Nondeduciblity on strategies in the temporal logic of knowledge

Cătălin Dima[1] and Constantin Enea[1,2]

[1] University Paris 12, 61 av. du Général de Gaulle, 94010 Créteil Cedex, France
[2] University "Al. I. Cuza", Str. General Berthlot 16, 740083, Iaşi, Romania

Abstract. We provide a syntactic characterization of Nondeducibility on Strategies in CTL* with knowledge and past time operators, based on prior work by Halpern and O'Neill. Our characterization is provided by means of a number of axioms that have to be satisfied by formulas specifying sets of strategies.

1 Introduction

Information flow is one of the main techniques that ensure confidentiality. There are several intuitions behind information flow, and they have been informally synthesized in statements about the (non-)dependence of high-level ("confidential") activity and low-level ("public") observation and/or deduction. Recently, Halpern and O'Neill [16] have investigated the possibility to relate some models of information flow with the semantic framework of Temporal Logics of Knowledge (TLK) [8]. They have shown that Generalized Noninterference (GNI) [14], Separability (Sep) [15], as well as Nondeducibility on Strategies [19] and its probabilistic form from [11], can be expressed by using a multiagent framework. Also syntactic forms for two of these information flow models were provided, stating that a system satisfies GNI or Sep iff $P_L\phi$ for some subclasses of formulas ϕ in TLK.

Our concern here is to provide a syntactic formulation of *Nondeducibility on Strategies* (NDS) of [19], which is a synchronous model of information flow that is weaker than Sep and stronger that GNI. NDS focuses on high-level strategies as means for High to interact with the system, and is inspired from previous work on computing covert channel capacity. One of the characteristics of the synchronous model of NDS is that High cannot refuse to interact with the system, as is the case with asynchronous, process-based models like BNDC [5].

Our approach is to give axiomatic and/or syntactic characterizations of *strategy formulas* for High in the original (unwinded) system $\mathcal{S}$ and then, similarly to [16], to define NDS syntactically as the validity in $\mathcal{S}$ of all the formulas of the type $P_L\phi$, for any strategy formula ϕ. Strategy formulas for High are basically formulas that specify "regular" families of *pure High strategies* – i.e. strategies for High to interact with the system, in which High makes his decisions by observing only his local state. They are specified as formulas in the full Computational Tree Logic with Knowledge and Past (KCTL*P) which have to satisfy axioms for (1) *locality* (i.e. the fact that High can only observe its local state and all his decisions are the same in different runs having the same local history) (2) *independence of the future* (i.e. the impossibility for High to guess the future behavior of the system) and (3) *totality* (i.e. the fact that local states represent inputs for High, whose only possibility to avoid being in a state is by choosing his *output actions*). We also give a subclass of formulas in the LTL with past fragment which satisfy these axioms and characterize NDS.

As already said, Halpern & O'Neill [16] have suggested to treat NDS as a particular case of their semantic framework, by including High strategies (called *protocols* in [16]) in the High local state and using an appropriate H-information function. However they do not give also a syntactic characterization for such H-information functions. Unfortunately, the semantic approach of [16] cannot be easily lifted at the syntactic level for several reasons: firstly, the trivial "solution" by providing one propositional symbol for each strategy – along the idea that anything that is "atomically" observable to an agent should represent an atomic syntactic item – cannot be a good choice, since it involves the creation of an uncountable set of propositional symbols. Secondly, putting the whole strategy in the local state at each time point i and therefore separating states that have a "common history" might also create problems when trying to construct formulas that specify "regular" sets of strategies. Our approach avoids these problems by keeping the original system unchanged, and focusing on the subclass of formulas that can be used to specify such "regular" sets of strategies.

On the other hand, Alternating Temporal Logic of [1] was not an option for specifying NDS for two reasons: firstly, NDS does not require an adversarial framework, as in ATL. In fact, between the three participants in the NDS framework (High, Low and the Environment), High and Low cooperate to produce information flow, but the Environment is not their adversary, but rather a "nondeterministic noise injector". As such, NDS is more of a worst case scenario[1], contrary to the approaches in [10, 2], in which Environment tries to avoid information flow. Secondly, to check NDS one has to specify the existence of *two* High-strategies that can be separated by Low-observations. This does not seem to be possible in ATL in the semantic framework of the initial system. It might be possible to specify it in a *modified* system, in which transitions are labeled with pairs of H-actions – but this hides the essence of our problem: to specify syntactically what NDS means for the initial system.

The rest of the paper is divided as follows: we recall the NDS model in the next section, and the syntax and semantics of KCTL*P in Section 3. Section 4 provides the axiomatic characterization of strategy formulas, and of Nondeducibility on Strategies in KCTL*P . We also give a syntactic characterization of a subclass of strategy formulas. We then show here that the classical formulation of NDS is equivalent with the KCTL*P formulation. We end with a section with conclusions and comments.

2 Nondeducibility on Strategies

Throughout the paper S^* denotes the set of finite sequences over a set S. The set of sequences over S of length m is denoted S^m while the set of sequences of length at most m is denoted $S^{\leq m}$. By ϵ we will understand the empty sequence and $S^+ = S^* - \{\epsilon\}$.

[1] In other words, stating NDS involves no quantifier alternation and checking it reduces to a reachability problem, see [4]

If $Tr = (Q, R, q_0)$ is a *transition system* where Q is the set of states, $R \subseteq Q \times Q$ is the transition relation and q_0 is the initial state, a *run of length* m in Tr is a sequence $\rho = \big(q_{i-1} \to q_i\big)_{1 \le i \le m}$ such that $R(q_{i-1}, q_i)$, for any $1 \le i \le m$, and q_0 is the initial state. We denote $\ell\mathsf{en}(\rho) = m$ the length of the run. A *run of infinite length* is then an infinite sequence of transitions $\rho = \big(q_{i-1} \to q_i\big)_{i \ge 1}$. We will also speak of ρ being an Tr*-run*. The set of runs for the transition system Tr is denoted $\mathsf{Runs}(Tr)$.

If $\rho = \big(q_{i-1} \to q_i\big)_{1 \le i \le m}$, then the *prefix of length* j *of* ρ, for some $1 \le j \le m$, is the run $\rho[1..j] = \big(q_{i-1} \to q_i\big)_{1 \le i \le j}$ (by an abuse of notation, we will consider that $\rho[1..0] = q_0$). We will also denote $\rho_1 \preceq \rho_2$ when ρ_1 is a prefix of length j of ρ_2, for some $0 \le j \le \ell\mathsf{en}(\rho)$. Moreover, we will use $\rho(j)$, for any $0 \le j \le \ell\mathsf{en}(\rho)$, to denote the jth state of ρ, q_j.

Definition 1. *A* **system for** n **agents** *is a tuple* $\mathcal{A} = \big((O_k \mid 1 \le k \le n), (I_k \mid 1 \le k \le n), R, (o_0^k \mid 1 \le k \le n), (i_0^k \mid 1 \le k \le n)\big)$ *where O_k is the set of outputs of the agent k, I_k is the set of inputs of the agent k, $o_0^k \in O_k$ is the initial output of agent k, $i_0^k \in O_k$ is the initial input of agent k, and $R \subseteq Q \times Q$ is the transition relation, where $Q = O_1 \times \cdots \times O_n \times I_1 \times \cdots \times I_n$ is the set of global states. We suppose that R is total, that is, for any $q \in Q$ there exists $q' \in Q$ such that $R(q, q')$.*

We assume that the global states of the system keep the current outputs received by each agent and the inputs they choose to continue the computation. We consider synchronous systems in which each agent must choose an input and the outputs are received in the same time.

