = \mathbf{b} = \mathbf{f}(\mathbf{w}_0, \mathbf{w}'_0, \mathbf{b}, \mathbf{e}_2).$$

Now, consider the decreasing sequence $\mathbf{b}_\alpha$, indexed by ordinal numbers, defined by $\mathbf{b}_0 = \mathbf{1}, \mathbf{b}_{\alpha+1} = \mathbf{f}(\mathbf{v}, \mathbf{v}', \mathbf{b}_\alpha, \mathbf{e}_2)$, $\mathbf{b}_\beta = \prod_{\alpha<\beta} \mathbf{b}_\alpha$.

Then $\mathbf{b} = \mathbf{b}_\gamma = \mathbf{b}_{\gamma+1}$ for some ordinal γ.

Since $\mathbf{f}$ has property S, for each successor ordinal $\alpha + 1 \leq \gamma + 1$ there exist $\mathbf{w}_{\alpha+1}$ and $\mathbf{w}'_{\alpha+1}$ such that $\mathbf{w}_0 \leq \mathbf{w}_{\alpha+1} \leq \mathbf{v}$ and

$$\mathbf{w}'_0 \leq \mathbf{w}'_{\alpha+1} \leq \mathbf{v}', \ \mathbf{w}_{\alpha+1} . \mathbf{w}'_{\alpha+1} = \mathbf{w}_0 . \mathbf{w}'_0 = \mathbf{u}.\mathbf{u}',$$

$$\mathbf{w}_{\alpha+1} + \mathbf{w}'_{\alpha+1} = \mathbf{b}_{\alpha+1} = \mathbf{f}(\mathbf{w}_{\alpha+1}, \mathbf{w}'_{\alpha+1}, \mathbf{b}_\alpha, \mathbf{e}_2).$$

Let $\mathbf{w} = \prod_{\alpha+1\leq\gamma+1} \mathbf{w}_{\alpha+1}$ and $\mathbf{w}' = \prod_{\alpha+1\leq\gamma+1} \mathbf{w}'_{\alpha+1}$. We claim that

1. $\mathbf{u} \leq \mathbf{w} \leq \mathbf{v}$ and $\mathbf{u}' \leq \mathbf{w}' \leq \mathbf{v}'$
2. $\mathbf{w}.\mathbf{w}' = \mathbf{w}_0 . \mathbf{w}'_0 = \mathbf{u}.\mathbf{u}'$,
3. $\mathbf{w} + \mathbf{w}' = \mathbf{b}$,
4. $\mathbf{b} = \nu\mathbf{x}.\mathbf{f}(\mathbf{w}, \mathbf{w}', \mathbf{x}, \mathbf{e}_2)$.

Since $\mathbf{u} \leq \mathbf{w}_0 \leq \mathbf{w}_{\alpha+1} \leq \mathbf{v}$ and $\mathbf{u}' \leq \mathbf{w}'_0 \leq \mathbf{w}'_{\alpha+1} \leq \mathbf{v}'$, the point 1 above is satisfied.

Since $\mathbf{w}_0 \leq \mathbf{w} \leq \mathbf{w}_{\alpha+1}$ and $\mathbf{w}'_0 \leq \mathbf{w}' \leq \mathbf{w}'_{\alpha+1}$, we have

$$\mathbf{u}.\mathbf{u}' = \mathbf{w}_0 . \mathbf{w}'_0 \leq \mathbf{w}.\mathbf{w}' \leq \mathbf{w}_{\alpha+1} . \mathbf{w}'_{\alpha+1} = \mathbf{u}.\mathbf{u}'$$

and the point 2 above is satisfied.

For the point 3, we have $\mathbf{b} = \mathbf{w}_0 + \mathbf{w}'_0 \leq \mathbf{w} + \mathbf{w}' \leq \mathbf{w}_{\gamma+1} + \mathbf{w}'_{\gamma+1} = \mathbf{b}$.

