A Sound and Complete Refinement Relation for Non-reducible Modal Transition Systems

Davide Basile

ISTI–CNR, Pisa, Italy

Abstract. Modal Transition Systems (MTS) are a well-known formalism that extend Labelled Transition Systems (LTS) with the possibility of specifying necessary and permitted behaviour. Whenever two MTS are not in modal refinement relation, it could still be the case that the set of implementations of one MTS is included in the set of implementations of the other. The challenge of devising an alternative notion of modal refinement that is both sound and complete with respect to the set of implementations, without disregarding valuable implementations, remains open. In this paper, we address this challenge. We introduce a subset of MTS called Non-reducible Modal Transition Systems (NMTS), together with a novel refinement relation $\preceq_n$ for NMTS. We show that $\preceq_n$ is sound and also complete with respect to its set of implementations. We illustrate through examples how the additional constraints imposed by NMTS are necessary for achieving completeness. Furthermore, we discuss a property holding for NMTS whose implementations are non-deterministic. We show that any implementation obtained through $\preceq_m$ but disregarded by $\preceq_n$ is violating this property.

1 Introduction

Modal Transition Systems (MTS) [13] extend Labelled Transition Systems (LTS) [9] by distinguishing two types of transitions, meant to describe necessary and optional behaviour in a system specification by means of transitions that must *necessarily* be implemented and transitions that may *optionally* be implemented. MTS come with a concept of *refinement*, which represents a step of the design process, namely the one in which some optional behaviour is discarded while other optional behaviour becomes necessary. Stepwise refinement of an MTS eventually results in an *implementation*, which is an LTS in which no further refinement is possible. Refinement of MTS is critical for enabling formal reasoning on the correctness of a system's design and implementation, by enabling gradually refining an abstract specification into a concrete one, ensuring that each step is correct. MTS are a well-known specification theory and significant advances have been made so far [1,10].

It is known that the (modal) refinement of MTS is not complete (cf., e.g., [12]). In other words, there are cases in which two MTS are not in a refinement relation although the set of implementations of one MTS is included in the set of implementations of the other MTS (this relation is known as thorough refinement). Furthermore, while determining MTS refinement can be computed in polynomial time, determining thorough refinement of MTS requires EXPTIME [7]. In [12], the problem of proposing an alternative notion of modal refinement that is both sound and complete with respect to its

set of implementations is left open [12]. An important aspect is to argue that the considered set of implementations is also interesting from a practical point of view (i.e., no valuable implementation is disregarded).

In this paper, we address this long-standing challenge by proposing a subset of MTS, called *Non-reducible Modal Transition Systems* (NMTS) together with their alternative notion of modal refinement $\preceq_n$ that is both sound and complete with respect to its set of implementations. A fundamental insight behind NMTS is that states non-deterministically reachable through the execution of identical sequences of actions are related. Specifically, the outgoing transitions sharing the same action label also share the same modality. Furthermore, when a refinement step deactivates one optional transition, this leads to the deactivation of all other transitions that share the same label from all other related (source) states.

The contributions of this paper are:

1. we introduce NMTS, a subset of MTS. In NMTS, the transitions sharing the same action label are constrained to also share the same modality whenever they are reachable by the same sequence of actions;
2. we equip NMTS with an alternative notion of modal refinement, called NMTS refinement. The refinement of NMTS is derived from modal refinement by imposing an additional constraint on the optional transitions of the system to be refined;
3. we provide different examples of MTS instances that fail to meet the requisites for being either NMTS or refinements of NMTS. These examples show that the constraints imposed by NMTS and their refinement are necessary to achive a sound and complete refinement relation;
4. we formally prove the soundness (Theorem 2) and completeness (Theorem 3) of NMTS refinement;
5. we introduce the *non-reducible non-determinism* property concerning optional, non-deterministic actions. This non-determinism is inherent in such actions and should be preserved in any implementation where the action remains active. All implementations accepted by the standard MTS refinement, but discarded by the NMTS refinement, are showed to be implementations violating the non-reducible non-determinism property.

Overview Section 2 introduces background on MTS and modal refinement. Section 3 presents Non-reducible MTS (NMTS) and their refinement, proving that NMTS refinement is both sound and complete. Section 4 discusses the property of non-reducible non-determinism, showing that the implementations discarded by NMTS refinement but accepted by modal refinement are violating this property. Section 5 discusses the related work, while Section 6 concludes the paper and discusses future work.

2 Background

We start by discussing some background on MTS. The standard definition of MTS accounts for two sets of transitions, *permitted* (or *may*) transitions, denoted by $\Delta_\Diamond$, and *necessary* (or *must*) transitions, denoted by $\Delta_\Box$, such that $\Delta_\Box \subseteq \Delta_\Diamond$, i.e., all (necessary) transitions are permitted. A transition $(q, a, q') \in \Delta_\Diamond$ is also denoted as

$q \xrightarrow{a}_\Diamond q'$ and likewise $q \xrightarrow{a}_\Box q'$ if $(q,a,q') \in \Delta_\Box$. The reader may be misled to think that $q \xrightarrow{a}_\Diamond q'$ excludes $q \xrightarrow{a}_\Box q'$, and vice versa that $q \xrightarrow{a}_\Box q'$ excludes $q \xrightarrow{a}_\Diamond q'$. However, the first statement is not always true and the second is always false, since $\Delta_\Box \subseteq \Delta_\Diamond$. For our purpose, it is irrelevant to indicate that a transition is permitted. For the sake of simplifying the presentation, we thus opt for a slightly revised definition of MTS, where we partition the set of transitions into *optional* and *necessary* transitions, and no longer indicate the fact that all transitions are *permitted*.

Definition 1 (MTS). *A* Modal Transition System (MTS) S *is a 5-tuple* $S = (Q, A, \overline{q}, \Delta_\bigcirc, \Delta_\Box)$*, with set* Q *of states, set* A *of actions, initial state* $\overline{s} \in Q$*, and transition relation* $\Delta \subseteq Q \times A \times Q$ *partitioned into* optional transitions*, denoted by* $\Delta_\bigcirc$*, and* necessary transitions*, denoted by* $\Delta_\Box$*, i.e.,* $\Delta_\bigcirc \cap \Delta_\Box = \emptyset$*. If* $(s,a,s') \in \Delta_\bigcirc$*, then we also write* $s \xrightarrow{a}_\bigcirc s'$*, and likewise we also write* $s \xrightarrow{a}_\Box s'$ *for* $(s,a,s') \in \Delta_\Box$*. We write* $s \xrightarrow{a} s'$ *when* $(s,a,s') \in \Delta$*. We may omit the target state when it is immaterial.*

Note that the standard definition of MTS is $(Q, A, \overline{q}, \Delta_\Diamond, \Delta_\Box)$, where $\Delta_\Diamond = \Delta_\bigcirc \cup \Delta_\Box$. An LTS is an MTS where $\Delta_\bigcirc = \emptyset$. In the sequel, the conversion from an MTS (and NMTS, cf. Section 3) $(Q, A, \overline{q}, \Delta_\bigcirc, \Delta_\Box)$ with $\Delta_\bigcirc = \emptyset$ to an LTS $(Q, A, \overline{q}, \Delta)$ with $\Delta = \Delta_\Box$ is implicit. Moreover, we will use subscripts or superscripts to indicate the origin of an element of a tuple, i.e., $S = (Q_S, A_S, \overline{s}, \Delta_S^\bigcirc, \Delta_S^\Box)$. We now define modal refinement of MTS.