In the following, for any state $q \in Q$, we will denote $q^k = q\big|_{O_k}$, for all $1 \le k \le n$ ($q\big|_{O_k}$ is the usual projection of the tuple q on O_k).

A system $\mathcal{A}$ is *total for k's inputs* or *k-total* if for any $q \in Q$ such that $R(q', q)$, for some $q' \in Q$, and for any $i \in I_k$, there exists $q'' \in Q$ such that $q''\big|_{O_k \times I_k} = (q\big|_{O_k}, i)$ and $R(q', q'')$. Hence, the k-totality is equivalent to the fact that agent k can anytime choose any input to continue the computation. This does not restrict the class of systems that can be verified, since any unwanted choice can be identified by its output.

The *k-projection* of an $\mathcal{A}$-run $\rho = \big(q_{i-1} \to q_i\big)_{1 \le i \le m}$, for any $1 \le k \le n$, is the run $\rho\big|_k = \big(q_{i-1}\big|_{O_k \times I_k} \to q_i\big|_{O_k \times I_k}\big)_{1 \le i \le m}$. This run is what agent k sees when ρ happens in the system $\mathcal{A}$. We will define also the *k-output projection* $\rho\big|_{O_k} = \big(q_{i-1}\big|_{O_k} \to q_i\big|_{O_k}\big)_{1 \le i \le m}$ and the *k-input projection* $\rho\big|_{I_k} = \big(q_{i-1}\big|_{I_k} \to q_i\big|_{I_k}\big)_{1 \le i \le m}$.

Definition 2. *A* **strategy** *for agent k, for any $1 \le k \le n$, is a mapping $s : (O_k)^* \to I_k$ such that $s(\epsilon) = i_0^k$. An m-***strategy** *for agent k is a mapping $s : (O_k)^{\le m} \to I_k$ such that $s(\epsilon) = i_0^k$.*

A strategy for agent k encodes the choices that this agent makes function of his observations of the system states. We assume that agent k does *not* have access to the whole system state when he makes his decisions. Note also that a strategy defines an input for k in any system state and provided any system history. By $s(\epsilon)$ we will understand the choice made by observing the initial output o_0^k which by definition is i_0^k. The set of strategies for agent k is denoted by Str_k.

If s_1 is an m_1-strategy for agent k and s_2 an m_2-strategy for agent k, with $m_1 \leq m_2$, we say that s_1 is a *prefix* of s_2 if $s_2(\lambda) = s_1(\lambda)$, for any sequence $\lambda \in (Q_X)^{\leq m_1}$.

Given s a strategy for k and $\rho = \big(q_{i-1} \to q_i\big)_{1 \leq i \leq m}$ a run, we say that s *is compatible with* ρ if

$$\forall 1 \leq i \leq m, s(q_1^k \dots q_i^k) = q_i\big|_{I_k}.$$

If s is a j-strategy for k and $\rho = \big(q_{i-1} \to q_i\big)_{1 \leq i \leq m}$, then we say that s *is compatible with* ρ if

$$\forall 1 \leq i \leq \min\{m, j\}, s(q_1^k \dots q_i^k) = q_i\big|_{I_k}.$$

In other words, s is compatible with ρ if $\rho\big|_k$ contains the sequence of "decisions" that agent k makes when acting like s, in accordance with the part of the current state that he may observe.

The set of strategies for agent k in the system $\mathcal{A}$ is denoted $\mathsf{Str}_k(\mathcal{A})$. Formally,

$$\mathsf{Str}_k(\mathcal{A}) = \{s \in \mathsf{Str}_k \mid \exists \rho \in \mathsf{Runs}(\mathcal{A}) \text{ such that } s \text{ is compatible with } \rho\}$$

The set of *behaviors observable by* i *when* j *acts following strategy* s is

$$\mathsf{Obs}_i(s) = \big\{\rho\big|_i \mid s \text{ is compatible with } \rho\big\}$$

Definition 3. *A system $\mathcal{A}$ satisfies **nondeducibility on strategies from i to j** (denoted $\mathsf{NDS}(i, j)$) if $\mathsf{Obs}_i(s_1) = \mathsf{Obs}_i(s_2)$, for any $s_1, s_2 \in \mathsf{Str}_j(\mathcal{A})$.*

If we consider a system with two agents, a high-level agent H and a low-level agent L, then $\mathsf{NDS}(L, H)$ is exactly the nondeduciblity on strategies from [19].

3 Temporal logic of knowledge

In the following, we will enhance the systems from the previous section with labeling functions that associate to each global state a set of atomic propositions.

Definition 4. *Let $AP = \bigcup_{1 \leq k \leq n} AP^k$ ($AP^i \cap AP^j = \emptyset$, for any $1 \leq i \neq j \leq n$) be a set of atomic propositions. A **Kripke structure for** n **agents** over AP is a couple $\mathcal{K} = (\mathcal{A}, L)$, where $\mathcal{A}$ is a system for n agents and $L : Q \to 2^{AP}$ is the labeling function.*

The semantics of a formula from the temporal logic of knowledge is given on interpreted systems which are defined as usual.

Definition 5. *Let $\mathcal{K}$ be a Kripke structure for n agents over some set of atomic propositions AP as above. The interpreted system corresponding to $\mathcal{K}$ is the couple $\mathcal{I}(\mathcal{K}) = (\mathsf{Runs}(\mathcal{K}), \pi)$, where $\pi : \mathsf{Runs}(\mathcal{K}) \times \mathbb{N} \to 2^{AP}$ is the interpretation function for the atomic propositions in $\mathcal{K}$ defined by $\pi((\rho, n)) = L(\rho(n))$, for any $\rho \in \mathsf{Runs}(\mathcal{K})$ and $n \in \mathbb{N}$.*

From now on, we will call a *point* any pair (ρ, n), where ρ is a run of $\mathcal{K}$ and $n \in \mathbb{N}$. We will denote by $\mathsf{Points}(\mathcal{I}(\mathcal{K}))$, the set of points of the interpreted system $\mathcal{I}(\mathcal{K})$.

On the set of points $\mathsf{Points}(\mathcal{I}(\mathcal{K}))$, we will define n equivalence relations $(\sim_k | 1 \leq k \leq n)$, such that $\sim_k$ relates states being "similar" to agent k. We will adopt a *synchronous perfect-recall semantics* of knowledge and consequently, we will consider that $(\rho, m) \sim_k (\rho', m')$ whenever $m = m'$ and $\rho[1..m]\big|_k = \rho'[1..m]\big|_k$.

In the following we will use CTL*P , which is CTL* combined with past time operators, as our supporting temporal logic. The set of formulas is defined as follows:

$$\phi = \psi \mid \neg\phi \mid \phi \wedge \phi \mid \bigcirc\phi \mid \Box\phi \mid \phi\mathcal{U}\phi \mid \bullet\phi \mid \blacksquare\phi \mid \phi\mathcal{S}\phi \mid \exists\phi,$$

where ψ is a *state formula*, that is, a propositional formula over AP.