For the point 4, we have

$$\mathbf{b} = \mathbf{f}(\mathbf{w}_0, \mathbf{w}'_0, \mathbf{b}, \mathbf{e}_2) \leq \mathbf{f}(\mathbf{w}, \mathbf{w}', \mathbf{b}, \mathbf{e}_2) \leq \mathbf{f}(\mathbf{w}_{\gamma+1}, \mathbf{w}'_{\gamma+1}, \mathbf{b}, \mathbf{e}_2) = \mathbf{b}$$

hence $\mathbf{b} \leq \nu\mathbf{x}.\mathbf{f}(\mathbf{w}, \mathbf{w}', \mathbf{x}, \mathbf{e}_2)$. Let

$$\mathbf{c} = \nu\mathbf{x}.\mathbf{f}(\mathbf{w}, \mathbf{w}', \mathbf{x}, \mathbf{e}_2) = \mathbf{f}(\mathbf{w}, \mathbf{w}', \mathbf{c}, \mathbf{e}_2)$$

and let us show, inductively, that $\mathbf{c} \leq \mathbf{b}_\alpha$ for any $\alpha \leq \gamma + 1$. Obviously, $\mathbf{c} \leq \mathbf{b}_0 = \mathbf{1}$. If $\mathbf{c} \leq \mathbf{b}_\alpha$ then

$$\mathbf{c} = \mathbf{f}(\mathbf{w}, \mathbf{w}', \mathbf{c}, \mathbf{e}_2) \leq \mathbf{f}(\mathbf{w}_{\alpha+1}, \mathbf{w}'_{\alpha+1}, \mathbf{b}_\alpha, \mathbf{e}_2) = \mathbf{b}_{\alpha+1},$$

and $\mathbf{c} \leq \mathbf{b}_\alpha$, for all $\alpha < \beta$, implies $\mathbf{c} \leq \prod_{\alpha<\beta} \mathbf{b}_\alpha = \mathbf{b}_\beta$.

The proof of the theorem is a direct consequence of the two previous lemmas. Let $\mathbf{h}(\mathbf{y}, \mathbf{z}) = \theta_1 \mathbf{x}_1 . \theta_2 \mathbf{x}_2 ... \theta_n \mathbf{x}_n . \mathbf{g}$ where $\mathbf{g}$ has the form explained at the beginning of this section. Then $\mathbf{h}$ has property S. Thus, $\mathbf{0} = \mathbf{0} + \mathbf{0} \leq \mathbf{h}(\mathbf{0}, \mathbf{0}) \leq \mathbf{h}(\mathbf{1}, \mathbf{1})$, there exist $\mathbf{w}$ and $\mathbf{w}'$ such that $0 = \mathbf{w} . \mathbf{w}'$ and $\mathbf{w} + \mathbf{w}' = \mathbf{h}(\mathbf{w}, \mathbf{w}') = \mathbf{h}(\mathbf{1}, \mathbf{1})$. But $\mathbf{0} = \mathbf{w} . \mathbf{w}'$ implies $\mathbf{w}' \leq \overline{\mathbf{w}}$, hence $\mathbf{h}(\mathbf{1}, \mathbf{1}) = \mathbf{h}(\mathbf{w}, \mathbf{w}') \leq \mathbf{h}(\mathbf{w}, \mathbf{w}') \leq \mathbf{h}(\mathbf{1}, \mathbf{1})$.

3.2. The general case

Here, we assume that the i-th component of $\mathbf{f}$ is $f_i = \sum_{j \in J_i} f_{i,j}$ where J_i is any set of indices. Without loss of generality, we may assume that the sets J_i are disjoint and we set $J = \bigcup_{i \in I} J_i$.

Let us consider Boolean variables y_j for $j \in J$ and write f_i in the form $\sum_{j \in J_i} y_j \cdot f_{i,j}$. Now $\mathbf{f}$ is a mapping from $\mathbb{B}^J \times (\mathbb{B}^I)^n$ to $\mathbb{B}^I$ and

$$\mathbf{g}(\mathbf{y}) = \theta_1 \mathbf{x}_1 . \theta_2 \mathbf{x}_2 ... \theta_n \mathbf{x}_n . \mathbf{f}(\mathbf{y}, \mathbf{x}_1, \mathbf{x}_2 ..., \mathbf{x}_n)$$

is a mapping from $\mathbb{B}^J$ to $\mathbb{B}^I$.