Definition 2 (modal refinement). *An MTS* S *is a* (modal) refinement *of an MTS* T*, denoted by* $S \preceq_m T$*, if and only if there exists a* refinement relation $\mathcal{R} \subseteq Q_S \times Q_T$ *such that* $(\overline{s}, \overline{t}) \in \mathcal{R}$ *and for all* $(s,t) \in \mathcal{R}$*, the following holds:*

1. *whenever* $t \xrightarrow{a}_\Box t'$*, for some* $t' \in Q_T$ *and* $a \in A_T$*, then* $a \in A_S$*,* $\exists\, s' \in Q_S : s \xrightarrow{a}_\Box s'$*, and* $(s', t') \in \mathcal{R}$*, and*
2. *whenever* $s \xrightarrow{a} s'$*, for some* $s' \in Q_S$ *and* $a \in A_S$*, then* $a \in A_T$*,* $\exists\, t' \in Q_T : t \xrightarrow{a} t'$*, and* $(s', t') \in \mathcal{R}$*.*

We also say that S *(modally) refines* T *when* $S \preceq_m T$*.*

Intuitively, S modally refines T if any necessary transition of T can be mimicked by a necessary transition of S, and every transition of S can be mimicked by a transition of T. The set of implementations of an MTS S, written $Impl_m(S)$ is defined as the set of LTS I such that $I \preceq_m S$. Indeed, LTS cannot be further refined and are considered implementations. In other words, every LTS refinement of an MTS S is an *implementation* of S.

In [12], it is shown that $S \preceq_m T$ implies $Impl_m(S) \subseteq Impl_m(T)$. In other words, modal refinement is *sound*, i.e., each time an MTS S modally refines an MTS T, it follows that the set of implementations of T also contains the implementations of S. However, the contrary is not true, i.e., modal refinement is not *complete*. Figure 1, reproduced from [7], shows an example where the set of implementations of T also contains the implementations of S, but S does not modally refine T.

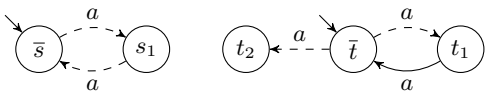

Fig. 1. From left two right, two MTS S and T such that $S \not\preceq_m T$ and $Impl_m(S) \subseteq Impl_m(T)$, showing that modal refinement is not complete (reproduced from [7]). Dashed arcs are used to depict optional transitions ($\Delta_\circ$), while solid arcs depict necessary transitions ($\Delta_\square$).

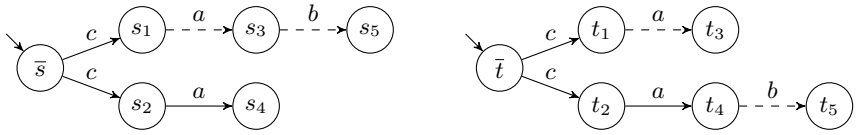

Fig. 2. From left two right, two MTS S and T such that $Impl_m(S) \subseteq Impl_m(T)$ but $S \not\preceq_m T$. Both S and T are not NMTS because $f^{\square}_S(c) \cap f^{\circ}_S(c) = \{a\}$ and $f^{\square}_T(c) \cap f^{\circ}_T(c) = \{a\}$

3 Non-Reducible MTS Refinement

All examples documented in the literature (e.g., [7,12]), which demonstrate that modal refinement is not complete (e.g., Figure 1), involve the utilization of a non-deterministic choice within the system under refinement. This non-deterministic choice, such as the outgoing transitions from state $\overline{t}$ in T (as depicted in Figure 1), is subsequently eliminated in the refined system, as it is the case in Figure 1 for system S.

Consider Figure 2. Similarly to Figure 1, it shows an example of two MTS S and T such that the implementations of S are included into the implementations of T, although S and T are not in modal refinement relation. Figure 2 differs from Figure 1 (and all other similar examples in the literature) in that it preserves the non-deterministic choices of T within S. In T, the states t_1 and t_2 are reachable by executing the same action c and both exhibit outgoing transitions labeled as a. Nonetheless, these two transitions do not share the same modality.

NMTS In this section, we identify the subset of MTS that exclusively discards systems as those in Figure 2. Indeed, Figure 2 shows how such MTS instances can result in a violation of completeness. We introduce *Non-reducible Modal Transition Systems* (NMTS). In NMTS, whenever a sequence of actions leads non-deterministically to different states, all these states are interconnected by the requirement that transitions associated with the same action must also have the same modality.

In the following, let $w = a_1 \dots a_n$ be a sequence of actions in A^*. The sequence of transitions $\overline{s} \xrightarrow{a_1} s_1$, $s_1 \xrightarrow{a_2} s_2$, …, $s_{n-1} \xrightarrow{a_n} s$ is written as $\overline{s} \xrightarrow{w} s$. Furthermore, we write $\overline{s} \not\xrightarrow{w} s$ when it is not possible to reach s from $\overline{s}$ through the sequence of actions w.

Definition 3 (NMTS). *A* Non-reducible Modal Transition System (NMTS) *S is a 6-tuple $S = (Q, A, \overline{q}, \Delta, f_\square, f_\circ)$, with set Q of states, set A of actions, initial state $\overline{s} \in Q$, and transition relation $\Delta \subseteq Q \times A \times Q$, where Δ is partitioned into $\Delta_\circ$, the set of* optional *transitions, and $\Delta_\square$, the set of* necessary *transitions, i.e., $\Delta_\circ \cap \Delta_\square = \emptyset$. Functions $f_\square : A^* \mapsto 2^A$ and $f_\circ : A^* \mapsto 2^A$ are such that*

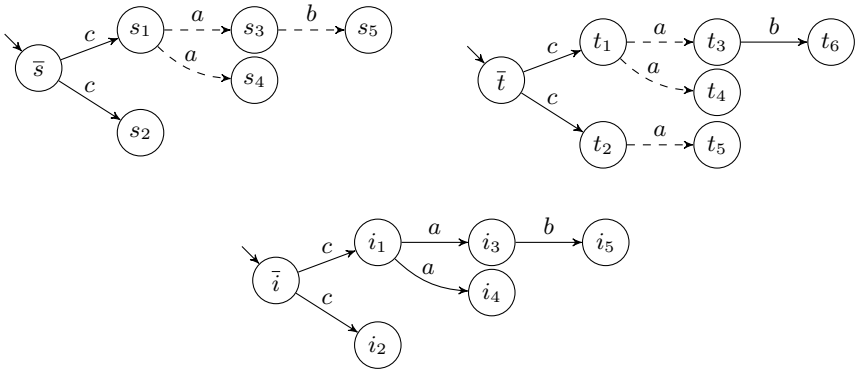

Fig. 3. Top row, from left two right, two NMTS S and T such that $Impl_m(S) \subseteq Impl_m(T)$ but $S \not\preceq_m T$. Furthermore, $S \not\preceq_n T$ and $Impl_n(S) \not\subseteq Impl_n(T)$. Bottom row, an implementation I such that $I \preceq_n S$, $I \not\preceq_n T$, but $I \preceq_m T$

- *for all* $w \in A^*$ *such that* $\overline{s} \xrightarrow{w} s$ *it holds that* $f_\Box(w) \cap f_\bigcirc(w) = \emptyset$,
- *for all* $w_1, w_2 \in A^*$ *whenever* $\overline{s} \xrightarrow{w_1} s$ *and* $\overline{s} \xrightarrow{w_2} s$ *then* $f_\Box(w_1) = f_\Box(w_2)$, $f_\bigcirc(w_1) = f_\bigcirc(w_2)$,
- *whenever* $(s, a, s') \in \Delta$ *there exists* $w \in A^*$ *such that* $\overline{s} \xrightarrow{w} s$ *and either*
  - $a \in f_\Box(w)$, *and in this case* $(s, a, s') \in \Delta_\Box$, *or*
  - $a \in f_\bigcirc(w)$, *and in this case* $(s, a, s') \in \Delta_\bigcirc$.
- *whenever* $a \in f_\Box(w) \cup f_\bigcirc(w)$ *for some* $w \in A^*$ *there exists a state* $s \in Q_S$ *such that* $\overline{s} \xrightarrow{w} s$ *and* $(s, a, s') \in \Delta$ *for some* $s' \in Q_S$.