We define the satisfaction relation $(\rho, m) \models \phi$, where $(\rho, m) \in \mathsf{Points}(\mathcal{I}(\mathcal{K}))$ and ϕ is a temporal logic formula as follows:

1. $(\rho, m) \models \psi$ iff ψ holds by interpreting the atomic propositions in $L(\rho, m)$ to true and the other ones to false;
2. $(\rho, m) \models \neg\phi$ iff $(\rho, m) \not\models \phi$;
3. $(\rho, m) \models \phi_1 \wedge \phi_2$ iff $(\rho, m) \models \phi_1$ and $(\rho, m) \models \phi_2$;
4. $(\rho, m) \models \bigcirc\phi_1$ iff $(\rho, m+1) \models \phi_1$;
5. $(\rho, m) \models \Box\phi_1$ iff $(\rho, m+j) \models \phi_1$, for all $j \geq 0$;
6. $(\rho, m) \models \phi_1\mathcal{U}\phi_2$ iff there exists $j \geq 0$ such that $(\rho, m+j) \models \phi_2$ and for every $0 \leq t < j$, $(\rho, m+t) \models \phi_1$;
7. $(\rho, m) \models \bullet\phi_1$ iff $m = 0$ or $m \geq 1 \wedge (\rho, m-1) \models \phi_1$;
8. $(\rho, m) \models \blacksquare\phi_1$ iff $(\rho, j) \models \phi_1$, for all $j \leq m$;
9. $(\rho, m) \models \phi_1\mathcal{S}\phi_2$ iff there exists $j \leq m$ such that $(\rho, j) \models \phi_2$ and for every $j < t \leq m$, $(\rho, t) \models \phi_1$;
10. $(\rho, m) \models \exists\phi_1$ iff there exists $\rho' \in \mathsf{Runs}(\mathcal{K})$ with $\rho'[1..m] = \rho[1..m]$ such that $(\rho', m) \models \phi_1$.

We define as syntactic sugar $\phi_1 \vee \phi_2 = \neg(\neg\phi_1 \wedge \neg\phi_2)$, $\Diamond\phi_1 = \neg\Box\neg\phi_1$, $\phi_1\mathcal{W}\phi_2 = \phi_1\mathcal{U}\phi_2 \vee \Box\phi_1$, $\blacklozenge\phi_1 = \neg\blacksquare\neg\phi_1$, $\phi_1\mathcal{B}\phi_2 = \phi_1\mathcal{S}\phi_2 \vee \blacksquare\phi_1$ and $\forall\phi_1 = \neg\exists\neg\phi_1$, for any temporal formulas ϕ_1 and ϕ_2. Also, we will define $\mathsf{false} = \phi \wedge \neg\phi$, $\mathsf{Init} = \bullet\mathsf{false}$ and $\mathsf{true} = \neg\mathsf{false}$.

If we add to the above temporal logic the knowledge operators K_i [9] for all $1 \leq i \leq n$, we obtain the temporal logic of knowledge, denoted by KCTL*P . The semantics of K_i is then the following:

11. $(\rho, m) \models K_i\phi_1$ iff for all $\rho' \in \mathsf{Runs}(\mathcal{K})$ with $(\rho', m) \sim_i (\rho, m)$ we have that $(\rho', m) \models \phi_1$.

We say that a formula ϕ of KCTL*P is *valid* in some interpreted system $\mathcal{I}(\mathcal{K})$ and denote this by $\mathcal{I}(\mathcal{K}) \models \phi$ if $(\rho, m) \models \phi$, for all $(\rho, m) \in \mathsf{Points}(\mathcal{K})$. Also, ϕ is called *satisfiable* in $\mathcal{I}(\mathcal{K})$ if there exists some point $(\rho, m) \in \mathsf{Points}(\mathcal{I}(\mathcal{K}))$ such that $(\rho, m) \models \phi$.

We will consider a special set of atomic propositions that identify the outputs and the inputs of each agent in each state. For simplicity we will denote them in the same way as the outputs $(O_k \mid 1 \leq k \leq n)$ and the inputs $(I_k \mid 1 \leq k \leq n)$. In the following, we will consider Kripke structures $\mathcal{K} = (\mathcal{A}, L)$ over some set of atomic propositions that includes $\bigcup_{1 \leq k \leq n}(O_k \cup I_k)$ and such that: $L((o^1, \dots, o^n, i^1, \dots i^n)) \cap (O_k \cup I_k) = \{o^k, i^k\}$, for any global state $(o^1, \dots, o^n, i^1, \dots i^n) \in Q$ and $1 \leq k \leq n$.

4 Nondeducibility on strategies in the temporal logic of knowledge

In this section we give a syntactic characterization of nondeducibility on strategies in the temporal logic of knowledge. In fact, we give a syntactic characterization for the formulas that specify families of strategies for an agent j to interact with the system and, then specify $\mathsf{NDS}(i, j)$ as the validity of $P_i\phi$, for any such formula ϕ. In the first subsection we give an axiomatic definition for these formulas and in the next subsection we give a subclass of formulas in the LTL with past that completely define NDS.

4.1 A necessary condition for NDS

A CTL*P formula ϕ is *limit closed* if, whenever there exists an infinite sequence of runs $(\rho_i)_{i\geq 0}$ such that $(\rho_i, 0) \models \phi$ and $\rho_i[1..i] = \rho_{i+1}[1..i]$, then there exists a run ρ with $\rho[1..i] = \rho_i[1..i]$ and such that $(\rho, 0) \models \phi$. In other words, the set of models of ϕ at 0 is a *closed set* in the usual topology of infinite sequences; or, even more, that ϕ is a *safety formula*.

Definition 6. *Let $\mathcal{K}$ be a Kripke structure for n agents and $\mathcal{I}(\mathcal{K})$ its corresponding interpreted system. A CTL*P formula ϕ* ***depends only on the past of agent*** *j if the following axioms hold for ϕ:*

$$\mathcal{I}(\mathcal{K}) \models \phi \to \blacksquare\Box\phi, \tag{1}$$

$$\mathcal{I}(\mathcal{K}) \models \phi \to K_j\exists\phi. \tag{2}$$

The first property (call it *extensibility*), says that once ϕ holds at a certain point on a run, then it holds throughout the whole run. Note that this implies that ϕ is limit closed.

The second property states that the choice of the truth value for ϕ at two j-similar points (ρ, m) and (ρ', m) does not depend on the set of possible continuations of ρ respectively ρ' after position m.

Example 1. Let $\mathcal{K} = (\mathcal{A}, L)$ be a Kripke structure for 2 agents over some set of atomic propositions AP, for which a fragment is depicted in Figure 1 (the two agents will be denoted H and L, respectively). We consider that:

- $O_H = \{o_0, o_1, o_2, o_3\}$, $I_H = \{i_1, i_2\}$, $O_L = \{r_0, r_1, r_2, r_3, r_4\}$ and $I_L = \{l\}$;
- the initial outputs for H and L are o_0 and r_0, respectively and the initial inputs for H and L are i_1 and l, respectively;
- $\mathcal{K}$ is total for H's inputs;

The formula $\phi_1 = \blacksquare\Box\CIRCLE(o_1 \to (i_1 \wedge \CIRCLE(o_0 \to i_1)))$ is an example of a formula that depends only on the past of H. This happens because its satisfaction in some point of $\mathcal{I}(\mathcal{K})$, (ρ, m), takes place only because of the atomic propositions from AP^H that hold in the states preceding (ρ, m).

