Logical Methods in Computer Science
Vol. 5 (4:5) 2009, pp. 1–24
www.lmcs-online.org

Submitted Oct. 6, 2008
Published Dec. 22, 2009

COMPUTATION TREE LOGIC WITH DEADLOCK DETECTION

ROB VAN GLABBEEK [a], BAS LUTTIK [b], AND NIKOLA TRČKA [c]

[a] National ICT Australia, and School of Comp. Sc. and Engineering, University of New South Wales, Sydney, Australia
e-mail address: rvg@cs.stanford.edu

[b,c] Dept. of Math. & Comp. Sc., Technische Universiteit Eindhoven, The Netherlands
e-mail address: {s.p.luttik,n.trcka}@tue.nl

Abstract. We study the equivalence relation on states of labelled transition systems of satisfying the same formulas in Computation Tree Logic without the next state modality ($\mathsf{CTL}_{-\mathsf{X}}$). This relation is obtained by De Nicola & Vaandrager by translating labelled transition systems to Kripke structures, while lifting the totality restriction on the latter. They characterised it as divergence sensitive branching bisimulation equivalence.

We find that this equivalence fails to be a congruence for interleaving parallel composition. The reason is that the proposed application of $\mathsf{CTL}_{-\mathsf{X}}$ to non-total Kripke structures lacks the expressiveness to cope with deadlock properties that are important in the context of parallel composition. We propose an extension of $\mathsf{CTL}_{-\mathsf{X}}$, or an alternative treatment of non-totality, that fills this hiatus. The equivalence induced by our extension is characterised as branching bisimulation equivalence with explicit divergence, which is, moreover, shown to be the coarsest congruence contained in divergence sensitive branching bisimulation equivalence.

1. Introduction

CTL^* [7] is a powerful state-based temporal logic combining linear time and branching time modalities; it generalises the branching time temporal logic CTL [6]. CTL^* is interpreted in terms of Kripke structures, directed graphs together with a labelling function assigning to every node of the graph a set of atomic propositions. As the *next state* modality X is incompatible with abstraction of the notion of state, it is often excluded in high-level specifications. By $\mathsf{CTL}^*_{-\mathsf{X}}$ we denote CTL^* without this modality. To characterise the equivalence induced on states of Kripke structures by validity of $\mathsf{CTL}^*_{-\mathsf{X}}$ formulas, Browne, Clarke & Grumberg [3] defined the notion of *stuttering equivalence*. They proved that two states in a finite Kripke structure are stuttering equivalent if and only if they satisfy the same $\mathsf{CTL}^*_{-\mathsf{X}}$ formulas, and moreover, they established that this is already the case if and only if the two states satisfy the same $\mathsf{CTL}_{-\mathsf{X}}$ formulas.

1998 ACM Subject Classification: F.4.1, D.2.4.

Key words and phrases: temporal logic, deadlock, parallel composition, stuttering equivalence, branching bisimulation equivalence, explicit divergence.

DOI:10.2168/LMCS-5 (4:5) 2009

There is an intuitive correspondence between the notions of stuttering equivalence on Kripke structures and *branching bisimulation equivalence* [10] on labelled transition systems (LTSs), directed graphs of which the edges are labelled with actions. De Nicola & Vaandrager [5] have provided a framework for constructing natural translations between LTSs and Kripke structures in which this correspondence can be formalised. Stuttering equivalence corresponds in their framework to a *divergence sensitive* variant of branching bisimulation equivalence, and conversely, branching bisimulation equivalence corresponds to a *divergence blind* variant of stuttering equivalence. The latter characterises the equivalence induced on states of Kripke structures by a divergence blind variant of validity of $\mathsf{CTL}^*_{-\mathsf{X}}$ formulas.

In [6, 7, 3] and other work on CTL^*, Kripke structures are required to be *total*, meaning that every state has an outgoing transition. These correspond with LTSs that are *deadlock-free*. In the world of LTSs requiring deadlock-freeness is considered a serious limitation, as deadlock is introduced by useful process algebraic operators like the *restriction* of CCS and the *synchronous parallel composition* of CSP. Conceptually, a deadlock may arise as the result of an unsuccessful synchronisation attempt between parallel components, and often one wants to verify that the result of a parallel composition is deadlock-free. This is, of course, only possible when working in a model of concurrency where deadlocks can be expressed.

Through the translations of [5] it is possible to define the validity of $\mathsf{CTL}^*_{-\mathsf{X}}$ formulas on states of LTSs. To apply $\mathsf{CTL}^*_{-\mathsf{X}}$-formulas to LTSs that may contain deadlocks, De Nicola & Vaandrager [5] consider Kripke structures with deadlocks as well, and hence lift the requirement of totality. They do so by using maximal paths instead of infinite paths in the definition of validity of $\mathsf{CTL}^*_{-\mathsf{X}}$ formulas. Without further changes, this amounts to the addition of a self-loop to every deadlock state. As a consequence, $\mathsf{CTL}^*_{-\mathsf{X}}$ formulas cannot see the difference between a state without outgoing transitions (a *deadlock*) and one whose only outgoing transition constitutes a self-loop (a *livelock*), and accordingly a deadlock state is stuttering equivalent to a livelock state that satisfies the same atomic propositions. This paper will challenge the wisdom of this set-up.