We write $f(w)$ *to denote* $f_\Box(w) \cup f_\bigcirc(w)$.

Definition 3 enhances Definition 1 by including two functions, namely $f_\Box$ and $f_\bigcirc$. These functions serve a dual purpose. Firstly, they establish a connection between states reachable through the execution of identical sequences of actions. Secondly, they constraint outgoing transitions from interconnected states that are sharing the same label to also share the same modality.

Note that NMTS are a stric subset of MTS because in NMTS, for all $w \in A^*$ such that $\overline{s} \xrightarrow{w} s$, the condition $f_\Box(w) \cap f_\bigcirc(w) = \emptyset$ holds (as defined in Definition 3). In contrast, within MTS, it is possible to have $f_\Box(w) \cap f_\bigcirc(w) \neq \emptyset$. If we were to remove this constraint from Definition 3, then NMTS would become equivalent to MTS.

Consider Figure 3. In contrast to Figure 2, Figure 3 presents two systems, denoted as S and T, satisfying the conditions of Definition 3 (i.e., S and T are NMTS), and satisfying the conditions $Impl_m(S) \subseteq Impl_m(T)$ and $S \not\preceq_m T$. Similarly to Figure 2, also in Figure 3 the non-deterministic choice in state t_1 in T is maintained in state s_1 in S. Figure 3 proves that, for achieving completeness, it is not sufficient to constrain MTS to be NMTS. In the following, we will show that it also necessary to introduce constraints on the refinement relation between NMTS.

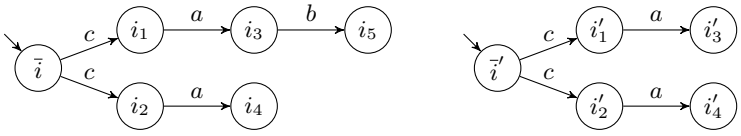

Fig. 4. Two LTS I and I' both implementations of the MTS S and T of Figure 2. The set $Impl_n(S)$ contains all and only LTS that are strongly bisimilar to either I or I'. It follows that $Impl_n(S) \subseteq Impl_n(T)$, and $S \not\preceq_n T$ (under the assumption that $\preceq_n$ is also applicable to MTS)

NMTS refinement We now introduce NMTS modal refinement $\preceq_n$. In contrast to standard modal refinement, an additional condition is introduced, which applies to the optional transitions within the system undergoing refinement. If an optional transition is deactivated during the refinement process, it is required that this deactivation applies uniformly to all other optional transitions sharing the same action. This uniform deactivation rule applies across all source states reachable through the same sequence of actions.

Definition 4 (NMTS refinement). *An NMTS S is an NMTS refinement of another NMTS T, denoted as $S \preceq_n T$, if there exists a refinement relation $\mathcal{R} \subseteq Q_S \times Q_T$ between the states of the two systems such that $(\overline{s}, \overline{t}) \in \mathcal{R}$ and for all $(s,t) \in \mathcal{R}$ there exists $w \in A_S^*$ such that $\overline{s} \xrightarrow{w} s$ and $\overline{t} \xrightarrow{w} t$ and*

1. *whenever $t \xrightarrow{a}_\square t'$ (for some $t' \in Q_T$, $a \in f_T^\square(w)$), then $a \in f_S^\square(w)$ and there exists a state $s' \in Q_S$ such that $s \xrightarrow{a}_\square s'$ and $(s',t') \in \mathcal{R}$.*
2. *whenever $t \xrightarrow{a}_\circ t'$ (for some $t' \in Q_T$, $a \in f_T^\circ(w)$), then one of the following holds:*
   - *$a \notin f_S(w)$*
   - *$a \in f_S(w)$ and there exists a state $s' \in Q_S$ such that $s \xrightarrow{a} s'$ and $(s',t') \in \mathcal{R}$.*
3. *whenever $s \xrightarrow{a} s'$ (for some $s' \in Q_S$, $a \in f_S(w)$), then $a \in f_T(w)$, and there exists a state $t' \in Q_T$ such that $t \xrightarrow{a} t'$ and $(s',t') \in \mathcal{R}$.*

As discussed earlier, Figure 3 shows that the further constraint imposed by Definition 3 is not sufficient to achieve completeness of modal refinement. Figure 2 and Figure 4 show that the additional constraint imposed by Definition 4 on the refinement relation, when considered independently, is also not sufficient to achieve completeness. Indeed, if we switch $\preceq_m$ with $\preceq_n$ in Figure 2, as showed in Figure 4, it would still hold that $Impl_n(S) \subseteq Impl_n(T)$ and $S \not\preceq_n T$, because S and T are not NMTS. In other words, the example in Figure 2 proves that if non-deterministic MTS do not meet the criteria to be classified as NMTS, then it is possible to build an example, as the one in Figure 2, showing that both modal refinement and NMTS refinement are not complete.

In summary, the examples in Figure 2 and Figure 3 show that the constraints on MTS and their refinement provided by Definition 3 and Definition 4 are both required to achieve completeness. By either dropping the constraints on MTS (i.e., Definition 3) or on their refinement (i.e., Definition 4), it is possible to demonstrate that the resulting refinement relation is not complete. In Theorem 3, we will prove that the constraints

Fig. 5. Two MTS S and T such that $S \preceq_m T$, $S \not\preceq_n T$. Furthermore, $T \preceq_m S$ and $T \not\preceq_n S$. In both directions, $\bar{s} \xrightarrow{a}_{\circ} s_2$, $\bar{t} \xrightarrow{a}_{\circ} t_1$, $t_1 \xrightarrow{b}_{\circ} t_2$, $b \in f_S(a)$ and $s_2 \not\xrightarrow{b}$

imposed by Definition 3 and Definition 4 are also sufficient to achieve completeness of the refinement relation.

Figure 5 depicts another example showcasing the differences between $\preceq_m$ and $\preceq_n$. Consider the LTS I_T obtained by switching all transitions of T (in Figure 5) to must. Clearly, $I_T \preceq_n T$, but $I_T \not\preceq_n S$ (note that this is not true for the case of $\preceq_m$).

Due to the coinductive nature of Definition 3, similarly to the complexity of deciding modal refinement or strong bisimulation, also the complexity of deciding an NMTS refinement is polynomial, provided that the input includes the functions $f_{\Box}$ and $f_{\circ}$.

Remark Note that as an alternative characterisation, the condition outlined in Definition 3 (namely, $f_{\Box}(w) \cap f_{\circ}(w) \neq \emptyset$) can be omitted, at the cost of modifying the refinement relation $\preceq_n$ to a new form, call it $\preceq'_n$, modified as follows. In $\preceq'_n$, whenever $a \in f_{\Box}(w) \cap f_{\circ}(w)$ for some $a \in A$, all transitions reachable via w and labeled with a are treated as necessary, even if they are declared optional. We argue that while this alternative characterisation would enable the inclusion of all MTS and not a limited subset, it would introduce ambiguity. This is because it would permit to denote a necessary transition δ as optional whenever there exists another necessary transition δ' with the same action as δ and reachable through the execution of the same sequence of actions. Therefore, whenever in an MTS it holds that $a \in f_{\Box}(w) \cap f_{\circ}(w)$ for some $a \in A$, rather than considering all transitions reachable via w and labeled with a as necessary, even if they are denoted as optional, we opt to exclude such MTS from consideration.

We show that $\preceq_n$ is a conservative extension of $\preceq_m$.