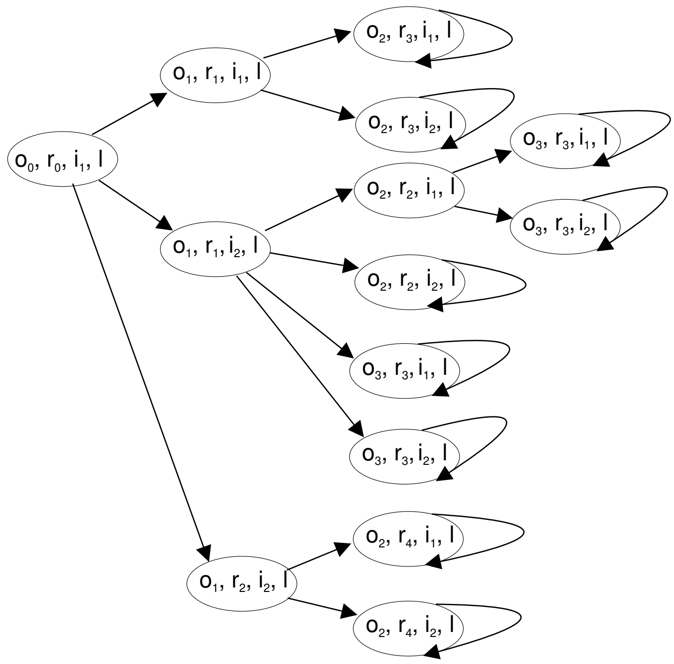

Fig. 1. An input-output Kripke structure for 2 agents

Another example of formula that depends only on the past of H is

$$\phi_2 = \blacksquare\square\big(o_0 \rightarrow (i_1 \wedge \bigcirc(o_1 \rightarrow (i_2 \wedge \bigcirc(o_2 \rightarrow i_2))))\big).$$

In this case, the dependability on the past of H is implied by the totality of $\mathcal{K}$ for H's inputs.

A formula that does not depend only on the past of H is $\phi_3 = \blacksquare\square\Diamond o_3$. Take two runs $\rho_1 = (o_0, r_0, i_1, l) \rightarrow (o_1, r_1, i_2, l) \rightarrow (o_2, r_2, i_1, l) \rightarrow (o_3, r_3, i_1, l) \rightarrow (o_3, r_3, i_1, l) \rightarrow \ldots$ and $\rho_2 = (o_0, r_0, i_1, l) \rightarrow (o_1, r_2, i_2, l) \rightarrow (o_2, r_4, i_1, l) \rightarrow (o_2, r_4, i_1, l) \rightarrow \ldots$. We have that $(\rho_1, 1) \models \phi_3$, $(\rho_1, 1) \sim_H (\rho_2, 1)$ but $\rho_2[0..1]$ can not be extended to an infinite run satisfying ϕ_3.

Definition 7. *Let $\mathcal{K}$ be a Kripke structure for n agents and $\mathcal{I}(\mathcal{K})$ its corresponding interpreted system. A CTL*P formula ϕ is j-**admissible** if it is satisfiable, it depends only on the past of agent j and satisfies the following axiom:*

$$\mathcal{I}(\mathcal{K}) \models (\phi \wedge \exists \bigcirc \pi) \rightarrow \exists \bigcirc (\phi \wedge \pi), \tag{3}$$

for any propositional formula π over O_j.

A j-admissible formula describes a strategy for agent j, that is, a decision to issue an action (identified as a propositional formula over I_j) at some moment after passing through some sequence of states that ends in a state identified by a propositional formula over O_j.

Example 2. Let $\mathcal{K}$ be the Kripke structure for 2 agents from Example 1. An example of an H-admissible formula is $\phi_4 = \blacksquare\square(o_0 \to i_1) \wedge (o_1 \to i_2) \wedge (o_2 \to i_1)$.

Notice that we can associate to ϕ_4 a set of strategies for H, s, such that $s(\xi o_0) = i_1$, $s(\xi o_1) = i_2$ and $s(\xi o_2) = i_1$, for any $\xi \in (O_H)^*$.

An example of a formula that depends only on the past of H but is not H-admissible is $\phi_5 = \blacksquare\square(o_3 \to \blacklozenge o_2)$. To prove this take ρ_1 a run as follows:

$$(o_0, r_0, i_1, l) \to (o_1, r_1, i_2, l) \to (o_2, r_2, i_1, l) \to (o_3, r_3, i_1, l) \to (o_3, r_3, i_1, l) \to \dots$$

Then $(\rho_1, 1) \models \phi_5 \wedge \exists \bigcirc o_3$ but there exist no run ρ with $\rho[0..1] = \rho_1[0..1]$ such that $(\rho, 2) \models \phi_5 \wedge o_3$.

Proposition 1. *Let $\mathcal{K}$ be a Kripke structure for n agents total for j's inputs, $\mathcal{I}(\mathcal{K})$ its corresponding interpreted system and ϕ a j-admissible formula, for some $1 \le j \le n$. Then ϕ satisfies the following j-**strategy admissibility** property:*

> *For any run ρ in $\mathcal{K}$ for which $(\rho, 0) \models \phi$, there exists a strategy for j, σ which is compatible with ρ and such that for any other run ρ' in $\mathcal{K}$ with which σ is compatible, $(\rho', 0) \models \phi$.*

The reverse implication also holds, in the following sense: if ϕ is a CTL*P formula which depends only on the past of agent j and satisfies j-strategy admissibility, then ϕ is also a j-admissible formula.

Proof. Suppose first that ϕ is a j-admissible formula and ρ a run in $\mathcal{K}$ for which $(\rho, 0) \models \phi$. This implies, by extensibility, that $(\rho, i) \models \phi$ for all $i \ge 0$. We will construct a strategy σ as required, by recursively defining all its k-length prefixes σ_k.

In fact, we will define the sequence of strategies $(\sigma_k | k \ge 0)$ such that σ_k is a k-strategy, σ_k is a prefix of σ_{k+1} and σ_k satisfies the following:

> (*) σ_k is compatible with ρ and for any other run ρ' of length k with which $\sigma_k$is compatible, there exists an infinite run ρ'_1 compatible with σ_k with $\rho'_1[1..k] = \rho'$ and such that $(\rho'_1, 0) \models \phi$.

The first strategy in the sequence, σ_0, is the only strategy of length 0 that exists. Clearly, σ_0 is compatible with ρ. Now, for any run ρ' of length 0 such that σ_0 is compatible with ρ', there exists $\rho'_1 = \rho$ such that $\rho'_1[1..0] = \rho'[1..0]$ and $(\rho'_1, 0) \models \phi$.

Then, for any $k \ge 1$, suppose we have built the strategy σ_{k-1}. In the following, we will construct σ_k with the property above. Since σ_{k-1} is a prefix of σ_k, we have to define choices only for sequences of outputs of length k.

Suppose we have some sequence of outputs from O_j of length $k+1$, $\lambda = o_0 \dots o_k$, with o_0 being the initial output of agent j. If there exists no infinite run ρ' in $\mathcal{K}$ such that $\rho'[1..k]\big\lfloor_{O_j} = \lambda$, then we choose randomly a value for $\sigma_k(o_1 \dots o_k)$.

Otherwise, if for all sequences of length k from I_j, $\lambda' = i_0 \dots i_{k-1}$, with i_0 being the initial input of agent j, there exists $1 \le p \le k-1$ such that $i_p \ne \sigma_k(o_1 \dots o_p)$ then we also choose randomly a value for $\sigma_k(o_1 \dots o_k)$.