We observe that for systems with deadlock, the divergence sensitive branching bisimulation equivalence of [5] fails to be a congruence for interleaving operators. We characterise the coarsest congruence contained in divergence sensitive branching bisimulation equivalence as the *branching bisimulation equivalence with explicit divergence* introduced in [10]. This equivalence differs from divergence sensitive branching bisimulation equivalence in that it distinguishes deadlock and livelock. For deadlock-free systems the equivalences coincide.

Having established that the framework of [5] turns $\mathsf{CTL}^*_{-\mathsf{X}}$ into a logic on LTSs that induces an equivalence under which interleaving parallel composition fails to be compositional, we propose two adaptations to this framework that both make $\mathsf{CTL}^*_{-\mathsf{X}}$ induce branching bisimulation equivalence with explicit divergence and thus restore compositionality. Our first adaptation preserves the treatment of non-totality of [5] as well as their translations between LTSs and Kripke structures, but extends the language $\mathsf{CTL}^*_{-\mathsf{X}}$ so that it can distinguish deadlock from successful termination. Our second adaptation preserves the totality requirement on Kripke structures but modifies the translation from LTSs to Kripke structures. One of our main results is that both adaptations are equivalent in the sense that they induce equally expressive logics on LTSs. In the following two paragraphs we discuss these adaptations in more detail.

That divergence sensitive branching bisimulation equivalence is not a congruence for interleaving operators means that there are properties of concurrent systems, pertaining to their deadlock behaviour, that (in the framework of [5]) cannot be expressed in $\mathsf{CTL}^*_{-\mathsf{X}}$, but that can be expressed in terms of the validity of a $\mathsf{CTL}^*_{-\mathsf{X}}$ formula on the result of putting these systems in a given context involving an interleaving operator. We find this unsatisfactory, and therefore propose an extension of $\mathsf{CTL}^*_{-\mathsf{X}}$ in which this type of property can be expressed directly. We obtain that two states are branching bisimulation equivalent with explicit divergence if and only if they satisfy the same formulas in the resulting logic. Treating $\mathsf{CTL}_{-\mathsf{X}}$ in the same way leads either to an extension of $\mathsf{CTL}_{-\mathsf{X}}$ or, equivalently, to a modification of its semantics. The new semantics we propose for $\mathsf{CTL}_{-\mathsf{X}}$ is a valid extension of the original semantics [6] to non-total Kripke structures. It slightly differs from the semantics of [5] and it is arguably better suited to deal with deadlock behaviour.

Instead of extending $\mathsf{CTL}^*_{-\mathsf{X}}$ or modifying $\mathsf{CTL}_{-\mathsf{X}}$ we also achieve the same effect by amending the translation from LTSs to Kripke structures in such a way that every LTS maps to a total Kripke structure. This amended translation consist of any of the translations in the framework of [5] followed by a postprocessing stage introducing a fresh state s_δ, labelled by a fresh atomic proposition expressing the property of having deadlocked, and a transition from all deadlock states, and s_δ itself, to s_δ. Adding self-loops and a fresh atomic proposition expressing deadlock (or just a fresh atomic proposition expressing deadlock) to deadlock states themselves does not have the desired effect, for it yields logics that are too expressive.

From the point of view of practical applications our work allows the rich tradition of verification by equivalence checking to be combined with the full expressive power of $\mathsf{CTL}^*_{-\mathsf{X}}$. In equivalence checking, three properties of the chosen equivalence have been found indispensable [2]: compositionality—in particular parallel composition being a congruence—is a crucial requirement to combat the state explosion problem; the ability to represent deadlock is crucial in ascertaining deadlock-freedom; and abstraction from internal activity—and thus from the concept of a "next state"—is crucial to get a firm grasp of correctness. Our work is the first that allows specification by arbitrary $\mathsf{CTL}^*_{-\mathsf{X}}$ formulas to be incorporated in this framework, without giving up any of these essential properties.

Given the existence of adequate translations between LTSs and Kripke structures, we could have presented the results of this paper entirely within the framework of Kripke structures, or entirely within the framework of LTSs. Using Kripke structures only would entail defining a parallel composition on Kripke structures—which is possible by lifting the parallel composition on LTSs through the appropriate translations. However, Kripke structures are traditionally used for global descriptions of systems; building system descriptions modularly by parallel composition, while worrying about deadlocks that may be introduced in this process, would be a novel approach in itself. For establishing the results of this paper it is much more appropriate to build on the rich tradition of composing LTSs by parallel composition, and the known importance of deadlock behaviour within this framework.