Theorem 1. *Let S and T be two NMTS. If $S \preceq_n T$ then $S \preceq_m T$.*

Proof. Let $\mathcal{R}$ be proving $S \preceq_n T$. It holds that $(\bar{s}, \bar{t}) \in \mathcal{R}$. Furthermore, for any $(s,t) \in \mathcal{R}$, by hypothesis there exists some $w \in A_S^*$ such that $\bar{s} \xrightarrow{w} s$ and $\bar{t} \xrightarrow{w} t$. Furthermore:

- whenever $t \xrightarrow{a}_{\Box} t'$, it holds that $a \in f_S^{\Box}(w)$ (therefore $a \in A_S$), $s \xrightarrow{a}_{\Box} s'$ and $(s', t') \in \mathcal{R}$;
- whenever $s \xrightarrow{a} s'$ it holds that $a \in f_T(w)$ (therefore $a \in A_T$), $t \xrightarrow{a} t'$ and it holds that $(s', t') \in \mathcal{R}$. □

Consider Figure 3. Since $S \not\preceq_m T$, by Theorem 1 it follows that $S \not\preceq_n T$.

We now show the relations between the functions $f^{\Box}$ and f° of two systems in NMTS refinement relation.

Lemma 1. *Let S and T be two NMTS such that $S \preceq_n T$. For all $w \in A_S^*$ such that $\bar{s} \xrightarrow{w} s$, it holds that $f_S^{\circ}(w) \subseteq f_T^{\circ}(w)$, $f_T^{\Box}(w) \subseteq f_S^{\Box}(w)$ and $f_S^{\Box}(w) \setminus f_T^{\Box}(w) \subseteq f_T^{\circ}(w) \setminus f_S^{\circ}(w)$.*

Proof. Each action A_S appears in some transition in Δ_S (there are no redundant elements in A_S). By hypothesis $S \preceq_n T$ and by point 3 of Definition 4 it holds that $A_S \subseteq A_T$ (we assume that all states are reachable, i.e., there are no redundant states). We first prove that for all $w \in A_S^*$ such that $\overline{s} \xrightarrow{w} s$ it holds $f_T^{\Box}(w) \subseteq f_S^{\Box}(w)$. By contradiction, assume that there exists some $w \in A_S^*$ such that $\overline{s} \xrightarrow{w} s$ and $a \in f_T^{\Box}(w) \backslash f_S^{\Box}(w)$. Hence, by Definition 3 there exists a transition $\delta \in \Delta_T^{\Box}$ labelled with a for some $t \in Q_T$ source state of δ such that $\overline{t} \xrightarrow{w} t$. By hypothesis, there must be some $s \in Q_S$ such that $(s,t) \in \mathcal{R}$, where $\mathcal{R}$ is the NMTS refinement relation for $S \preceq_n T$. By Definition 4 it holds that $s \xrightarrow{a}_{\Box} s' \in \Delta_S$ and $a \in f_S^{\Box}(w)$. We reached a contradiction.

We now show that for all $w \in A_S^*$ such that $\overline{s} \xrightarrow{w} s$ it holds $f_S^{\bigcirc}(w) \subseteq f_T^{\bigcirc}(w)$. By contradiction, assume that there exists some $w \in A_S^*$ with $\overline{s} \xrightarrow{w} s$ and an action $a \in f_S^{\bigcirc}(w) \setminus f_T^{\bigcirc}(w)$. Hence, there exists a transition $\delta \in \Delta_{\bigcirc}^S$ reachable via w and labelled with a. Let s be the source state of δ. By Definition 4, since $A_S \subseteq A_T$, for some $t \in Q_T$ it holds that $\overline{t} \xrightarrow{w} t$ and $(s,t) \in \mathcal{R}$. By Definition 4 it holds that $t \xrightarrow{a} t' \in \Delta_T$. Since $a \notin f_T^{\bigcirc}(w)$, it must be the case that $a \in f_T^{\Box}(w)$, hence $a \in f_S^{\Box}(w)$. We reached a contradiction.

Finally, we prove that for all $w \in A_S^*$ such that $\overline{s} \xrightarrow{w} s$ it holds $f_S^{\Box}(w) \setminus f_T^{\Box}(w) \subseteq f_T^{\bigcirc}(w) \setminus f_S^{\bigcirc}(w)$. Let $a \in f_S^{\Box}(w) \setminus f_T^{\Box}(w)$. Since $f_S^{\Box}(w) \cap f_S^{\bigcirc}(w) = \emptyset$, we have $a \notin f_S^{\bigcirc}(w)$. Moreover, there exists some transition $s \xrightarrow{a} s' \in \Delta_S$ with $\overline{s} \xrightarrow{w} s$. By Definition 4, for some $t \in Q_T$ it holds that $\overline{t} \xrightarrow{w} t$, $(s,t) \in \mathcal{R}$, $t \xrightarrow{a} t' \in \Delta_T$, $a \in f_T(w)$ and $(s',t') \in \mathcal{R}$. Since $a \in f_S^{\Box}(w) \setminus f_T^{\Box}(w)$, it must be the case that $a \in f_T^{\bigcirc}(w)$. □

We now show that, similarly to $\preceq_m$, also $\preceq_n$ is a preorder.

Lemma 2. *The relation $\preceq_n$ is a preorder.*

Proof. Let S be an NMTS. Clearly, $\{(s,s) \mid s \in Q_S\}$ shows that $S \preceq_n S$. Let T and U be two NMTS such that $S \preceq_n T$ and $T \preceq_n U$.

We now prove that the relation $\mathcal{R} = \{(s,u) \mid (s,t) \in \mathcal{R}_{S \preceq_n T}, (t,u) \in \mathcal{R}_{T \preceq_n U}, t \in Q_T\}$ shows that $S \preceq_n U$. Clearly $(\overline{s}, \overline{u}) \in \mathcal{R}$. Whenever $(s,u) \in \mathcal{R}$ for some $w \in A_S^*$ where $\overline{s} \xrightarrow{w} s$ and $\overline{u} \xrightarrow{w} u$ then:

- if $u \xrightarrow{a}_{\Box} u'$, by $(t,u) \in \mathcal{R}_{T \preceq_n U}$ it holds $t \xrightarrow{a}_{\Box} t'$ and $(t',u') \in \mathcal{R}_{T \preceq_n U}$. By $(s,t) \in \mathcal{R}_{S \preceq_n T}$ it holds $s \xrightarrow{a}_{\Box} s'$, $(s',t') \in R_{S \preceq_n T}$. Therefore, $(s',u') \in \mathcal{R}$;
- if $u \xrightarrow{a}_{\bigcirc} u'$ by $(t,u) \in \mathcal{R}_{T \preceq_n U}$ we distinguish two cases:
  - either $a \notin f_T(w)$. By $(s,t) \in \mathcal{R}_{S \preceq_n T}$ and Lemma 1 (i.e., $f_S(w) \subseteq f_T(w)$), it follows $a \notin f_S(w)$;
  - $a \in f_T(w)$, $t \xrightarrow{a} t'$ and $(t',u') \in \mathcal{R}_{T \preceq_n U}$. By $(s,t) \in \mathcal{R}_{S \preceq_n T}$ either, $a \notin f_S(w)$ or $a \in f_S(w)$ $s \xrightarrow{a} s'$, $(s',t') \in \mathcal{R}_{S \preceq_n T}$ and $(s',u') \in \mathcal{R}$;
- if $s \xrightarrow{a} s'$ by $(s,t) \in \mathcal{R}_{S \preceq_n T}$ it follows that $t \xrightarrow{a} t'$ and $(s',t') \in \mathcal{R}_{S \preceq_n T}$. By $(t,u) \in \mathcal{R}_{T \preceq_n U}$ it follows that $u \xrightarrow{a} u'$ and $(t',u') \in \mathcal{R}_{T \preceq_n U}$. Hence $(s',u') \in \mathcal{R}$.

□

Given an MTS S we denote with $Impl_n(S)$ the set of LTS I such that $I \preceq_n S$. The soundness of $\preceq_n$ is straightforward.