If even the latter does not happen, let $\lambda' = i_0 \dots i_{k-1}$ be the sequence of inputs from I_j such that $i_p = \sigma_k(o_1 \dots o_p)$, for all $1 \le p \le k-1$ (this sequence is unique because σ_k is a function). By the totality of $\mathcal{K}$ for j's inputs, there exists some run $\rho_{\lambda,\lambda'} \in \mathsf{Runs}(\mathcal{K})$ such that $\{o_p, i_p\} \subseteq L(\rho_{\lambda,\lambda'}(p))$, for all $0 \leq p \leq k-1$, and $o_k \in L(\rho_{\lambda,\lambda'}(k))$. If also, $\{o_p, i_p\} \subseteq L(\rho(p))$, for all $0 \leq p \leq k-1$, and $o_k \in L(\rho(k))$, we take $\rho_{\lambda,\lambda'} = \rho$.

From the conditions on the sequence λ', we have that σ_{k-1} is compatible with the run $\rho_{\lambda,\lambda'}[1..k-1]$ and consequently, there exists an infinite run $\rho'_{\lambda,\lambda'}$ with $\rho'_{\lambda,\lambda'}[1..k-1] = \rho_{\lambda,\lambda'}[1..k-1]$ such that $(\rho'_{\lambda,\lambda'}, 0) \models \phi$. If $\rho_{\lambda,\lambda'} = \rho$ then we choose $\rho'_{\lambda,\lambda'} = \rho$ which obviously, satisfies all the needed requirements.

Hence, $(\rho'_{\lambda,\lambda'}, k-1) \models \phi \wedge \exists \bigcirc o_k$ which by j-admissibility implies $(\rho'_{\lambda,\lambda'}, k-1) \models \exists \bigcirc (\phi \wedge o_k)$. The latter means that there exists an infinite run $\rho_{\lambda,\lambda',o_k}$ such that $\rho_{\lambda,\lambda',o_k}[1..k-1] = \rho'_{\lambda,\lambda'}[1..k-1] = \rho_{\lambda,\lambda'}[1..k-1]$, $o_k \in L(\rho_{\lambda,\lambda',o_k}(k))$ and $(\rho_{\lambda,\lambda',o_k}, k) \models \phi$. Again, if $\rho_{\lambda,\lambda'} = \rho'_{\lambda,\lambda'} = \rho$ then, we choose $\rho_{\lambda,\lambda',o_k} = \rho$. We will define $\sigma_k(o_1 \dots o_k) = i_k$, where $i_k \in L(\rho_{\lambda,\lambda',o_k}(k))$.

Now, we will prove that σ_k satisfies property (*). Take any run ρ' of length k compatible with σ_k. If we take $\lambda = \rho'[1..k-1]\big|_{O_j}$ and $\lambda' = \rho'[1..k-1]\big|_{I_j}$ and suppose that $o_k \in L(\rho'(k))$ then, $(\rho', k) \sim_j (\rho_{\lambda,\lambda',o_k}, k)$, where $\rho_{\lambda,\lambda',o_k}$ is the run used in the construction of σ_k.

The fact that $(\rho_{\lambda,\lambda',o_k}, k) \models \phi$ implies, by property 2, that $(\rho_{\lambda,\lambda',o_k}, k) \models K_j \exists \phi$. Hence, there exists ρ'_1 compatible with σ_k with $\rho'_1[1..k] = \rho'$ such that $(\rho'_1, k) \models \phi$ which implies, by property 1, that $(\rho'_1, 0) \models \phi$.

All that is left for proving is that the strategy σ defined by $\sigma(\lambda) = \sigma_{|\lambda|}(\lambda)$, for all $\lambda \in O_j^*$ ($|\lambda|$ denotes the length of the sequence λ) satisfies the j-strategy admissibility property. But this is an easy corollary of the fact that ϕ is invariant: suppose that ρ_3 (infinite run) is compatible with σ – therefore, for each k, $\rho_3[1..k]$ is also compatible with σ_k. By property (*), there exists an infinite run ρ_3^k with $\rho_3^k[1..k] = \rho_3[1..k]$ with $(\rho_3^k, 0) \models \phi$. Limit closure for ϕ implies then that for ρ_3, which is the unique run with $\rho_3[1..k] = \rho_3^k[1..k]$, we have that $(\rho_3, 0) \models \phi$. The fact that σ is compatible with ρ can be easily deduced from the construction above.

For the reverse proof, note first that it suffices to prove the j-admissibility property only for propositional formulas of the form $\pi = o$ where $o \in O_j$. To this end, suppose that, for some $o \in O_j$, $(\rho, k) \models \phi$ and there exists ρ' with $\rho'[1..k] = \rho[1..k]$ and $(\rho', k+1) \models o$.

Note first that Property 1 implies that $(\rho, 0) \models \phi$. This implies the existence of a strategy for j, σ, compatible with ρ with the extra properties forming j-strategy admissibility.

Consider that $L(\rho'(p)) \cap O_j = \{o_p\}$, $L(\rho'(p)) \cap I_j = \{i_p\}$, for any $p \geq 0$ and $o = o_{k+1}$. Denote $i = \sigma(o_1 \dots o_{k+1})$. By the totality for j's inputs there exists an infinite run ρ'' such that $\rho''[1..k] = \rho'[1..k] = \rho[1..k]$, $\{o, i\} \subseteq L(\rho''(k+1))$ and σ is compatible with ρ''. By strategy admissibility, we have that $(\rho'', 0) \models \phi$ which implies $(\rho'', k+1) \models \phi$. Since we also have that $(\rho'', k+1) \models o$, Property 3 for ϕ is proved. □

Definition 8. *Let $\mathcal{K}$ be a Kripke structure for n agents, $\mathcal{I}(\mathcal{K})$ its corresponding interpreted system and i, j two agents ($i \neq j$). We say that **agent i cannot deduce j-strategies in** $\mathcal{I}(\mathcal{K})$ (denoted $\mathsf{ANS}(i,j)$) if for any j-admissible formula ϕ we have that:*

$$\mathcal{I}(\mathcal{K}) \models P_i \phi.$$

Theorem 1. *Let $\mathcal{K} = (\mathcal{A}, L)$ be a Kripke structure for n agents and $\mathcal{I}(\mathcal{K})$ its corresponding interpreted system. If $\mathcal{A}$ satisfies $\mathsf{NDS}(i,j)$, for some $1 \leq i \neq j \leq n$ and it is total for j's inputs, then $\mathcal{I}(\mathcal{K})$ satisfies $\mathsf{ANS}(i,j)$.*

Proof. By means of Proposition 1, we will actually prove that, if there exists a formula ϕ which depends only on the past of j and satisfies j-strategy admissibility but for which $\mathcal{I}(\mathcal{K}) \not\models P_i\phi$, then $\mathcal{A}$ cannot satisfy $\mathsf{NDS}(i,j)$.

Since ϕ is satisfiable there exists some point $(\rho, m) \in \mathsf{Points}(\mathcal{I}(\mathcal{K}))$ such that $(\rho, m) \models \phi$. By the extensibility property, we have that $(\rho, 0) \models \phi$ and consequently, by the j-strategy admissibility, there exists a strategy for j, σ, which is compatible with ρ and satisfies: for any other run ρ' in $\mathcal{K}$ such that σ is compatible with ρ', $(\rho', 0) \models \phi$.

Now, suppose that there exists a point (ρ', m') with $(\rho', m') \not\models P_i\phi$. This implies that for any infinite run ρ'' with $(\rho'', m') \sim_i (\rho', m')$ we have that $(\rho'', m') \not\models \phi$. The latter implies that σ is not compatible with ρ''. Moreover, let σ' be one of the strategies for j compatible with ρ'.