Using just LTSs, on the other hand, would require lifting $\mathsf{CTL}^*_{-\mathsf{X}}$ to the world of LTSs.[1] Here we could build on the work of De Nicola and Vaandrager [4], who defined the logic ACTL^* on LTSs and showed that it corresponds neatly, through the translations of [5],

[1] A tempting alternative appears to be to use the *weak modal μ-calculus* [15] instead of $\mathsf{CTL}^*_{-\mathsf{X}}$. This is the modal μ-calculus of Kozen [12] with *weak* action modalities $\langle\langle\alpha\rangle\rangle$ and $[\![a]\!]$ instead of $\langle a\rangle$ and $[a]$ in order to abstract from internal activity. However, as observed in [15], this logic cannot distinguish states that are *weakly bisimilar*, and hence, contrary to what is suggested in the introduction of [15], lacks the expressiveness of $\mathsf{CTL}^*_{-\mathsf{X}}$.

with CTL^* on Kripke structures. However, whereas abstracting from the notion of state in CTL^* can be done elegantly by removing the next state modality X from the language, in ACTL^* this additionally requires parametrising the *until*-modality by two *action formulas* [4]. Doing this would make the resulting logic $\mathsf{ACTL}^*_{-\mathsf{X}}$ appear less than a wholly canonical action-based incarnation of $\mathsf{CTL}^*_{-\mathsf{X}}$, and the reader might wonder whether the failure of $\mathsf{ACTL}^*_{-\mathsf{X}}$ to generate an equivalence on LTSs that is a congruence for parallel composition would be due to it being an imperfect rendering of $\mathsf{CTL}^*_{-\mathsf{X}}$ in the action-based world.

By presenting our analysis directly for $\mathsf{CTL}^*_{-\mathsf{X}}$, we make clear that this is not the case, and the problem stems from $\mathsf{CTL}^*_{-\mathsf{X}}$ itself. Having to work in both LTSs and Kripke structures, with translations between them, appears to be a small price to pay. In addition, we feel that in many applications, such as process algebra with data, in may be preferable to work directly in a model of concurrency that features both state and action labels, and thus benefits from the ability to smoothly combine LTSs and Kripke structures [16].

Nevertheless, all our work applies just as well to $\mathsf{ACTL}^*_{-\mathsf{X}}$, with the very same problems and the very same solutions.

At the end of the paper we briefly consider Linear Temporal Logic without the next state modality ($\mathsf{LTL}_{-\mathsf{X}}$). The equivalence induced by the validity of $\mathsf{LTL}_{-\mathsf{X}}$-formulas is not a congruence for interleaving parallel composition either. The coarsest coarsest congruence included in the equivalence induced by the validity of $\mathsf{LTL}_{-\mathsf{X}}$-formulas is obtained much in the same way as the coarsest congruence included in the equivalence induced by the validity of $\mathsf{CTL}_{-\mathsf{X}}$-formulas. Adding the ∞-modality to $\mathsf{LTL}_{-\mathsf{X}}$, however, yields a logic that induces a strictly finer equivalence than the obtained congruence.

2. $\mathsf{CTL}^*_{-\mathsf{X}}$ and stuttering equivalence

We presuppose a set $\mathbf{AP}$ of *atomic propositions*. A *Kripke structure* is a tuple $(S, \mathscr{L}, \rightarrow)$ consisting of a set of states S, a *labelling function* $\mathscr{L}\colon S \to 2^{\mathbf{AP}}$ and a *transition relation* $\rightarrow \subseteq S \times S$. For the remainder of the section we fix a Kripke structure $(S, \mathscr{L}, \rightarrow)$.

A *finite path* from s is a finite sequence of states $s_0, \ldots, s_n$ such that $s = s_0$ and $s_k \longrightarrow s_{k+1}$ for all $0 \leq k < n$. An *infinite path* from s is an infinite sequence of states $s_0, s_1, s_2, \ldots$ such that $s = s_0$ and $s_k \longrightarrow s_{k+1}$ for all $k \in \omega$. A *path* is a finite or infinite path. A *maximal path* is an infinite path or a finite path $s_0, \ldots, s_n$ such that $\neg\exists s'.\ s_n \longrightarrow s'$. We write $\pi \trianglerighteq \pi'$ if the path π' is a suffix of the path π, and $\pi \triangleright \pi'$ if $\pi \trianglerighteq \pi'$ and $\pi \neq \pi'$.

Temporal properties of states in S are defined using $\mathsf{CTL}^*_{-\mathsf{X}}$ formulas.

Definition 2.1. The classes Φ of $\mathsf{CTL}^*_{-\mathsf{X}}$ *state formulas* and Ψ of $\mathsf{CTL}^*_{-\mathsf{X}}$ *path formulas* are generated by the following grammar:

$$\varphi ::= \ p \ \mid \ \neg\varphi \ \mid \ \bigwedge \Phi' \ \mid \ \exists\psi \qquad\qquad \psi ::= \ \varphi \ \mid \ \neg\psi \ \mid \ \bigwedge \Psi' \mid \ \psi \,\mathsf{U}\, \psi$$

with $p \in \mathbf{AP}$, $\varphi \in \Phi$, $\Phi' \subseteq \Phi$, $\psi \in \Psi$ and $\Psi' \subseteq \Psi$.

In case the cardinality of the set of states of our Kripke structure is less than some infinite cardinal κ,[2] we may require that $|\Phi'| < \kappa$ and $|\Psi'| < \kappa$ in conjunctions, thus obtaining a *set* of formulas rather than a proper class. Normally, S is required to be finite, and accordingly $\mathsf{CTL}^*_{-\mathsf{X}}$ admits finite conjunctions only.

[2] In fact it suffices to require that for every state s the cardinality of the set of states reachable from s is less than κ.