Theorem 2 ($\preceq_n$ soundness). *Let S and T be two MTS. If $S \preceq_n T$ then $Impl_n(S) \subseteq Impl_n(T)$.*

Proof. Pick an implementation $I \preceq_n S$, since $S \preceq_n T$ by transitivity $I \preceq_n T$. □

Before proceeding to prove the completeness of $\preceq_n$, we establish two auxiliary lemmata. The first lemma demonstrates that a refinement can occur by either asserting (i.e., switching to necessary) or removing a set of optional transitions that are reachable through the same sequence of actions and share the same action label.

Lemma 3. *Let S be an NMTS and let $S' = (Q_{S'}, A_{S'}, \overline{s}, \Delta_{S'}, f^{\Box}_{S'}, f^{\bigcirc}_{S'})$ be obtained from S as follows:*

- *there exists a sequence $w \in A^*_S$ such that $\overline{s} \xrightarrow{w} s$ for some $s \in Q_S$ and*
- *$\forall w' \in A^*_S$ such that $(i) \exists s' \in Q_S . \overline{s} \xrightarrow{w} s'$ and $(ii)\ \forall s'' \in Q_S . \overline{s} \xrightarrow{w} s'' \vee \overline{s} \xrightarrow{w'} s''$, it holds that $f^{\Box}_{S'}(w') = f^{\Box}_{S}(w')$ and $f^{\bigcirc}_{S'}(w') = f^{\bigcirc}_{S}(w')$ and*
- *there exists $a \in f^{\bigcirc}_{S}(w)$ such that $a \notin f^{\bigcirc}_{S'}(w)$ and either $a \in f^{\Box}_{S'}(w)$ (assert action) or $a \notin f^{\Box}_{S'}(w)$ (remove action).*

Furthermore $Q_{S'} = \{s \mid s \in Q_S, s \text{ is reachable in } S'\}$ and $A_{S'} = \{a \mid a \in A_S, (s, a, s') \in \Delta_{S'} \text{ for some } s, s' \in Q_{S'}\}$. It holds that $S' \preceq_n S$.

Proof. Let $\mathcal{R} = \{(s, s) \mid s \in Q_{S'}\}$. We show that $\mathcal{R}$ proves $S' \preceq_n S$. Trivially $(\overline{s}, \overline{s})$. Furthermore, for all couples $(s, s) \in \mathcal{R}$ such that $\overline{s} \not\xrightarrow{w} s$ the outgoing transitions of s are identical in S and S' and the conditions in Definition 4 hold trivially. When $(s, s) \in \mathcal{R}$ is such that $\overline{s} \xrightarrow{w} s$ it holds that:

- whenever $s \xrightarrow{a'}_{\Box} s' \in \Delta_S$ ($a' \in f^{\Box}_S(w)$), we need to show that $a \neq a'$, otherwise, in case of remove, we would have $a \notin f^{\Box}_{S'}(w)$. Since $a \in f^{\bigcirc}_S(w)$ and $f^{\bigcirc}_S(w) \cap f^{\Box}_S(w) = \emptyset$, it follows that $a \neq a'$, $a' \in f^{\Box}_{S'}(w)$, $s \xrightarrow{a'}_{\Box} s' \in \Delta_{S'}$ and $(s', s') \in \mathcal{R}$;
- whenever $s \xrightarrow{a'}_{\bigcirc} s' \in \Delta_S$ ($a' \in f^{\bigcirc}_S(w)$), if $a \neq a'$ then $a \in f^{\bigcirc}_{S'}(w)$, $s \xrightarrow{a'}_{\bigcirc} s' \in \Delta_{S'}$ and $(s', s') \in \mathcal{R}$. Otherwise, $a \notin f^{\bigcirc}_{S'}(w)$;
- whenever $s \xrightarrow{a'} s' \in \Delta_{S'}$ ($a' \in f_S(w)$), then $a' \in f_S(w)$, $s \xrightarrow{a'} s' \in \Delta_S$ and $(s', s') \in \mathcal{R}$. □

The second lemma shows the conditions under which it is possible to switch a set of necessary transitions (whose source state is reachable by the same sequence of actions) to optional ones, whilst preserving NMTS refinement.

Lemma 4. *Let S and T be two NMTS such that $S \preceq_n T$, where for some $s \in Q_S$ there exists a sequence $w \in A^*_S . \overline{s} \xrightarrow{w} s$ such that $a \in f^{\Box}_S(w) \setminus f^{\Box}_T(w)$. It holds $S' \preceq_n T$, where $S' = (Q_S, A_S, \overline{s}, \Delta_{S'}, f^{\Box}_{S'}, f^{\bigcirc}_{S'})$ and:*

- *$\forall w' \in A^*_S$ such that $(i) \exists s' \in Q_S . \overline{s} \xrightarrow{w} s'$ and $(ii)\ \forall s \in Q_S . \overline{s} \not\xrightarrow{w} s \vee \overline{s} \xrightarrow{w'} s$, it holds that $f^{\Box}_{S'}(w') = f^{\Box}_{S}(w')$ and $f^{\bigcirc}_{S'}(w') = f^{\bigcirc}_{S}(w')$ and*
- *$f^{\Box}_{S'}(w) = f^{\Box}_{S}(w) \setminus \{a\}$ and $f^{\bigcirc}_{S'}(w) = f^{\bigcirc}_{S}(w) \cup \{a\}$.*

Proof. Firstly, since $S \preceq_n T$, by Lemma 1, for all $w' \in A_S^*$ such that $\overline{s} \xrightarrow{w'} s$, it holds $f_S^{\square}(w') \setminus f_T^{\square}(w') \subseteq f_T^{\bigcirc}(w') \setminus f_S^{\bigcirc}(w')$. Therefore, by hypothesis, $a \in f_T^{\bigcirc}(w)$. Assume that $\mathcal{R}$ proves $S \preceq_n T$. Then, we show that the relation $\mathcal{R}$ also proves $S' \preceq_n T$. Firstly, $(\overline{s}, \overline{t}) \in \mathcal{R}$. For all $(s,t) \in \mathcal{R}$ such that $\overline{s} \overset{w}{\not\longrightarrow} s$ and $\overline{t} \overset{w}{\not\longrightarrow} t$, we have that the outgoing transitions of s in S' are identical to those in S, and the conditions in Definition 4 hold trivially. Otherwise, for all $(s,t) \in \mathcal{R}$ such that $\overline{s} \xrightarrow{w} s$ and $\overline{t} \xrightarrow{w} t$ it holds:

1. Whenever $t \xrightarrow{a'} t' \in \Delta_T$:
   (a) if $a' \in f_T^{\square}(w)$, by hypothesis it holds $a' \neq a$. Since $(s,t) \in \mathcal{R}$, it holds $a' \in f_{S'}^{\square}(w)$, $s \xrightarrow{a'}_{\square} s' \in \Delta_{S'}$ and $(s',t') \in \mathcal{R}$;
   (b) if $a' \in f_T^{\bigcirc}(w)$ and $a' \in f_S(w)$, then $a' \in f_{S'}(w)$ and by $(s,t) \in \mathcal{R}$, it holds $s \xrightarrow{a'} s' \in \Delta_{S'}$ and $(s',t') \in \mathcal{R}$;
   (c) if $a' \in f_T^{\bigcirc}$ and $a' \notin f_S(w)$, then by construction also $a' \notin f_{S'}(w)$;
2. whenever $s \xrightarrow{a'} s' \in \Delta_{S'}$, then by construction $a' \in f_S(w)$, thus $s \xrightarrow{a'} s' \in \Delta_S$, and since $(s,t) \in \mathcal{R}$, we have $t \xrightarrow{a'} t' \in \Delta_T$ and $(s',t') \in \mathcal{R}$. □

We are now ready to prove the main result of this section, the completeness of $\preceq_n$.