Then the theorem is equivalent to the following statement:

Let $\mathbf{g}(\mathbf{y}) = \theta_1 \mathbf{x}_1 . \theta_2 \mathbf{x}_2 ... \theta_n \mathbf{x}_n . \mathbf{f}$. Then there exists $\mathbf{u} = (u_j)_{j \in J} \in \mathbb{B}^J$ such that $\mathbf{g}(\mathbf{1}) = \mathbf{g}(\mathbf{u})$ and for any $i \in I$ there is exactly one j in J_i such that $u_j = 1$.

Remark that in the last condition above, we can replace "exactly one" by "at most one".

The proof is quite similar to the proof for the dyadic case As above, we define the *property* S for $\mathbf{f}(\mathbf{y}, \mathbf{x}) : \mathbb{B}^J \times (\mathbb{B}^I)^m \to \mathbb{B}^I$. The two functions

$\mathbf{u} + \mathbf{u}'$ and $\mathbf{u} \,.\, \mathbf{u}'$ that appear in this definition have to be replaced by the two monotonic functions S and P from $\mathbb{B}^J$ to $\mathbb{B}^I$ defined as follows. For $\mathbf{u} = (u_j)_{j \in J} \in \mathbb{B}^J$

the i-th component of $S(\mathbf{u})$ is equal to $\sum_{j \in J_i} u_j$,

• the i-th component of $P(\mathbf{u})$ is equal to 0 if and only if there is at most one j in J_i such that $u_j = 1$.

Now, $\mathbf{f}(\mathbf{y}, \mathbf{x})$ has property S if $\forall \mathbf{u}, v \in \mathbb{B}^I$ such that $\mathbf{u} \leq \mathbf{v}$, $\forall \mathbf{e}_1, \mathbf{e}_2 \in (\mathbb{B}^I)^m$ such that $\mathbf{e}_1 \leq \mathbf{e}_2$, if $S(\mathbf{u}) \leq \mathbf{f}(\mathbf{u}, \mathbf{e}_1)$ then there exist $\mathbf{w} \in \mathbb{B}^J$ such that

- $\mathbf{u} \leq \mathbf{w} \leq \mathbf{v}$,
- $P(\mathbf{u}) = P(\mathbf{w})$,
- $S(\mathbf{w}) = \mathbf{f}(\mathbf{w}, \mathbf{e}_2) = \mathbf{f}(\mathbf{v}, \mathbf{e}_2)$,

To prove the basis of the induction, it is enough to prove that

$$f(\mathbf{y}, \mathbf{x}) = \sum_{j \in J} y_j \cdot f_j(\mathbf{x})$$

has property S. Let $\mathbf{u} \leq \mathbf{v}$, $\mathbf{e}_1 \leq \mathbf{e}_2$ and $S(\mathbf{u}) \leq f(\mathbf{u}, \mathbf{e}_1)$. Then $S(\mathbf{u}) \leq f(\mathbf{u}, \mathbf{e}_1) \leq f(\mathbf{v}, \mathbf{e}_2) \leq S(\mathbf{v})$. If $S(\mathbf{u}) = 1$ or $f(\mathbf{v}, \mathbf{e}_2) = 0$, we can take $\mathbf{w} = \mathbf{u}$. If $S(\mathbf{u}) = 0$ and $f(\mathbf{v}, \mathbf{e}_2) = 1$, then $\forall j \in J$, $u_j = 0$ and, since $f(\mathbf{v}, \mathbf{e}_2) = \sum_{j \in J} v_j \cdot f_j(\mathbf{e}_2) = 1$, there exists j_0 such that $v_{j_0} = 1$ and $f_{j_0}(\mathbf{e}_2) = 1$. Then, we take $\mathbf{w}$ defined by $w_j = 1$ if and only if $j = j_0$.

To prove the induction step, we proceed exactly like in the dyadic case. The only difference is that since sum and product are replaced by S and P, we need, for the case $\theta = \mu$, the following property: if $(\mathbf{w}_\alpha)_{\alpha < \beta}$ is an increasing sequence of elements of $\mathbb{B}^J$ such that $\mathbf{u} \leq \mathbf{w}_\alpha$ and $P(\mathbf{u}) = P(\mathbf{w}_\alpha)$ then $P(\mathbf{u}) = P(\sum_{\alpha < \beta} \mathbf{w}_\alpha)$ and $S(\sum_{\alpha < \beta} \mathbf{w}_\alpha) = \sum_{\alpha < \beta} S(\mathbf{w}_\alpha)$. This property is proved exactly like the similar one with sum and product.