The above results say that $\rho'[1..m']\Big|_i \xi \notin \mathsf{Obs}_i(\sigma)$, for any $\xi \in (O_i \times I_i)^*$, and $\rho'\Big|_i \in \mathsf{Obs}_i(\sigma')$, which imply that $\mathcal{A}$ does not satisfy $\mathsf{NDS}(i,j)$. $\square$

4.2 Characterizing NDS using strategy formulas

In the following, we will define the set of strategy formulas which will be used to give a characterization of nondeducibility of strategies in the temporal logic of knowledge.

Let $\mathcal{K} = (\mathcal{A}, L)$ be a Kripke structure for n agents and $\mathcal{I}(\mathcal{K})$ its corresponding interpreted system. We define the set of *strategy formulas for agent k* as follows:

$$\phi = o \to i \mid o \to (i \wedge \bigcirc\phi) \mid \phi \wedge \phi \mid \phi \vee \phi \mid \bigcirc\phi \mid \Box\phi \mid \phi\mathcal{W}o,$$

where $o \in O_k$ and $i \in I_k$. We will denote by $\mathsf{FStr}_k(\mathcal{I}(\mathcal{K}))$ the set of strategy formulas for agent k in $\mathcal{I}(\mathcal{K})$.

Strategy formulas are meant to describe strategies. For instance, in the interpreted system $\mathcal{I}(\mathcal{K})$ from Example 1, the formula $\phi = o_0 \to (i_1 \wedge \bigcirc(o_1 \to (i_2 \wedge \bigcirc(o_2 \to i_1))))$ describes the set of strategies for H, s, with $s(o_1) = i_2$ and $s(o_1o_2) = i_1$.

However, there are satisfiable strategy formulas that express more than a strategy. For example, the formula $o \to i \wedge o \to i'$ is true in all the points (ρ, m) for which $o \notin L((\rho, m))$ and hence, it does not characterize strategies. It says that agent k should not receive o as output. In the following, we will identify the subclass of strategy formulas that do not contain such formulas and express only things about the strategy of agent k.

In order to do that, we will define two functions $\delta^k : (O_k)^+ \times \mathsf{FStr}_k(\mathcal{I}(\mathcal{K})) \to \mathcal{FP}(I_k)$ and $\xi^k : (O_k)^+ \times \mathsf{FStr}_k(\mathcal{I}(\mathcal{K})) \to \mathsf{FStr}_k(\mathcal{I}(\mathcal{K}))$, where $\mathcal{FP}(I_k)$ represents the set of propositional formulas over I_k (the first argument will be represented as an index). Intuitively, $\delta^k_\pi(\phi)$, for some $\pi \in (O_k)^+$, represents the propositional formula that must hold in the state reached after passing through the local states of agent k from π. The formula that must hold in the path that follows the state reached by passing through the local states from π is given by $\xi^k_\pi(\phi)$. These functions are inspired from the derivatives of regular expressions [3] and are defined as follows:

- $\delta^k_o(\mathsf{true}) = \mathsf{true}$ and $\delta^k_o(\mathsf{false}) = \mathsf{false}$;

- $\delta^k_o(o \rightarrow i) = i$ and $\delta^k_{o'}(o \rightarrow i) = \mathsf{true}$, for any $o' \neq o$;
- $\delta^k_o(o \rightarrow (i \wedge \bigcirc\phi)) = i$ and $\delta^k_{o'}(o \rightarrow (i \wedge \bigcirc\phi)) = \mathsf{true}$, for any $o' \neq o$;
- $\delta^k_o(\phi_1 \wedge \phi_2) = \delta^k_o(\phi_1) \wedge \delta^k_o(\phi_2)$ and $\delta^k_o(\phi_1 \vee \phi_2) = \delta^k_o(\phi_1) \vee \delta^k_o(\phi_2)$;
- $\delta^k_o(\bigcirc\phi) = \mathsf{true}$;
- $\delta^k_o(\Box\phi) = \delta^k_o(\phi)$;
- $\delta^k_{o'}(\phi\mathcal{W}o) = \delta^k_{o'}(\phi)$, for any $o' \neq o$ and $\delta^k_o(\phi\mathcal{W}o) = \mathsf{true}$;
- $\xi^k_o(\mathsf{true}) = \mathsf{true}$ and $\xi^k_o(\mathsf{false}) = \mathsf{false}$;
- $\xi^k_o(o' \rightarrow i) = \mathsf{true}$, for any $o, o' \in O_k$;
- $\xi^k_o(o \rightarrow (i \wedge \bigcirc\phi)) = \phi$ and $\xi^k_{o'}(o \rightarrow (i \wedge \phi)) = \mathsf{true}$, for any $o' \neq o$;
- $\xi^k_o(\phi_1 \wedge \phi_2) = \xi^k_o(\phi_1) \wedge \xi^k_o(\phi_2)$ and $\xi^k_o(\phi_1 \vee \phi_2) = \xi^k_o(\phi_1) \vee \xi^k_o(\phi_2)$;
- $\xi^k_o(\bigcirc\phi) = \phi$;
- $\xi^k_o(\Box\phi) = \Box\phi \wedge \xi^k_o(\phi)$;
- $\xi^k_{o'}(\phi\mathcal{W}o) = \phi\mathcal{W}o \wedge \xi^k_{o'}(\phi)$, for any $o' \neq o$ and $\xi^k_o(\phi\mathcal{W}o) = \mathsf{true}$;
- $\delta^k_{\pi o}(\phi) = \delta^k_o(\xi^k_\pi(\phi))$, for all $\pi \in (O_k)^+$;
- $\xi^k_{\pi o}(\phi) = \xi^k_o(\xi^k_\pi(\phi))$, for all $\pi \in (O_k)^+$.

The intuition behind the two functions above is proved in the following result.

Proposition 2. *Let $\mathcal{K} = (\mathcal{A}, L)$ be a Kripke structure for n agents, $\mathcal{I}(\mathcal{K})$ its corresponding interpreted system and ϕ a strategy formula for agent k. Then, for all $m \geq 0$:*

$$(\rho, m) \models \phi \Leftrightarrow \forall j \geq 0 : (\rho, m+j) \models \delta^k_{o_m \cdots o_{m+j}}(\phi),$$

where $o_p \in L(\rho, p) \cap O_k$, for all $p \geq 0$.

Definition 9. *Let $\mathcal{K} = (\mathcal{A}, L)$ be a Kripke structure for n agents, $\mathcal{I}(\mathcal{K})$ its corresponding interpreted system and ϕ a strategy formula for agent k. The formula ϕ is called* **admissible** *if for any $\pi \in (O_k)^+$, $\delta^k_\pi(\phi)$ is satisfiable.*

A few words on admissible strategy formulas are in order. If $\delta^k_\pi(\phi)$ is not satisfiable for some $\pi \in (O_k)^+$, then the formula ϕ just forbids the sequence of outputs π and does not offer any information about some strategy. This is why we will avoid this kind of formulas. For admissible formulas, we can prove that for any strategy for agent k, s, and any $m \in \mathbb{N}$ there exists some admissible strategy formula $\phi_{m,s}$ that describes the choices defined by s on sequences of outputs of length at most $m+1$ (the first output is the initial output which is represented by the empty sequence when defining strategies).