Theorem 3 ($\preceq_n$ completeness). *$Impl_n(S) \subseteq Impl_n(T)$ implies $S \preceq_n T$.*

Proof. Let $I_S = (Q_S, A_S, \overline{s}, \Delta_{I_S}, f_{I_S}^{\bigcirc}, f_{I_S}^{\square})$, where for all $w \in A_S^*$.$f_{I_S}^{\square}(w) = f_S(w)$, $f_{I_S}^{\bigcirc} = \emptyset$ be the implementation obtained from S by repeatedly applying until exhaustion the assert operation from Lemma 3. By Lemma 3, $I_S \preceq_n S$, therefore $I_S \in Impl_n(S)$. By hypothesis, $I_S \preceq_n T$. Note that I_S is an implementation since $\Delta_{I_S}^{\bigcirc} = \emptyset$, whilst $\Delta_{I_S}^{\square} = \Delta_S$.

Let $I'_S = (Q'_S, A'_S, \overline{s}, \Delta_{I_{S'}}, f_{I'_S}^{\bigcirc}, f_{I'_S}^{\square})$ be the implementation computed from S by repeatedly applying until exhaustion the remove operation from Lemma 3. It holds that for all $w \in A_S^*$, $f_{I'_S}^{\square}(w) = f_S^{\square}(w)$, $f_{I'_S}^{\bigcirc}(w) = \emptyset$, $\Delta_{I_{S'}}^{\bigcirc} = \emptyset$, $\Delta_{I_{S'}}^{\square} = \Delta_S^{\square}$. By Lemma 3, it holds that $I'_S \preceq_n S$, therefore $I'_S \in Impl_n(S)$. By hypothesis $I'_S \preceq_n T$.

For any $w \in A_S^*$ such that $\overline{s} \xrightarrow{w} s$ by Lemma 1 and $f_T^{\square}(w) \subseteq f_{I'_S}^{\square}(w) = f_S^{\square}(w)$ it holds $f_S^{\bigcirc}(w) \cap f_T^{\square}(w) = \emptyset$.

If for all $w \in A_S^*$ such that $\overline{s} \xrightarrow{w} s$ it holds $f_S^{\bigcirc}(w) = \emptyset$, then since $f_S^{\bigcirc}(w) \cap f_S^{\square}(w) = \emptyset$ we have that $S = I_S$ and the thesis follows. Hence, assume that for some $s \in Q_S$ such that $\overline{s} \xrightarrow{w} s$, $w \in A_S^*$, it holds $f_S^{\bigcirc}(w) \neq \emptyset$. We perform two nested iteration loops. In the external loop, we iterate on the states in the set $P = \{ s \mid s \in Q_S, w \in A_S^*, \overline{s} \xrightarrow{w} s, f_S^{\bigcirc}(w) \neq \emptyset \}$. We start by selecting an $s^1 \in Q_S$ and $w^1 \in A_S^*$ such that $\overline{s} \xrightarrow{w^1} s^1$ and $f_S^{\bigcirc}(w^1) \neq \emptyset$. In the internal loop, for each selected state, we iterate on the actions $a \in f_S^{\bigcirc}(w^1)$. We pick an action $a \in f_S^{\bigcirc}(w^1)$, thus $a \notin f_T^{\square}(w^1)$ and $a \in f_{I_S}^{\square}(w^1)$. From I_S, T, and a by applying Lemma 4 we obtain an NMTS $S_1^1 = (Q_S, A_S, \overline{s}, \Delta_{S_1^1}, f_{S_1^1}^{\square}, f_{S_1^1}^{\bigcirc})$ such that for all w' with $\overline{s} \overset{w'}{\not\longrightarrow} s^1$ it holds $f_{S_1^1}^{\square}(w') = f_{I_S}^{\square}(w')$, $f_{S_1^1}^{\bigcirc}(w') = f_{I_S}^{\bigcirc}(w') = \emptyset$. Furthermore, $f_{S_1^1}^{\square}(w^1) = f_{I_S}^{\square}(w^1) \setminus \{a\}$, $f_{S_1^1}^{\bigcirc}(w^1) = \{a\}$. By Lemma 4, since $I_S \preceq_n T$, $a \in f_{I_S}^{\square}(w^1) \setminus f_T^{\square}(w^1)$, it holds $S_1^1 \preceq_n T$.

We re-iterate (internal iteration) and pick the next action. From S_1^1, T, and an action $b \in f_S^{\bigcirc}(w^1)$, $b \notin f_T^{\square}(w^1)$ such that $b \neq a$, hence $b \in f_{S_1^1}^{\square}(w^1)$, we build an NMTS $S_1^2 = (Q_S, A_S, \overline{s}, \Delta_{S_1^2}, f_{S_1^2}^{\square}, f_{S_1^2}^{\bigcirc})$ such that for all w' with $\overline{s} \xrightarrow{w'} s^1$ it holds $f_{S_1^2}^{\square}(w') = f_{S_1^1}^{\square}(w')$, $f_{S_1^2}^{\bigcirc}(w') = f_{S_1^1}^{\bigcirc}(w')$, and $f_{S_1^2}^{\square}(w^1) = f_{S_1^1}^{\square}(w^1) \setminus \{b\}$, $f_{S_1^2}^{\bigcirc}(w^1) = f_{S_1^1}^{\bigcirc}(w^1) \cup \{b\} = \{a, b\}$. By Lemma 4, since $S_1^1 \preceq_n T$, $b \in f_{S_1^1}^{\square}(w^1)$ and $b \notin f_T^{\square}(w^1)$, it holds $S_1^2 \preceq_n T$.

We re-iterate (internal iteration) for all actions in $f_S^{\bigcirc}(w^1)$. We obtain an NMTS $S_1^n = (Q_S, A_S, \overline{s}, \Delta_{S_1^n}, f_{S_1^n}^{\square}, f_{S_1^n}^{\bigcirc})$ where $|f_S^{\bigcirc}(w^1)| = n$ such that $f_{S_1^n}^{\square}(w^1) = f_S^{\square}(w^1)$, $f_{S_1^n}^{\bigcirc}(w^1) = f_S^{\bigcirc}(w^1)$.

We repeat again the (external) iteration for all states in P. At the second (external) iteration, we pick a state $s^2 \in P$ and a sequence of actions $w^2 \in A_S^*$ such that $\overline{s} \xrightarrow{w^2} s^2$, $f_S^{\bigcirc}(w^2) \neq \emptyset$ and $\overline{s} \not\xrightarrow{w^2} s^i$ for all $i < 2$. If this last condition is not satisfied (i.e., for all $w^2 \in A_S^*$ it holds that $\overline{s} \xrightarrow{w^2} s^i$ for some $i < 2$) then we skip this iteration and continue with the next (the external counter is incremented nonetheless). We pick an action $a \in f_S^{\bigcirc}(w^2)$, thus $a \notin f_T^{\square}(w^2)$ and $a \in f_{S_1^n}^{\square}(w^2) = f_{I_S}^{\square}(w^2)$. From S_1^n, T, and a we build an NMTS $S_2^1 = (Q_S, A_S, \overline{s}, \Delta_{S_2^1}, f_{S_2^1}^{\square}, f_{S_2^1}^{\bigcirc})$ such that for all w' with $\overline{s} \not\xrightarrow{w'} s^2$ it holds $f_{S_2^1}^{\square}(w') = f_{S_1^n}^{\square}(w')$, $f_{S_2^1}^{\bigcirc}(w') = f_{S_1^n}^{\bigcirc}(w')$, and $f_{S_2^1}^{\square}(w^2) = f_{S_1^n}^{\square}(w^2) \setminus \{a\}$, $f_{S_2^1}^{\bigcirc}(w^2) = \{a\}$. By Lemma 4, since $S_1^n \preceq_n T$, $a \in f_{S_1^n}^{\square}(w^2)$ and $a \notin f_T^{\square}(w^2)$, it holds $S_2^1 \preceq_n T$. At the end of the second (external) iteration we obtain an NMTS S_2^m where $m = |f_S^{\bigcirc}(w^2)|$ such that $f_{S_2^m}^{\square}(w^i) = f_S^{\square}(w^i)$, $f_{S_2^m}^{\bigcirc}(w^i) = f_S^{\bigcirc}(w^i)$ for $i \in \{1, 2\}$.