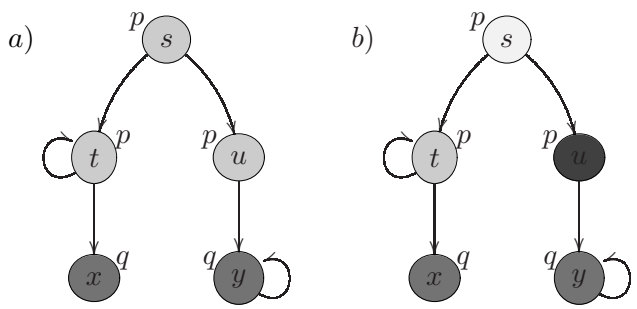

Figure 1: Difference between a) $\approx_{dbs}$ and b) $\approx_s$.

Definition 2.2. We define when a $\mathsf{CTL}^*_{-\mathsf{X}}$ state formula φ is *valid* in a state s (notation: $s \models \varphi$) and when a $\mathsf{CTL}^*_{-\mathsf{X}}$ path formula ψ is *valid* on a maximal path π (notation: $\pi \models \psi$) by simultaneous induction as follows:

- $s \models p$ iff $p \in \mathscr{L}(s)$;
- $s \models \neg\varphi$ iff $s \not\models \varphi$;
- $s \models \bigwedge \Phi'$ iff $s \models \varphi$ for all $\varphi \in \Phi'$;
- $s \models \exists\psi$ iff there exists a maximal path π from s such that $\pi \models \psi$;
- $\pi \models \varphi$ iff s is the first state of π and $s \models \varphi$;
- $\pi \models \neg\psi$ iff $\pi \not\models \psi$;
- $\pi \models \bigwedge \Psi'$ iff $\pi \models \psi$ for all $\psi \in \Psi'$; and
- $\pi \models \psi \,\mathsf{U}\, \psi'$ iff there exists a suffix π' of π such that $\pi' \models \psi'$, and $\pi'' \models \psi$ for all $\pi \trianglerighteq \pi'' \rhd \pi'$.

A formula $\psi \,\mathsf{U}\, \psi'$ says that, along a given path, ψ holds *until* ψ' holds. One writes $\top$ for the empty conjunction (which is always valid), $\mathsf{F}\psi$ for $\top \,\mathsf{U}\, \psi$ ("ψ will hold *eventually*") and $\mathsf{G}\psi$ for $\neg\mathsf{F}\neg\psi$ ("ψ holds *always* (along a path)").

The above is the standard interpretation of $\mathsf{CTL}^*_{-\mathsf{X}}$ [7, 3], but extended to Kripke structures that are not required to be total. Following [5], this is achieved by using maximal paths in the definition of validity of $\mathsf{CTL}^*_{-\mathsf{X}}$ formulas, instead of the traditional use of infinite paths [7, 3]. The resulting definition generalises the traditional one, because for total Kripke structures a path is maximal iff it is infinite.

An equivalent way of thinking of this generalisation of $\mathsf{CTL}^*_{-\mathsf{X}}$ to non-total Kripke structures is by means of a transformation that makes a Kripke structure K total by the addition of a self-loop $s \longrightarrow s$ to every deadlock state s, together with the convention that a formula is valid in a state of K iff it is valid in the same state of the total Kripke structure obtained by this transformation. It is not hard to check that this yields the same notion of validity as our Definition 2.2.

The *divergence blind* interpretation of [5] (notation: $s \models_{db} \varphi$ and $\pi \models_{db} \psi$) is obtained by dropping the word "maximal" in the fourth clause of Definition 2.2. In contrast, we call the the standard interpretation *divergence sensitive*, because it does not abstract from *divergences*, i.e., infinite paths consisting of states with the same label. For instance, in Figure 1a we have $t \models \exists\mathsf{G}p$, due to the divergence $t, t, t, \ldots$, whereas $u \not\models \exists\mathsf{G}p$. Under the divergence blind interpretation there is no formula distinguishing these two states.

Definition 2.3. A *colouring* is a function $\mathcal{C} : S \to \mathbf{C}$, for $\mathbf{C}$ any set of *colours*.

Given a colouring $\mathcal{C}$ and a (finite or infinite) path $\pi = s_0, s_1, s_2, \ldots$ from s, let $\mathcal{C}(\pi)$ be the sequence of colours obtained from $\mathcal{C}(s_0), \mathcal{C}(s_1), \mathcal{C}(s_2), \ldots$ by contracting all its (finite or infinite) maximal consecutive subsequences $C, C, C, \ldots$ to C. The sequence $\mathcal{C}(\pi)$ is called a *$\mathcal{C}$-coloured trace* of s; it is *complete* if π is maximal.

A colouring $\mathcal{C}$ is *[fully] consistent* if two states of the same colour always satisfy the same atomic propositions and have the same [complete] $\mathcal{C}$-coloured traces. Two states s and t are *divergence blind stuttering equivalent*, notation $s \approx_{dbs} t$, if there exists a consistent colouring $\mathcal{C}$ such that $\mathcal{C}(s) = \mathcal{C}(t)$. They are *(divergence sensitive) stuttering equivalent*, notation $s \approx_s t$, if there exists a fully consistent colouring $\mathcal{C}$ such that $\mathcal{C}(s) = \mathcal{C}(t)$. The difference between $\approx_{dbs}$ and $\approx_s$ is illustrated in the following example.