Proposition 3. *Let $\mathcal{K} = (\mathcal{A}, L)$ be a Kripke structure for n agents, $\mathcal{I}(\mathcal{K})$ its corresponding interpreted system and s a strategy for agent k. Then, for any $m \in \mathbb{N}$, there exists an admissible strategy formula $\phi_{m,s}$ for agent k, such that:*

$$\forall \rho \in \mathsf{Runs}(\mathcal{K}) : s \textit{ is compatible with } \rho[1..m] \Leftrightarrow (\rho, 0) \models \phi_{m,s}.$$

Proof. We define $\phi_{m,s} = \bigwedge_{\pi \in (O_k)^m} \phi_{m,s,\pi}$, where $\phi_{m,s,\pi}$ describes the choices implied by s on the sequence $o^k_0\pi$. Let $\pi = o_1 \ldots o_m$ and $i_j = s(o_1 \ldots o_j)$, for all $1 \leq j \leq m$. We will define $\phi_{m,s,\pi}$ as follows:

$$o^k_0 \rightarrow (i^k_0 \wedge \bigcirc(o_1 \rightarrow (i_1 \wedge \ldots (i_{m-1} \wedge \bigcirc(o_m \rightarrow i_m)) \ldots).$$

We can easily prove that $\phi_{m,s}$ is the admissible strategy formula needed in the claim of the theorem. $\Box$

Now, we can characterize the nondeducibility of strategies in the temporal logic of knowledge.

Theorem 2. *Let $\mathcal{K} = (\mathcal{A}, L)$ be a Kripke structure for n agents total for j's inputs, for some $1 \leq j \leq n$, and $\mathcal{I}(\mathcal{K})$ its corresponding interpreted system. $\mathcal{A}$ satisfies $\mathsf{NDS}(i, j)$, for some $1 \leq i \neq j \leq n$, iff for any admissible strategy formula ϕ:*

$$\mathcal{I}(\mathcal{K}) \models P_i \blacksquare\Box(\mathsf{Init} \rightarrow \phi).$$

Proof. ($\Rightarrow$) We will prove that all the formulas of the form $\blacksquare\Box(\mathsf{Init} \rightarrow \phi)$ with ϕ an admissible strategy formula are j-admissible formulas. To prove that axiom 2 from Definition 6 holds, let $(\rho, m), (\rho', m) \in \mathsf{Points}(\mathcal{I}(\mathcal{K}))$ such that $\mathcal{I}(\mathcal{K}) \models \blacksquare\Box(\mathsf{Init} \rightarrow \phi)$ and $(\rho, m) \sim_j (\rho', m)$. We will construct a sequence of runs from $\mathcal{K}$, $(\rho_k \mid k \geq 0)$ such that $\rho_0 = \rho'$, $\rho_{k+1}[1..m+k] = \rho_k[1..m+k]$ and $(\rho_k, p) \models \delta^j_{\pi^k_p}(\phi)$, for any $0 \leq p \leq m+k$, where $\pi^k_p = \rho_k[1..p]\big|_{O_j}$. Suppose we have build ρ_k, for some $k \geq 0$. If $(\rho_k, m+k+1) \models \delta^j_{\pi^k_{m+k+1}}(\phi)$, then we take $\rho_{k+1} = \rho_k$. Otherwise, by the j-totality of $\mathcal{K}$, there exists ρ_{k+1} such that $\rho_{k+1}[1..m+k] = \rho_k[1..m+k]$, $\rho_{k+1}(m+k+1)\big|_{O_j} = \rho_k(m+k+1)\big|_{O_j}$ and $\rho_{k+1}(m+k+1)\big|_{I_j}$ is one of the inputs for agent j that appears in the disjunction equivalent to $\delta^j_{\pi^k_{m+k+1}}(\phi)$.

Having build the sequence above we obtain that there exists $\rho'' \in \mathsf{Runs}(\mathcal{K})$ such that $\rho''[1..m] = \rho'[1..m]$ and $\rho''(m+k) = \rho_k(m+k)$, for any $k \geq 1$. Moreover, we have that $(\rho'', p) \models \delta^j_{\pi_p}(\phi)$, for any $p \geq 0$, where $\pi_p = \rho''[1..p]\big|_{O_j}$. The latter implies, by Property 2, that $(\rho'', 0) \models \phi$ which terminates our proof for the validity of the axiom 2 from Definition 6.

A similar procedure can be applied to prove that the axiom 3 from Definition 7 holds. Consequently, we can apply Theorem 1 and obtain the needed result.

($\Leftarrow$) Suppose by contradiction that $\mathcal{I}_{\mathcal{K}}$ has the property above and $\mathcal{A}$ does not satisfy $\mathsf{NDS}(i, j)$. Consequently, there exist two strategies $s_1, s_2 \in \mathsf{Str}_j(\mathcal{A})$ such that $\mathsf{Obs}_i(s_1) \neq \mathsf{Obs}_i(s_2)$ which implies that there exists a finite run $\rho \in \mathsf{Runs}(\mathcal{K})$ of length m, for some $m \in \mathbb{N}$, such that s_1 is compatible with ρ but for any other run $\rho' \in \mathsf{Runs}(\mathcal{K})$ with $\rho'[1..m]\big|_i = \rho\big|_i$, s_2 is not compatible with ρ'.

By Proposition 3, for s_2 and m, we can find an admissible strategy formula ϕ_{m,s_2} such that for any $\rho_1 \in \mathsf{Runs}(\mathcal{K})$, s_2 is compatible with $\rho_1[1..m]$ iff $(\rho_1, 0) \models \phi_{m,s_2}$.

Consequently, we have that $(\rho', m) \not\models P_i \blacksquare\Box(\mathsf{Init} \rightarrow \phi_{m,s_2})$, which contradicts the hypothesis. $\Box$

5 Conclusions

We have investigated here the possibility to define syntactically Wittbold & Johnson's notion of Nondeducibility on Strategies. We have identified a subclass of KCTL*P formulas which can be used to specify families of strategies in a system, and provided a formulation of NDS in KCTL*P , similar to [16].

An interesting question is whether the *dependence on the past* axiom 2 can be expressed without the knowledge operator. A negative answer would also suggest that knowledge operators strictly increase the expressivity of CTL* (with past).