4. APPLICATIONS

4.1. Games on graphs

A McNaughton's game [5, 8] is played by two players (Val and Andy) on a directed graph $G = \langle V_V, V_A, E \rangle$ where V_V and V_A are two disjoint sets of vertices and the set of directed edges is a subset E of $V_V \times V_A \cup V_A \times V_V$. Moreover it is assumed that any vertex in G is the source of an edge.

A *position* is just a vertex. It is a position for Val if this vertex is in V_V and a position for Andy if it is in V_A. In a position v for some player, a *move* is performed by that player by choosing a position v' such that $\langle v, v' \rangle \in E$, that is a position for the other player. Any sequence of moves can be extended into an infinite one that is called a *play*.

To decide which player wins a play, we define a set C of infinite sequences of $V = V_A \cup V_V$. A play p is won by Val if and only p is in C. We denote by W_V the set of positions where Val has a winning strategy.

Now, we assume that the membership in C of a play p does not depend on any of its finite prefixes, *i.e.*, if $p \in V^\omega$, $p' \in V^*$, $p'' \in V^*$, then $p' p \in C$ iff $p'' p \in C$.

It follows that a vertex v is in W_V if and only if

$v \in V_A$ (v is a position for Andy) and all successors of v are in W_V (whichever move Andy plays, he reaches a position winning for Val),

$v \in V_V$ (v is a position for Val) and there is a successor of v that is in W_V (Val can reach a winning position).

Let us introduce a Boolean value w_v for each vertex v such that $w_v = 1$ iff $v \in W_V$. Then the above condition can be translated into:

$$\forall v \in V,\ w_v = \begin{cases} \sum_{\langle v, v' \rangle \in E} w_{v'} & \text{if} \quad v \in V_V, \\ \prod_{\langle v, v' \rangle \in E} w_{v'} & \text{if} \quad v \in V_A, \end{cases}$$

or in vectorial form, $\mathbf{w} = \mathbf{f}(\mathbf{w})$.

Obviously, this equation may have a lot of solutions. An interesting case, where we can characterize the solution defining W_V is when the set C is defined by a *parity condition* or *chained Rabin condition*. Let n be a positive natural number and $r : V \to \{1, \ldots, n\}$. With a play $p = v_0 v_1 \ldots \in V^\omega$, we associate the sequence $r(v_0), r(v_1), \ldots$ and we say that p is in C if and only if the least number that appears infinitely often in this sequence is even. In this case, we associate with each number i in $1, \ldots, n$ a family $\mathbf{w}_i$ of Boolean variables $w_{i,v}$ indexed by vertices in V. We also consider $\mathbf{f}(\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_n) : (\mathbb{B}^V)^n \to \mathbb{B}^V$ whose the component of index v is

$$\begin{cases} \sum_{\langle v, v' \rangle \in E} w_{r(v'), v'} & \text{if} \quad v \in V_V, \\ \prod_{\langle v, v' \rangle \in E} w_{r(v'), v'} & \text{if} \quad v \in V_A. \end{cases}$$

Remark that only some of the variables $w_{i,v}$ occur in $\mathbf{f}$.

Then one can show that W_V, seen as an element of $\mathbb{B}^V$, is exactly the following fixed point of $\mathbf{f}$:

$$\mu\,\mathbf{w}_1\,.\,\nu\,\mathbf{w}_2 ... \theta\mathbf{w}_n\,.\,\mathbf{f}\,(\mathbf{w}_1,\,\mathbf{w}_2,\,...,\,\mathbf{w}_{\tilde{n}}).$$

By the result above,

$$\begin{aligned}&\mu\,\mathbf{w}_1\,.\,\nu\,\mathbf{w}_2 ... \theta\,\mathbf{w}_n\,.\,\mathbf{f}\,(\mathbf{w}_1,\,\mathbf{w}_2,\,...,\,\mathbf{w}_n)\\ &\quad = \mu\,\mathbf{w}_1\,.\,\nu\,\mathbf{w}_2 ... \theta\,\mathbf{w}_n\,.\,\mathbf{g}\,(\mathbf{w}_1,\,\mathbf{w}_2,\,...,\,\mathbf{w}_n)\end{aligned}$$

where the component of index v of $\mathbf{g}$ is

$$\begin{cases} w_{r\,(v'),\,v'} & \text{for some } v' \text{ such that } \langle v,\,v'\rangle \in E, \text{ if } v \in V_V, \\ \displaystyle\prod_{\langle v,\,v'\rangle\in E} w_{r\,(v'),\,v'} & \text{if } v \in V_A. \end{cases}$$

That $\mathbf{g}$ defines a memoryless winning strategy for Val: When Val is in a position $v \in V_V$, she moves to the vertex v' such that the component of index v of $\mathbf{g}$ is $w_{r\,(v'),\,v'}$.