Example 2.4. Consider the Kripke structure and its colouring depicted in Figure 1a. This colouring is consistent, implying $s \approx_{dbs} t \approx_{dbs} u$ and $x \approx_{dbs} y$, but it is not fully consistent because state t has a complete trace ● while u does not. Note that t has, due to the self-loop, a complete coloured trace that consists of just the colour of a p-labelled state, whereas the unique complete coloured trace of u contains the colour of a q-labelled state too. Since a consistent colouring assigns different colours to states with different labels, every fully consistent colouring must assign different colours to states t and u, i.e. it must be that $t \not\approx_s u$. One such colouring is given in Figure 1b. This colouring shows that $x \approx_s y$.

Lemma 2.5. *Let $\mathcal{C}$ be a colouring such that two states with the same colour satisfy the same atomic propositions and have the same $\mathcal{C}$-coloured traces of length two. Then $\mathcal{C}$ is consistent.*

Proof. Suppose $\mathcal{C}(s_0) = \mathcal{C}(t_0)$ and $C_0, C_1, C_2, \ldots$ is an infinite coloured trace of s_0. Then, for $i > 0$, there are states s_i and finite paths π_i from s_{i-1} to s_i, such that $\mathcal{C}(\pi_i) = C_{i-1}, C_i$. With induction on $i > 0$ we find states t_i with $C(s_i) = C(t_i)$ and finite paths ρ_i from t_{i-1} to t_i such that $\mathcal{C}(\rho_i) = C_{i-1}, C_i$. Namely, the assumption about $\mathcal{C}$ allows us to find ρ_i given t_{i-1}, and then t_i is defined as the last state of ρ_i. Concatenating all the paths ρ_i yields an infinite path ρ from t_0 with $\mathcal{C}(\rho) = C_0, C_1, C_2, \ldots$.

The case that $\mathcal{C}(s_0) = \mathcal{C}(t_0)$ and $C_0, \ldots, C_n$ is a finite coloured trace of s_0 goes likewise. □

Lemma 2.6. *Let $\mathcal{C}$ be a colouring such that two states with the same colour satisfy the same atomic propositions and have the same $\mathcal{C}$-coloured traces of length two, and the same complete $\mathcal{C}$-coloured traces of length one. Then $\mathcal{C}$ is fully consistent.*

Proof. Suppose $\mathcal{C}(s) = \mathcal{C}(t)$ and σ is a complete $\mathcal{C}$-coloured trace of s. Then $\sigma = \mathcal{C}(\pi)$ for a maximal path π from s. By Lemma 2.5, σ is also a $\mathcal{C}$-coloured trace of t. It remains to show that it is a *complete* $\mathcal{C}$-coloured trace of t. Let ρ be a path from t with $\mathcal{C}(\rho) = \sigma$. If ρ is infinite, we are done. Otherwise, let t' be the last state of ρ. Then $\mathcal{C}(t')$ is the last colour of σ. Therefore, there is a state s' on π such that the suffix π' of π starting from s' is a maximal path with $\mathcal{C}(\pi') = \mathcal{C}(s') = \mathcal{C}(t')$. By the assumption about $\mathcal{C}$, $\mathcal{C}(t')$ must also be a complete $\mathcal{C}$-coloured trace of t', i.e. there is a maximal path ρ' from t' with $\mathcal{C}(\rho') = \mathcal{C}(t')$. Concatenating ρ and ρ' yields a maximal path ρ'' from t with $\mathcal{C}(\rho'') = \sigma$. □

The following two theorems were proved in [5] and [3], respectively, for states s and t in a finite Kripke structure. Here we drop the finiteness restriction.

Theorem 2.7. *$s \approx_{dbs} t$ iff $s \models_{db} \varphi \Leftrightarrow t \models_{db} \varphi$ for all $\mathsf{CTL}^*_{-\mathsf{X}}$ state formulas φ.*

Proof. "Only if": Let $\mathcal{C}$ be a consistent colouring. With structural induction on φ and ψ we show that

$$\mathcal{C}(s) = \mathcal{C}(t) \Rightarrow (s \models_{db} \varphi \Leftrightarrow t \models_{db} \varphi) \quad \text{and} \quad \mathcal{C}(\pi) = \mathcal{C}(\rho) \Rightarrow (\pi \models_{db} \psi \Leftrightarrow \rho \models_{db} \psi).$$

The case $\varphi = p$ for $p \in \mathbf{AP}$ follows immediately from Definition 2.3. The cases $\varphi = \neg\varphi'$ and $\varphi = \bigwedge \Phi'$ follow immediately from the induction hypothesis.

Suppose $\mathcal{C}(s) = \mathcal{C}(t)$ and $s \models_{db} \exists\psi$. Then there exists a path π from s such that $\pi \models_{db} \psi$. $\mathcal{C}(\pi)$ is a coloured trace of s, and hence of t. Thus there must be a path ρ from t with $\mathcal{C}(\pi) = \mathcal{C}(\rho)$. By induction, $\rho \models_{db} \psi$. Hence, $t \models_{db} \exists\psi$.

The case $\psi \in \Phi$ follows since the first states of two paths with the same colour also have the same colour. The cases $\psi = \neg\psi'$ and $\psi = \bigwedge \Psi'$ follow immediately from the induction hypothesis.