References

1. R. Alur, T. Henzinger, and O. Kupferman. Alternating-time temporal logic. *J. ACM*, 49(5):672–713, 2002.
2. D. Beauquier and R. Lanotte. Hiding information in multi level systems. In *Proceedings of FAST 2006*, LNCS, 2006. to appear.
3. Janusz A. Brzozowski. Derivatives of regular expressions. *Journal of the ACM*, 11(4):481–494, 1964.
4. C. Dima, C. Enea, and R. Gramatovici. A synchronous model for information flow. Technical report, LACL, Université Paris 12, 2006. Available at `http://www.univ-paris12.fr/lacl/Rapports/publications/TR-2006-02.pdf`.
5. R. Focardi and R. Gorrieri. A taxonomy of security properties for process algebras. *Journal of Computer Security*, 3(1):5–34, 1995.
6. R. Focardi and R. Gorrieri. Classification of security properties (part i: Information flow). In *FOSAD*, pages 331–396, 2000.
7. J.A. Goguen and J. Meseguer. Security policies and security models. In *Proceedings of the IEEE Symposium on Security and Privacy*, pages 11–20, Oakland, CA, USA, 1982.
8. J. Halpern. *Reasoning about knowledge*. MIT Press, 2003.
9. Joseph Y. Halpern, Ronald Fagin, Yoram Moses, and Moshe Y. Vardi. *Reasoning About Knowledge*. MIT Press, 2003.
10. L. Hélouët, M. Zeitoun, and A. Degorre. Scenarios and covert channels: Another game... *Electr. Notes Theor. Comput. Sci.*, 119(1):93–116, 2005.
11. J. W. Gray III and P. Syverson. A logical approach to multilevel security of probabilistic systems. *Distributed Computing*, 11(2):73–90, 1998.
12. H. Mantel. Possibilistic definitions of security - an assembly kit. In *Proceedings of the IEEE Computer Security Foundations Workshop*, pages 185–199, Cambridge, UK, 2000.
13. F. Martinelli. Partial model checking and theorem proving for ensuring security properties. In *CSFW*, pages 44–52, 1998.
14. D. McCullough. Specifications for multi-level security and a hook-up property. In *Proceedings of the IEEE Symposium on Security and Privacy*, pages 161–166, Oakland, CA, USA, 1987.
15. J. McLean. A general theory of composition for trace sets closed under selective interleaving functions. In *Proceedings of the IEEE Symposium on Security and Privacy*, pages 79–93, Oakland, CA, USA, 1994.
16. Kevin R. O'Neill and Joseph Y. Halpern. Secrecy in multiagent systems. *CoRR*, cs.CR/0307057, 2003.
17. Peter Y. A. Ryan and Steve A. Schneider. Process algebra and non-interference. In *CSFW*, pages 214–227, 1999.
18. D. Sutherland. A model of information. In *Proceedings of the 9th National Computer Security Conference*, pages 175–183, 1986.
19. J. Todd Wittbold and Dale M. Johnson. Information flow in nondeterministic systems. In *IEEE Symposium on Security and Privacy*, pages 144–161, 1990.
20. A. Zakinthinos and E.S. Lee. A general theory of security properties. In *Proceedings of the IEEE Symposium on Security and Privacy*, pages 94–102, Oakland, CA, USA, 1997.

6 Appendix

Proof of Proposition 2 We proceed by structural induction:

- if $\phi = o \to i$ then, $(\rho, m) \models \phi$ implies $o \in L(\rho, m) \Rightarrow i \in L(\rho, m)$. By definition, $\delta^k_{o_m}(\phi) = i$ if $o_m = o$ and $\delta^k_{o_m}(\phi) = \mathtt{true}$ if $o_m \neq o$. Consequently, $\delta^k_{o_m}(\phi)$ holds in (ρ, m). Moreover, $\delta^k_{o_m\pi}(\phi) = \mathtt{true}$, for all $\pi \in (O_k)^+$ and consequently $\delta^k_{o_m \cdots o_{m+j}}$ is true in $(\rho, m+j)$, for all $j \geq 0$.
- if $\phi = o \to (i \wedge \bigcirc\phi_1)$ then, $(\rho, m) \models \phi$ implies $o \in L(\rho, m) \Rightarrow (i \in L(\rho, m) \wedge (\rho, m+1) \models \phi_1)$. As before, we obtain that $\delta^k_{o_m}(\phi)$ holds in (ρ, m). If $o_m \neq o$ then, $\delta^k_{o_m\pi}(\phi) = \mathtt{true}$, for all $\pi \in (O_k)^+$ and the proof is finished. Otherwise, we use the fact that $\delta^k_{o_m\pi}(\phi) = \delta^k_\pi(\phi_1)$, for all $\pi \in (O_k)^+$, and the inductive hypothesis for $(\rho, m+1) \models \phi_1$, to obtain the needed result.
- the cases $\phi = \phi_1 \wedge \phi_2$ and $\phi = \phi_1 \vee \phi_2$ are obtained directly from the inductive hypothesis.
- if $\phi = \bigcirc\phi_1$ then $(\rho, m) \models \bigcirc\phi_1$ implies $(\rho, m+1) \models \phi_1$. Using $\delta^k_{o_m}(\phi) = \mathtt{true}$ and $\delta^k_{o_m\pi}(\phi) = \delta^k_\pi(\phi_1)$, for all $\pi \in (O_k)^+$, we obtain from the inductive hypothesis, that $(\rho, m+j) \models \delta^k_{o_m \cdots o_{m+j}}(\phi)$, for all $j \geq 0$.
- if $\phi = \Box\phi_1$ then $(\rho, m) \models \Box\phi_1$ implies $(\rho, m+p) \models \phi_1$, for all $p \geq 0$.
  We will prove by induction on j that:

  $$\xi^k_{o_m \ldots o_{m+j}}(\Box\phi_1) = \Box\phi_1 \wedge \xi^k_{o_m \ldots o_{m+j}}(\phi_1) \wedge \xi^k_{o_{m+1} \ldots o_{m+j}}(\phi_1) \wedge \cdots \wedge \xi^k_{o_{m+j}}(\phi_1) \quad (4)$$

  The case $j = 0$ follows directly from the definition of ξ^k. Now, suppose that (4) holds for some j. We will prove that it holds also for $j+1$:

  $$\begin{aligned} \xi^k_{o_m \ldots o_{m+j+1}}(\Box\phi_1) &= \xi^k_{o_{m+j+1}}(\xi^k_{o_m \ldots o_{m+j}}(\Box\phi_1)) \\ &= \xi^k_{o_{m+j+1}}(\Box\phi_1) \wedge \xi^k_{o_{m+j+1}}(\xi^k_{o_m \ldots o_{m+j}}(\phi_1)) \wedge \\ &\quad \wedge \xi^k_{o_{m+j+1}}(\xi^k_{o_{m+1} \ldots o_{m+j}}(\phi_1)) \wedge \cdots \wedge \xi^k_{o_{m+j+1}}(\xi^k_{o_{m+j}}(\phi_1)) \\ &= \Box\phi_1 \wedge \xi^k_{o_{m+j+1}}(\phi_1) \wedge \xi^k_{o_m \ldots o_{m+j+1}}(\phi_1) \wedge \\ &\quad \wedge \xi^k_{o_{m+1} \ldots o_{m+j+1}}(\phi_1) \wedge \cdots \wedge \xi^k_{o_{m+j} o_{m+j+1}}(\phi_1). \end{aligned}$$

  Following an analogous procedure and using (4), we obtain:

  $$\delta^k_{o_m \ldots o_{m+j}}(\Box\phi_1) = \delta^k_{o_m \ldots o_{m+j}}(\phi_1) \wedge \delta^k_{o_{m+1} \ldots o_{m+j}}(\phi_1) \wedge \cdots \wedge \delta^k_{o_{m+j}}(\phi_1) \quad (5)$$

  Now, from $(\rho, m+p) \models \phi_1$, by applying the inductive hypothesis, we obtain that $(\rho, m+p+j) \models \delta^k_{o_{m+p} \ldots o_{m+p+j}}(\phi_1)$, for all $p, j \geq 0$. Consequently, $(\rho, m+j) \models \delta^k_{o_m \ldots o_{m+j}}(\phi)$, for all $j \geq 0$.
- if $\phi = \phi_1 \mathcal{W} o$, we can proceed as in the previous case, but now, the equation (5) holds for all $0 \leq j < p$, where p is the minimum number with the property $o_{m+p} = o$. If $j \geq p$, we have that:

  $$\delta^k_{o_m \ldots o_{m+j}}(\Box\phi_1) = \delta^k_{o_m \ldots o_{m+p-1}}(\phi_1) \wedge \delta^k_{o_{m+1} \ldots o_{m+p-1}}(\phi_1) \wedge \cdots \wedge \delta^k_{o_{m+p-1}}(\phi_1)$$

For the reverse we proceed analogously. □