4.2. Modal μ-calculus

Let A be a finite alphabet and P a set of proportional symbols. A closed vectorial modal μ-term over A is an expression

$$\tau = \theta_1\,\mathbf{x}_1 ... \theta_n\,\mathbf{x}_n\,.\,\mathbf{f}\,(\mathbf{x}_1,\,...,\,\mathbf{x}_n),$$

where each $\mathbf{x}_i$ is a vector of variables of length k and $\mathbf{f}\,(\mathbf{x}_1,\,...,\,\mathbf{x}_n)$ is a vector of length k whose each component is a propositional symbol $p \in P$ or has one of the following form: $z \cup z'$, $z \cap z'$, $\langle a\rangle\,z$, $[a]\,z$, for any $a \in A$, where z and z' are variables belonging to some $\mathbf{x}_i$.

Let $\mathcal{S} = \langle S,\,T,\,P_S\rangle$ be a labeled transition system where S is a set of states, $T \subseteq S \times A \times S$ is a set of transitions, and P_S is a collection $\{p_S | p \in P\}$ of subsets of S. $\mathcal{S}$ is said to be *bounded-branching* if there exists a natural number d such that for any state $s \in S$ and any letter $a \in A$, there are at most d states s' such that $\langle s,\,a,\,s'\rangle \in T$.

The interpretation $[\tau]_{\mathcal{S}}$ of τ in $\mathcal{S}$ is defined as

$$\theta_1\,\mathbf{x}_1 ... \theta_n\,\mathbf{x}_n\,.\,[\mathbf{f}]_{\mathcal{S}}\,(\mathbf{x}_1,\,...,\,\mathbf{x}_n)$$

where $[\mathbf{f}]_{\mathcal{S}}$ is the monotonic maping from $(\mathcal{P}(S)^k)^n$ into $\mathcal{P}(S)^k$ obtained by replacing each component p by $p_{\mathcal{S}}$, $\langle a \rangle z$ by the mapping that associates with $Q \subseteq S$ the set $\{s \in S | \exists s' \in Q : \langle s, a, s' \rangle \in T\}$ and $[a] z$ by the mapping that associates with $Q \subseteq S$ the set $\{s \in S | \forall s' \in S, \langle s, a, s' \rangle \in T \Rightarrow s' \in Q\}$.

Thus, $[\tau]_{\mathcal{S}}$ belongs to $\mathcal{P}(S)^k$ and $\mathcal{S}$ is said to be a *model* of τ if the first component of $[\tau]_{\mathcal{S}}$ is not empty.

In [6], Streett and Emerson have proved that if a μ-term has a model then it has a bounded-branching model. We are going to prove this result as a consequence of the above theorem.

Because $\mathcal{P}(S)$ is obviously isomorphic to $\mathbb{B}^S$, there is a close connection between modal μ-calculus and Boolean μ-calculus that has been used to study and improve model-checking algorithms for the modal μ-calculus [3, 7, 1]. Let us explicit this connection.

Let τ and $\mathcal{S}$ be as above. For each vector $\mathbf{x}_i$ of k variables we consider the vector $\mathbf{y}_i$ indexed by $\{1, \ldots, k\} \times S$, *i.e.*, $\mathbf{y}_i$ is the set $\{y_{\langle z, s \rangle} | z \in \mathbf{x}_i, s \in S\}$. We associate with the vector $\mathbf{f}$ of length k, the vector $\mathbf{g}$ indexed by $\{1, \ldots, k\} \times S$ defined as follows, where f_i denotes the i-th component of $\mathbf{f}$: for any index i and any state s, the component $g_{\langle i, s \rangle}$ of index $\langle i, s \rangle$ of $\mathbf{g}$ is