Finally, suppose $\mathcal{C}(\pi) = \mathcal{C}(\rho)$ and $\pi \models_{db} \psi \,\mathsf{U}\, \psi'$. Then there exists a suffix π' of π such that $\pi' \models_{db} \psi'$ and $\pi'' \models_{db} \psi$ for all $\pi \trianglerighteq \pi'' \rhd \pi'$. As $\mathcal{C}(\pi) = \mathcal{C}(\rho)$, there must be a suffix ρ' of ρ such that $\mathcal{C}(\pi') = \mathcal{C}(\rho')$ and for every path ρ'' such that $\rho \trianglerighteq \rho'' \rhd \rho'$ there exists a path π'' with $\pi \trianglerighteq \pi'' \rhd \pi'$ such that $\mathcal{C}(\pi'') = \mathcal{C}(\rho'')$. By induction, this implies $\rho' \models_{db} \psi'$ and $\rho'' \models_{db} \psi$ for all $\rho \trianglerighteq \rho'' \rhd \rho'$. Hence $\rho \models_{db} \psi \,\mathsf{U}\, \psi'$.

"If": Let $\mathcal{C}$ be the colouring given by $\mathcal{C}(s) = \{\varphi \in \Phi \mid s \models_{db} \varphi\}$. It suffices to show that $\mathcal{C}$ is consistent. So suppose $\mathcal{C}(s) = \mathcal{C}(t)$. Trivially, s and t satisfy the same atomic propositions. By Lemma 2.5 it remains to show that s and t have the same coloured traces of length two. Suppose s has a coloured trace C, D. Let $s_0, \ldots, s_k$ be a path from s such that $\mathcal{C}(s_i) = C$ for $0 \leq i < k$ and $\mathcal{C}(s_k) = D \neq C$. Let

$$\mathcal{U} = \{u \mid \text{there is a path from } t \text{ to } u \text{ and } \mathcal{C}(u) \neq C\},$$
$$\mathcal{V} = \{v \mid \text{there is a path from } t \text{ to } v \text{ and } \mathcal{C}(v) \neq D\}.$$

For every $u \in \mathcal{U}$ pick a $\mathsf{CTL}^*_{-\mathsf{X}}$ formula $\varphi_u \in C - \mathcal{C}(u)$ (using negation on a formula in $\mathcal{C}(u) - C$ if needed), and for every $v \in \mathcal{V}$ pick a $\mathsf{CTL}^*_{-\mathsf{X}}$ formula $\varphi'_v \in D - \mathcal{C}(v)$. Now $s \models_{db} \exists(\bigwedge_{u\in\mathcal{U}} \varphi_u) \,\mathsf{U}\, (\bigwedge_{v\in\mathcal{V}} \varphi'_v)$ and, as $\mathcal{C}(s) = \mathcal{C}(t)$, also $t \models_{db} \exists(\bigwedge_{u\in\mathcal{U}} \varphi_u) \,\mathsf{U}\, (\bigwedge_{v\in\mathcal{V}} \varphi'_v)$. Thus, there is a path $t_0, \ldots, t_\ell$ from t such that $t_\ell \models_{db} \bigwedge_{v\in\mathcal{V}} \varphi'_v$ and $t_j \models_{db} \bigwedge_{u\in\mathcal{U}} \varphi_u$ for $0 \leq j < \ell$. It follows that $t_\ell \notin \mathcal{V}$ and $t_j \notin \mathcal{U}$ for $0 \leq j < \ell$. Hence $\mathcal{C}(t_\ell) = D$ and $\mathcal{C}(t_j) = C$ for $0 \leq j < \ell$, so C, D is also a coloured trace of t. □

Theorem 2.8. *$s \approx_s t$ iff $s \models \varphi \Leftrightarrow t \models \varphi$ for all $\mathsf{CTL}^*_{-\mathsf{X}}$ state formulas φ.*

Proof. "Only if" goes exactly as in the previous proof, reading $\models$ for $\models_{db}$, but requiring $\mathcal{C}$ to be *fully* consistent and, in the second paragraph, the paths π and ρ to be maximal and $\mathcal{C}(\pi)$ to be a *complete* coloured trace of s and t.

"If" goes as in the previous proof, but this time we have to show that $\mathcal{C}$ is *fully* consistent. Thus, applying Lemma 2.6, and assuming $\mathcal{C}(s) = \mathcal{C}(t)$, we additionally have to show that s and t have the same complete coloured traces of length one. Let π be a maximal path from s with $\mathcal{C}(\pi) = C$. Let

$$\mathcal{U} = \{u \mid \text{there is a path from } t \text{ to } u \text{ and } \mathcal{C}(u) \neq C\}.$$

For every $u \in \mathcal{U}$ pick a $\mathsf{CTL}^*_{-\mathsf{X}}$ formula $\varphi_u \in C - \mathcal{C}(u)$. Now $s \models \exists\mathsf{G}(\bigwedge_{u\in\mathcal{U}} \varphi_u)$ and, as $\mathcal{C}(s) = \mathcal{C}(t)$, also $t \models \exists\mathsf{G}(\bigwedge_{u\in\mathcal{U}} \varphi_u)$. Thus, there is a maximal path ρ from t such that $t' \models \bigwedge_{u\in\mathcal{U}} \varphi_u$ for all states t' in ρ. It follows that $t' \notin \mathcal{U}$. Hence $\mathcal{C}(t') = C$ and thus $\mathcal{C}(\rho) = C$. □

Since $\Leftrightarrow$ is an equivalence relation on predicates, we obtain the following corollary to Theorems 2.7 and 2.8.