Every subsequent (external) iteration starts by reusing the last NMTS computed at the previous (external) iteration. Let $o = |P|$ (recall that we incremented the external counter also when skipping some element of P), and $p = |f_S^{\bigcirc}(w^o)|$, where w^o is the trace selected at the last, o-th iteration of the procedure. The returned NMTS $S_o^p = (Q_S, A_S, \overline{s}, \Delta_{S_o^p}, f_{S_o^p}^{\square}, f_{S_o^p}^{\bigcirc})$ is such that for all $w \in A_S^*$, $f_{S_o^p}^{\square}(w) = f_S^{\square}(w)$, $f_{S_o^p}^{\bigcirc}(w) = f_S^{\bigcirc}(w)$, and by Definition 3, $\Delta_{S_o^p} = \Delta_S$. Therefore, $S_o^p = S$. It follows that $S \preceq_n T$. □

A practical consequence of Theorem 3 is that the complexity of deciding $Impl_n(S) \subseteq Impl_n(T)$ is equivalent to the complexity of deciding $S \preceq_n T$.

4 Non-determinism of NMTS is Non-reducible

In the previous section, we showed how the further constraints imposed on MTS and their refinement (i.e., Definition 3 and Definition 4) are necessary and sufficient to obtain a sound and complete refinement relation. An important challenge discussed in [12] is to argue that the considered set of implementations is also interesting from a practical point of view (i.e., no valuable implementation is disregarded by $\preceq_n$).

In this section we discuss a property concerning non-deterministic optional transitions that is violated by all implementations accepted by $\preceq_m$ and discarded by $\preceq_n$. MTS allow to express transitions that must be enabled in all implementations. In this

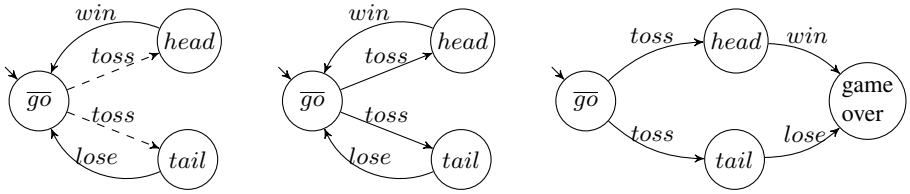

Fig. 6. From left to right, the NMTS modelling a coin toss game, an NMTS implementation allowing infinite plays, an NMTS implementation allowing one play.

case, the presence of non-determinism is unaltered in all implementations, because must transitions cannot be disabled. Conversely, optional transitions can be arbitrarily disabled, and in MTS the non-determinism in optional branches can be reduced or fully resolved. However, the standard semantics of MTS do not provide the means to specify actions that are susceptible to both enablement and disablement, yet inevitably yield non-deterministic outcomes. This issue arises since any action capable of being deactivated (i.e., an optional action) also opens the possibility of diminishing its associated non-determinism. We term the property stating that all optional actions in an MTS can be enabled or disabled, while retaining their irreducible non-determinism, as *non-reducible non-determinism*.

In formal specifications expressed as MTS, non-determinism is commonly used to express under-specifications. This variant of non-determinism does not necessitate preservation across all implementations of an MTS. Consequently, modal refinement can reduce the non-determinism to fully determine a specification, i.e., modal refinement does not satisfy the non-reducible non-determinism property (see, e.g., Figure 5). There exists a distinction between non-determinism present in all implementations (as showed in the next example) and the non-determinism that characterizes under-specifications. However, both these forms of non-determinism are expressed in an identical way within MTS. This inherent ambiguity contributes to the incompleteness of modal refinement. To address this, we assume that non-deterministic behaviour of MTS is always preserved across all implementations, thereby eliminating non-determinism as a source of under-specification. Consequently, NMTS refinement satisfies the property of non-reducible non-determinism, whilst this is not the case for modal refinement.

In the following, we discuss an example showcasing the need to establish the non-reducible non-determism property. Consider the NMTS in Figure 6 (left). This NMTS serves as a model for a coin toss game. We visualize the actions of this NMTS as buttons that light up and can only be pressed when the respective action becomes enabled. Upon pressing an enabled button, the associated action is carried out.

Initially, only one action, namely $toss$, is enabled. Upon executing the $toss$ action, the outcome can result in either head or tail. If the outcome is head, the win action becomes enabled, while in the case of tail, the $lose$ action is enabled. Upon the execution of either win or $lose$, the NMTS reverts back to its initial state. The NMTS does not specify whether the coin is biased.

The $toss$ action exemplifies the property of non-reducible non-determinism. In essence, any implementation that enables the $toss$ action must consistently manifest

the same non-deterministic behavior. Notably, the $toss$ action can be deactivated. An implementation that restricts the coin's outcomes solely to either heads or tails is considered invalid. However, under the standard modal refinement $\preceq_m$, such invalid implementations are deemed acceptable. Figure 6 (center and right) depicts two valid implementations of the NMTS. In one, an indefinite number of plays are feasible, while in the other, only a single play is permitted. Both these implementations are preserving the non-determinisc nature of the $toss$ action.

The introduced NMTS refinement (see Definition 4) exclusively permits implementations like the one showcased in Figure 6 whilst forbidding invalid implementations as those forcing the coin to only return either head or tail. Clearly, by relaxing the constraints in either Definition 3 or Definition 4, it is possible to define systems whose implementations may violate the non-reducible non-determinism property (see Section 3).

5 Related Work

MTS and their dialects are widely studied in the literature. Given two MTS S and T, S is a thorough refinement of T whenever the set of implementations of S is included in the set of implementations of T. In [12], four different refinement relations are studied extensively, including thorough refinement, and an MTS is said to be *consistent* if it admits at least one non-empty implementation. MTS that allow inconsistent specifications, where transitions can be necessary but not permitted, are called Mixed Transition Systems [8,1].

In [7, Corollary 4.6], it is proved that, similarly to modal refinement, thorough refinement is decidable in polynomial time for deterministic MTS, whilst thorough refinement is decidable in EXPTIME for non-deterministic MTS. The authors describe a tableau-style algorithm [7, Section 6] for deciding thorough refinement, which runs in exponential time in the worst case. While thorough refinement does not always imply modal refinement of MTS, in [6, Lemma 3.6] it is proved that thorough refinement implies modal refinement of a deterministic overapproximation of (non-deterministic) MTS.

In [12, Theorem 3], it is proved that any alternative notion $\preceq_{alt}$ of modal refinement that is both sound and complete cannot be decided in polynomial time unless $P = NP$. This is obtained by reducing the problem of deciding thorough refinement to the problem of deciding whether a 3-DNF formula is a tautology. However, in this case, thorough refinement considers all implementations obtained through modal refinement $\preceq_m$, and not only those obtained using the alternative notion $\preceq_{alt}$. The problem of proposing an alternative notion of modal refinement that is both sound and complete with respect to its set of implementations is left open [12]. The main challenge is to argue that the considered set of implementations is also interesting from a practical point of view. In this paper, we addressed this challenge and discussed how all implementations retained by $\preceq_m$ and discarded by $\preceq_n$ are violating the non-reducible non-determinsm property (see Section 4).