if $f_i = p$ then $g_{\langle i, s \rangle} = \begin{cases} 1 & \text{if} \quad s \in p_{\mathcal{S}}, \\ 0 & \text{if} \quad s \notin p_{\mathcal{S}}, \end{cases}$

if $f_i = z \cup z'$ then $g_{\langle i, s \rangle} = y_{\langle z, s \rangle} + y_{\langle z', s \rangle}$,

if $f_i = z \cup z'$ then $g_{\langle i, s \rangle} = y_{\langle z, s \rangle}\, y_{\langle z', s \rangle}$,

if $f_i = \langle a \rangle z$ then $g_{\langle i, s \rangle} = \sum_{\langle s, a, s' \rangle \in T} y_{\langle z, s' \rangle}$,

if $f_i = [a] z$ then $g_{\langle i, s \rangle} = \prod_{\langle s, a, s' \rangle \in T} y_{\langle z, s' \rangle}$,

and it is easy to see that s belongs to the i-th component of $[\tau]_{\mathcal{S}}$ if and only if the component of index $\langle i, s \rangle$ of $\theta_1 \mathbf{y}_1 \ldots \theta_n \mathbf{y}_n \cdot \mathbf{g}(\mathbf{y}_1, \ldots, \mathbf{y}_n)$ is equal to 1.

By the above theorem,

$$\theta_1 \mathbf{y}_1 \ldots \theta_n \mathbf{y}_n \cdot \mathbf{g}(\mathbf{y}_1, \ldots, \mathbf{y}_n) = \theta_1 \mathbf{y}_1 \ldots \theta_n \mathbf{y}_n \cdot \mathbf{h}(\mathbf{y}_1, \ldots, \mathbf{y}_n),$$

where $\mathbf{h}$ is obtained by replacing every sum $\sum_{\langle s, a, s' \rangle \in T} y_{\langle z, s' \rangle}$ by some $y_{\langle z, s' \rangle}$.

Now, let us define the transition system $\mathcal{S}' = \langle S', T', P_{\mathcal{S}'} \rangle$ by $S' = S$, $P_{\mathcal{S}'} = P_{\mathcal{S}}$ and T' is the set of all $\langle s, a, s' \rangle$ such that $\sum_{\langle s, a, s' \rangle \in T} y_{\langle z, s' \rangle}$ has been replaced by $y_{\langle z, s' \rangle}$. Obviously $\mathcal{S}'$ is bounded-branching: the number of s' such that $\langle s, a, s' \rangle \in T'$ is at most equal to the number of components of

$\mathbf{f}$ in the form $\langle a \rangle\, z$. Now, let us consider the Boolean function $\mathbf{g}'$ associated with $\mathbf{f}$ and $\mathcal{S}'$, in the same way as $\mathbf{g}$ is associated with $\mathbf{f}$ and $\mathcal{S}$. It is clear that $\mathbf{h} \leq \mathbf{g}'$. Hence,

$$\theta_1\, \mathbf{y}_1 \cdots \theta_n\, \mathbf{y}_n \cdot \mathbf{g}\,(\mathbf{y}_1, \ldots, \mathbf{y}_n) = \theta_1\, \mathbf{y}_1 \cdots \theta_n\, \mathbf{y}_n \,.\, \mathbf{h}\,(\mathbf{y}_1, \ldots, \mathbf{y}_n) \leq \theta_1\, \mathbf{y}_1 \cdots \theta_n\, \mathbf{y}_n \cdot \mathbf{g}'\,(\mathbf{y}_1, \ldots, \mathbf{y}_n),$$

and $[\tau]_{\mathcal{S}} \subseteq [\tau']_{\mathcal{S}}$. It follows that if $\mathcal{S}$ is a model of τ, the bounded-branching transition system $\mathcal{S}'$ is also a model of τ.

4.3. The regularity theorem

The regularity theorem states that any tree language recognized by a tree automaton contains a regular tree.

If a tree automaton over an alphabet A is given with a parity condition, the set of trees it recognizes can be defined as the first component of some μ-term $\tau = \theta_1\, \mathbf{x}_1 \ldots \theta_n\, \mathbf{x}_n \,.\, \mathbf{f}$, where each component f_i of $\mathbf{f}$ has the form

$$\sum_{j \in J_i} a_{i,\,j}\,(z_{i,\,j},\, z'_{i,\,j});$$

this μ-term being interpreted in the powerset $\mathcal{P}\,(T_A)$, the powerset of all trees over A.