Corollary 2.9. *$\approx_{dbs}$ and $\approx_s$ are equivalence relations.* □

Note that, for any colouring $\mathcal{C}$, the $\mathcal{C}$-coloured traces of a state s are completely determined by the complete $\mathcal{C}$-coloured traces of s, namely as their prefixes. Hence, any colouring that is fully consistent is certainly consistent, and thus $\approx_s$ is a finer (i.e. smaller, more discriminating) equivalence relation than $\approx_{dbs}$.

Above, the divergence blind interpretation of $\mathsf{CTL}^*_{-\mathsf{X}}$ is defined by using paths instead of maximal paths. It can equivalently be defined in terms of a transformation on Kripke structures, namely the addition of a self-loop $s \longrightarrow s$ for every state s.[3] Now $s \approx_{dbs} t$ holds in a certain Kripke structure iff $s \approx_s t$ holds in the Kripke structure obtained by adding all these self-loops. This is because the colour of a path doesn't change when self-loops are added to it, and up to self-loops any path is maximal. Likewise, $s \models_{db} \varphi$ in the original Kripke structure iff $s \models \varphi$ in the modified one.

Just like $\approx_{dbs}$ can be expressed in terms of $\approx_s$ by means of a transformation on Kripke structures, by means of a different transformation, at least for finite Kripke structures, $\approx_s$ can be expressed in terms of $\approx_{dbs}$. This is done in [5], Definitions 3.2.6 and 3.2.7.

3. Branching bisimulation equivalence in terms of coloured traces

We presuppose a set A of *actions* with a special element $\tau \in A$. A *labelled transition system* (LTS) is a structure $(S, \rightarrow)$ consisting of a set of states S and a *transition relation* $\rightarrow \subseteq S \times A \times S$. For the remainder of the section we fix an LTS $(S, \rightarrow)$. We write $s \xrightarrow{a} s'$ for $(s, a, s') \in \rightarrow$.

A *path* from s is an alternating sequence $s_0, a_1, s_1, a_2, \ldots$ of states and actions, ending with a state if the sequence is finite, such that $s = s_0$ and $s_{k-1} \xrightarrow{a_k} s_k$ for all relevant $k > 0$. A *maximal path* is an infinite path or a finite path $s_0, a_1, s_1, a_2, \ldots, a_n, s_n$ such that $\neg\exists a, s'.\ s_n \xrightarrow{a} s'$. We write $\pi \trianglerighteq \pi'$ if the path π' is a suffix of the path π, and $\pi \triangleright \pi'$ if $\pi \trianglerighteq \pi'$ and $\pi \neq \pi'$.

Definition 3.1. A *colouring* is a function $\mathcal{C} : S \to \mathbf{C}$, for $\mathbf{C}$ any set of *colours*.

For $\pi = s_0, a_1, s_1, a_2, \ldots$ a path from s, let $\mathcal{C}(\pi)$ be the alternating sequence of colours and actions obtained from $\mathcal{C}(s_0), a_1, \mathcal{C}(s_1), a_2, \ldots$ by contracting all finite maximal consecutive subsequences $C, \tau, C, \tau, \ldots, \tau, C$ and all infinite maximal consecutive subsequences $C, \tau, C, \tau, \ldots$ to C. The sequence $\mathcal{C}(\pi)$ is called a *$\mathcal{C}$-coloured trace* of s; it is *complete* if π is maximal; it is *divergent* if it is finite whilst π is infinite.

A colouring $\mathcal{C}$ is *[fully] consistent* if two states of the same colour always have the same [complete] $\mathcal{C}$-coloured traces. Two states s and t are *(divergence blind) branching bisimulation equivalent*, notation $s \leftrightarrows_b t$, if there exists a consistent colouring $\mathcal{C}$ such that $\mathcal{C}(s) = \mathcal{C}(t)$.

They are *divergence sensitive branching bisimulation equivalent*, notation $s \leftrightarrows_b^\lambda t$, if there exists a fully consistent colouring $\mathcal{C}$ such that $\mathcal{C}(s) = \mathcal{C}(t)$.

[3] In the beginning of this section we proposed a transformation that adds a self-loop $s \longrightarrow s$ merely to every *deadlock* state s. Both transformations make any Kripke structure total. However, whereas the previous transformation preserves the divergence sensitive interpretation of $\mathsf{CTL}^*_{-\mathsf{X}}$, the current one preserves the divergence blind interpretation, and expresses it in terms of the divergence sensitive one.

A consistent colouring *preserves divergence* if two states of the same colour always have the same divergent $\mathcal{C}$-coloured traces. Two states s and t are *branching bisimulation equivalent with explicit divergence*, notation $s \leftrightarrows_b^\Delta t$, if there exists a consistent, divergence preserving colouring $\mathcal{C}$ with $\mathcal{C}(s) = \mathcal{C}(t)$.

