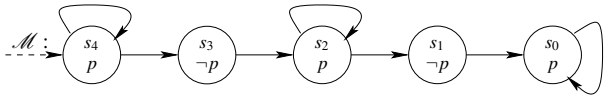

Fig. 5 Systems $\mathscr{M}_i$ that satisfy $\diamondsuit\Box p$.

assumption of black-box checking [29]. Clearly, this combination of universal and existential path quantification is impossible to express in LTL.

6 CTL*

As mentioned in the previous section, LTL and CTL are different. However, in order to compare them formally, we have to reason about the same sets of models. In order to do that, we think about both LTL and CTL as characterizing sets of FDSs. We then show that LTL and CTL are uncomparable. We show families of models that can be distinguished by LTL formulas and no CTL formula can distinguish and vice versa. This leads to the definition of CTL*, an expressive logic that combines both LTL and CTL. Effectively, it combines the full LTL with the path quantifiers introduced in CTL.

6.1 Branching vs. Linear time

As explained, models of LTL formulas are infinite sequences and models of CTL formulas are FDSs. In order to be able to compare the two, we consider the definition of implementation for both logics. We show that some formulas in LTL cannot be expressed in CTL and some formulas in CTL cannot be expressed in LTL.

We start by showing that LTL can express properties that cannot be expressed in CTL. Specifically, the formula $\diamondsuit\Box p$ cannot be expressed in CTL. As we explain below, the natural CTL candidate to express the same property is $\mathbf{A}\diamondsuit(\mathbf{A}\Box(p))$. However, the latter requires that p starts holding in all futures simultaneously, which is more than the LTL formula stipulates. We define a a family of systems $\mathscr{M}$ such that $\diamondsuit\Box p$ holds over $\mathscr{M}$. We show that every CTL formula that holds over all the systems in $\mathscr{M}$ must hold also over a system that falsifies $\diamondsuit\Box p$. The system is depicted in Fig. 5. For convenience, we depict all the family $\mathscr{M}$ as one infinite state system, however, every instance in the family includes a finite number of states. Formally, using $a \dot{-} b \equiv \mathsf{max}(0, a-b)$ we set $\mathscr{M}_i = \langle \{p, y\}, \rho_i, p \wedge y = i \rangle$, where p is a Boolean variable and y ranges over $\{0, \ldots, i\}$ and ρ_i is defined as follows.

$$\rho_i \equiv (p \rightarrow y = y') \wedge (\neg p \rightarrow y' = y \dot{-} 1) \wedge ((p \wedge y > 0) \vee p')$$

It is simple to see that for $j \geq 1$ state s_{2j-1} corresponds to the valuation $y = j$ and $\neg p$ and for $j \geq 0$ state s_{2j} corresponds to the valuation $y = j$ and p. Also, every infinite path eventually remains in state s_{2j} for some j. Hence, every infinite path satisfies $\Box \diamondsuit p$ and every system $\mathscr{M}_i$ satisfies the LTL formula $\diamondsuit \Box p$.

We now show that this cannot be the case for a CTL formula.

Lemma 6. *For every* CTL *formula* φ *such that forall* $i \geq 0$ *we have* $\mathscr{M}_i, t_{2i} \models \varphi$ *there is a system* $\mathscr{N}$ *such that* $\mathscr{N} \models \varphi$ *and* $\mathscr{N} \not\models \diamondsuit \Box p$.

Proof. Let n be the number of subformulas of φ and let m denote 2^n. Consider the system $\mathscr{M}_m$. We are going to identify two states t_{2i} and t_{2j} for $i < j \leq m$ such that the set of subformulas of φ that hold in t_{2i} and t_{2j} is identical. Furthermore, we are going to identify a path between t_{2i} and t_{2j} such that all universal eventualities that should be true in t_{2i} are fulfilled before arriving to t_{2j} and all existential eventualities that should be true in t_{2i} are fulfilled on paths that diverge from this identified path. Then, we create a modified system where this specific path between t_{2i} and t_{2j} is closed to a loop. Clearly, this path falsifies the LTL formula $\diamondsuit \Box p$. However, from the construction of this path, all subformulas of φ that hold in t_{2m} still hold in the modified system. In particular, φ holds in t_{2m} showing that φ cannot be equivalent to $\diamondsuit \Box p$.

We modify the system $\mathscr{M}_m$ as follows. Consider the state t_{2m} and let C_m be the set of subformulas of φ that hold in t_{2m}. Consider subformula $\psi \in C_m$ of the form $\psi = \mathbf{A}(\psi_1 \mathscr{U} \psi_2)$. As ψ holds in t_{2m} it must be the case that ψ_2 holds in t_{2m}, otherwise ψ does not hold on the path $t_{2m}, t_{2m}, t_{2m}, \ldots$. Consider the set of subformulas of the form $\mathbf{E}\bigcirc(\psi_1)$ or $\mathbf{E}(\psi_1 \mathscr{U} \psi_2)$ that hold in t_{2m}. There is a finite set of paths that start in t_{2m} and show satisfaction of all existential path formulas. Of all these paths, there is a maximal number k_m of repetitions of the state t_{2m} on a path. Let $\mathscr{N}_m$ denote the system that is obtained from $\mathscr{M}_m$ by replacing the state t_{2m} by a chain of states $t_{2m}^1, \ldots, t_{2m}^{k_m}$ such that t_{2m}^j is connected to t_{2m}^{j-1} and to a copy of $\mathscr{M}_{m-1}$. Clearly, all formulas of C_m still hold over $\mathscr{N}_m$ and all eventualities that are promised in t_{2m}^1 are fulfilled before arriving to $t_{2m}^{k_m}$.

We now modify $\mathscr{N}_m$ by changing the copy of t_{2m-2} that is connected $t_{2m}^{k_m}$ to create $\mathscr{N}_{m-1}$ by the same process. We repeat this process until at some point, we find that the set of subformulas of φ that hold in t_{2i} is equivalent to C_m. Then, we simply connect t_{2m}^1 instead of t_{2i} and create a loop.

The modified system still satisfies all CTL formulas that are promised to hold in C_m and in particular φ.

Our proof is based on Rabin's result about expressiveness of tree automata [35]. An alternative proof based on systems with fairness constraints is available in [7].

Corollary 2. CTL *is not as expressive as* LTL.

We now show that LTL is not as expressive as CTL, establishing the two as incomparable. As a first observation, an existential formula cannot be expressed in LTL. However, this seems less than satisfying as it may be the negation of an LTL formula.