Parametric MTS (PMTS) [5,11,4] were introduced to enhance the expressiveness of MTS. PMTS are LTS equipped with an obligation function Φ, which is a parametric Boolean proposition over the outgoing transitions from each state. The satisfying as-

signments of Φ yield the allowed combinations of outgoing transitions. When Φ is not parametric, PMTS are called Boolean MTS (BMTS). PMTS are capable of expressing, among others, *persistent* choices (i.e., once some outgoing transition is enabled, it must be enabled also everywhere else). It is shown that MTS are a special case of BMTS, and that BMTS are a special case of PMTS. Rather than extending MTS, in this paper we presented a subset of MTS for which a sound and complete refinement relation is proposed. Thorough refinement is computable in NEXPTIME for both BMTS and PMTS, while we show in this paper that thorough refinement is polynomial for NMTS. Modal refinement of MTS, BMTS, and PMTS is not complete, whereas we show in this paper that NMTS refinement is complete (Lemma 3). The deterministic variants of PMTS and BMTS are called, respectively, DPMTS and DBMTS. When restricting to only deterministic systems, similarly to NMTS, also DBMTS modal refinement is complete, whereas DPMTS modal refinement is still not complete.

In [2,3], Coherent MTS (CMTS) are introduced as a model for software product lines (SPL). In CMTS, the features of an SPL are identified with the actions of an MTS. Therefore, in CMTS an action cannot be the label of both a necessary and an optional transition, since a feature is either mandatory or optional. The notion of 'consistent' product derivation requires that whenever an optional transition is discarded in an implementation, all transitions sharing the same label must also be discarded. This consistency requirement mimicks the aforementioned persistency of PMTS [5,11,4] and it is not to be confused with the above mentioned notion of consistency as studied in [12]. In [2] the refinement of CMTS is presented, which is demonstrated to be both sound and complete in relation to its set of implementations.

CMTS and their refinement [2] are an important milestone in addressing the long-standing problem proposed at CONCUR 2007 [12]. NMTS and CMTS are currently the only available subsets of MTS that possess the capacity to preserve both non-deterministic specifications and completeness of the refinement relation. In contrast, all the other MTS extensions mentioned above do not possess completeness of refinement in the case of non-deterministic specifications. In CMTS, by interpreting SPL features as MTS actions, 'consistency' and 'coherence' are enforced globally across all system states. NMTS are a generalization of CMTS. In NMTS, the SPL-derived limitations are discarded (i.e., actions are not interpreted as features of an SPL). The constraints that in CMTS are applied globally, in NMTS are instead applied exclusively to the set of states reachable through the same sequence of actions. Consequently, NMTS strictly include CMTS while introducing a refinement concept that remains sound and complete. Differently from the restrictions imposed by CMTS and their refinement, in Section 3, we identified the restrictions imposed by NMTS and their refinement as necessary to achieve completeness in the refinement relation. Furthermore, in Section 4 we presented a property that is violated by all implementations discarded by the NMTS refinement relation but accepted through modal refinement.

6 Conclusion

We have introduced a subset of Modal Transition Systems (MTS) called Non-reducible MTS (NMTS) and their refinement relation ($\preceq_n$).

In NMTS, states reached through the execution of identical action sequences are related. Outgoing transitions from related states that are labeled by the same action also exhibit the same modality. Disabling an optional transition within a refinement results in the deactivation of all transitions that share both the same action label and are outgoing from related states. We showed that these two conditions are necessary to achieve completeness. If either of these conditions is relaxed, it becomes possible to construct two systems that are not in refinement relation, yet their respective sets of implementations still maintain a relation of set inclusion. We proved that $\preceq_n$ is both sound and complete with respect to its set of implementations. By interpreting the optional non-determinism present in MTS as non-reducible (i.e., non-deterministic behaviour within MTS is consistently maintained in all implementations), we have showed that all implementations permitted by $\preceq_m$ (modal refinement) but rejected by $\preceq_n$ are considered invalid.

Future work In Section 4, we investigated optional non-determinism of MTS, which can be interpreted in two distinct ways: as either under-specifications or optional actions with irreducible non-determinism across all implementations. To resolve this ambiguity and the challenge posed by [12], we opted to associate the latter interpretation with non-deterministic optional actions. However, this decision brings forth a new challenge: introducing the means to express under-specifications while preserving the completeness of the refinement relation requires further investigations.

References

1. Antonik, A., Huth, M., Larsen, K.G., Nyman, U., Wąsowski, A.: 20 Years of Modal and Mixed Specifications. B. EATCS **95**, 94–129 (2008), https://vbn.aau.dk/files/16474238/BEATCS2008.pdf
2. Basile, D., ter Beek, M.H., Fantechi, A., Gnesi, S.: Coherent modal transition systems refinement, submitted for publication
3. ter Beek, M.H., Fantechi, A., Gnesi, S., Mazzanti, F.: Modelling and analysing variability in product families: Model checking of modal transition systems with variability constraints. J. Log. Algebr. Meth. Program. **85**(2), 287–315 (2016). https://doi.org/10.1016/j.jlamp.2015.11.006
4. Beneš, N., Křetínský, J., Larsen, K.G., Møller, M.H., Sickert, S., Srba, J.: Refinement checking on parametric modal transition systems. Acta Inform. **52**(2-3), 269–297 (2015). https://doi.org/10.1007/s00236-015-0215-4
5. Beneš, N., Křetínský, J., Larsen, K.G., Møller, M.H., Srba, J.: Parametric Modal Transition Systems. In: Bultan, T., Hsiung, P. (eds.) Proceedings 9th International Symposium on Automated Technology for Verification and Analysis (ATVA'11). LNCS, vol. 6996, pp. 275–289. Springer (2011). https://doi.org/10.1007/978-3-642-24372-1_20
6. Beneš, N., Křetínský, J., Larsen, K.G., Srba, J.: On determinism in modal transition systems. Theor. Comput. Sci. **410**(41), 4026–4043 (2009). https://doi.org/10.1016/j.tcs.2009.06.009
7. Beneš, N., Křetínský, J., Larsen, K.G., Srba, J.: EXPTIME-completeness of thorough refinement on modal transition systems. Inf. Comput. **218**, 54–68 (2012). https://doi.org/10.1016/j.ic.2012.08.001
8. Dams, D., Gerth, R., Grumberg, O.: Abstract Interpretation of Reactive Systems. ACM Trans. Program. Lang. Syst. **19**(2), 253–291 (1997). https://doi.org/10.1145/244795.244800

9. Keller, R.M.: Formal Verification of Parallel Programs. Commun. ACM **19**(7), 371–384 (1976). https://doi.org/10.1145/360248.360251
10. Křetínský, J.: 30 Years of Modal Transition Systems: Survey of Extensions and Analysis. In: Aceto, L., Bacci, G., Bacci, G., Ingólfsdóttir, A., Legay, A., Mardare, R. (eds.) Models, Algorithms, Logics and Tools, LNCS, vol. 10460, pp. 36–74. Springer (2017). https://doi.org/10.1007/978-3-319-63121-9_3
11. Kretínský, J., Sickert, S.: On Refinements of Boolean and Parametric Modal Transition Systems. In: Liu, Z., Woodcock, J., Zhu, H. (eds.) Proceedings 10th International Colloquium on Theoretical Aspects of Computing (ICTAC'13). LNCS, vol. 8049, pp. 213–230. Springer (2013). https://doi.org/10.1007/978-3-642-39718-9_13
12. Larsen, K.G., Nyman, U., Wąsowski, A.: On Modal Refinement and Consistency. In: Caires, L., Vasconcelos, V.T. (eds.) Proceedings 18th International Conference on Concurrency Theory (CONCUR'07). LNCS, vol. 4703, pp. 105–119. Springer (2007). https://doi.org/10.1007/978-3-540-74407-8_8
13. Larsen, K.G., Thomsen, B.: A Modal Process Logic. In: Proceedings 3rd Symposium on Logic in Computer Science (LICS'88). pp. 203–210. IEEE (1988). https://doi.org/10.1109/LICS.1988.5119