Let us consider one letter a in A and let us substitute a for any letter in τ. We get the μ-term $\tau' = \theta_1\, \mathbf{x}_1 \ldots \theta_n\, \mathbf{x}_n \,.\, \mathbf{f}'$, where each component f'_i of $\mathbf{f}$ has the form $\sum_{j \in J_i} a\,(z_{i,\,j},\, z'_{i,\,j})$.

It is clear that the i-th component of τ is not empty iff the i-th component of τ', interpreted in $\mathcal{P}\,(T_{\{a\}})$, is not empty. But $T_{\{a\}}$ has only one element, so that $\mathcal{P}\,(T_{\{a\}})$ can be identified with the Boolean algebra $\mathbb{B}$. The union becomes the Boolean sum, and since $a\,(Z,\, Z')$ is empty iff Z is empty or Z' is empty, the operation $a\,(z,\, z')$ can be identified with the Boolean product.

It follows that the Boolean μ-term $\tau'' = \theta_1\, \mathbf{x}_1 \ldots \theta_n\, \mathbf{x}_n \,.\, \mathbf{g}$, where each component g_i of $\mathbf{g}$ has the form $\sum_{j \in J_i} z_{i,\,j}\, z'_{i,\,j}$, has the same value as the characteristic function (for emptyness) of τ.

Applying the selection property, we get that τ'' has the same value as $\theta_1\, \mathbf{x}_1 \ldots \theta_n\, \mathbf{x}_n \,.\, \mathbf{g}'$, where each component g'_i of $\mathbf{g}'$ has the form $z_{i,\,j_i}\, z'_{i,\,j_i}$.

It follows that τ has the same characteristic function as $\theta_1\, \mathbf{x}_1 \ldots \theta_n\, \mathbf{x}_n \,.\, \mathbf{h}$, where each component h_i of $\mathbf{h}$ has the form $a_{i,\,j_i}\,(z_{i,\,j_i},\, z'_{i,\,j_i})$.

If the first component of τ is not empty, the first component of this last μ-terms defines a unique tree, that is regular and belongs to the first component of τ.

ACKNOWLEDGEMENTS

The result presented in this note as well as its proof came out from long and fruitful discussions with W. Zielonka and I. Walukiewicz about McNaughton's games on infinite graphs.

REFERENCES

1. H. R. ANDERSEN, Model checking and boolean graphs. *Theor. Comp. Sci.*, 1994, *126*, pp. 3-30.
2. A. ARNOLD, An initial semantics for the μ-calculus on trees and Rabin's complementation lemma. *Theor. Comp. Sci.*, 1995, *148*, pp. 121-132.
3. A. ARNOLD and P. CRUBILLÉ, A linear algorithm to solve fixed-point equations on transition systems. *Information Processing Letters*, 1988, *29*, pp. 57-66.
4. A. ARNOLD and D. NIWIŃSKI, Fixed point characterization of weak monadic logic definable sets of trees. In M. Nivat and A. Podelski, editors, *Tree Automata and Languages*, 1992, pp. 159-188, Elsevier.
5. R. McNAUGHTON, Infinite games played on finite graphs. *Annals of Pure and Applied Logic*, 1993, *65*, pp. 149-184.
6. R. S. STREETT and E. A. EMERSON, An automata theoretic decision procedure for the propositional mu-calculus. *Information and Computation*, 1989, *81*, pp. 249-264.
7. B. VERGAUWEN and J. LEWI, A linear algorithm for solving fixed-point equations on transition systems. In J.-C. Raoult, editor, *CAAP'92*, p. 321-341. *Lect. Notes Comput. Sci.*, 1992, *581*.
8. I. WALUKIEWICZ, Monadic second order logic on tree-like structures. In *STACS'96*, p. 401-414. *Lect. Notes Comput. Sci.*, 1996, *1046*.
9. W. ZIELONKA, Infinite games on finitely coloured graphs with applications to automata on infinite trees. Technical Report 1091-95, LaBRI, Université Bordeaux I, 1995.