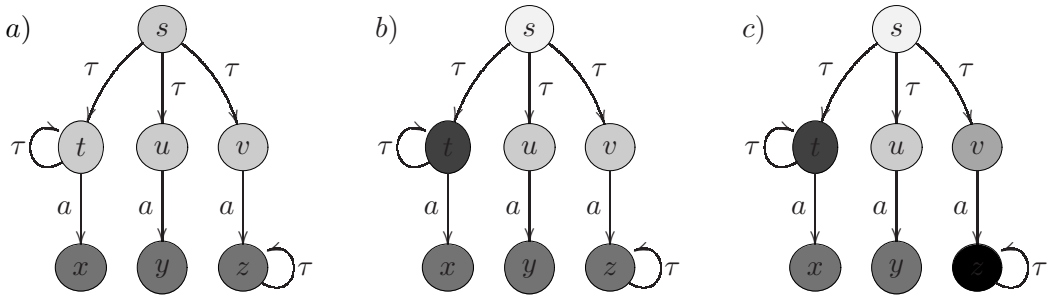

Figure 2: Difference between a) $\leftrightarrows_b$, b) $\leftrightarrows_b^\lambda$, and c) $\leftrightarrows_b^\Delta$.

The difference between $\leftrightarrows_b$, $\leftrightarrows_b^\lambda$, and $\leftrightarrows_b^\Delta$ is illustrated in the following example.

Example 3.2. Consider first the LTS and its colouring depicted in Figure 2a. This colouring is consistent and we have $s \leftrightarrows_b t \leftrightarrows_b u \leftrightarrows_b v$ and $x \leftrightarrows_b y \leftrightarrows_b z$. It is not fully consistent because state t has a complete trace ● whereas u has not. It is easy to see that every fully consistent colouring must assign different colours to states t and u, and so that $t \not\leftrightarrows_b^\lambda u$. One such colouring is given in Figure 2b and it shows that $u \leftrightarrows_b^\lambda v$ and $x \leftrightarrows_b^\lambda y \leftrightarrows_b^\lambda z$. Note, however, that this colouring, although fully consistent, does not preserve divergence. State v has a divergent trace ● a ● whereas u has not, and similarly state z has a divergent trace ● whereas y has not. Any colouring that preserves divergence must assign different colours to states u and v and to states y and z, meaning that $u \not\leftrightarrows_b^\Delta v$ and $y \not\leftrightarrows_b^\Delta z$. One such colouring is given in Figure 2c. It shows that $x \leftrightarrows_b^\Delta y$. In fact, these are the only two (different) states that are branching bisimulation equivalent with explicit divergence.

In the definition of $\leftrightarrows_b^\Delta$ above, consistency and preservation of divergence appear as two separate properties of colourings. Instead we could have integrated them by adding an extra bit (Δ) at the end of those finite coloured traces that stem from infinite paths. Likewise, $\leftrightarrows_b^\lambda$ could have been defined by adding such an extra bit at the end of those finite coloured traces that stem from maximal paths.

Lemmas 2.5 and 2.6 about colourings on Kripke structures apply to labelled transition systems as well. The proofs are essentially the same.

Lemma 3.3. *Let $\mathcal{C}$ be a colouring such that two states with the same colour have the same $\mathcal{C}$-coloured traces of length three (i.e. colour - action - colour). Then $\mathcal{C}$ is consistent.* □

Lemma 3.4. *Let $\mathcal{C}$ be a consistent colouring such that two states with the same colour have the same complete $\mathcal{C}$-coloured traces of length one. Then $\mathcal{C}$ is fully consistent.* □

Lemma 3.5. *Let $\mathcal{C}$ be a consistent colouring such that two states with the same colour have the same divergent $\mathcal{C}$-coloured traces of length one. Then $\mathcal{C}$ preserves divergence.*

Proof. Exactly like the proof of Lemma 2.6, but letting σ be a *divergent* $\mathcal{C}$-coloured trace of s; π, π' *infinite* paths; $\mathcal{C}(t')$ a *divergent* $\mathcal{C}$-coloured trace of t'; and ρ', ρ'' *infinite* paths. □

Branching bisimulation equivalence and branching bisimulation equivalence with explicit divergence were originally defined in Van Glabbeek & Weijland [10]. There, only *finite* coloured traces are considered, and a consistent colouring was defined as a colouring with the property that two states have the same colour only if they have the same finite coloured traces. By Lemma 3.3 this yields the same concept of consistent colouring as Definition 3.1 above.

In [10], a consistent colouring is said to *preserve divergence* if no divergent state has the same colour as a nondivergent state. Here a state s is *divergent* if it is the starting point of an infinite path of which all nodes have the same colour. This is the case if s has a divergent coloured trace of length one. Now Lemma 3.5 says that the definition of preservation of divergence from [10] agrees with the one proposed above. Hence the concepts of branching bisimulation and branching bisimulation with explicit divergence of [10] agree with ours.

Theorem 3.6. *$\leftrightarrows_b$, $\leftrightarrows_b^\lambda$ and $\leftrightarrows_b^\Delta$ are equivalence relations.*

Proof. We show the proof for $\leftrightarrows_b$; the other two cases proceed likewise.

We will regard any equivalence relation on S as a colouring, the colour of a state being its equivalence class. Conversely, any colouring can be considered as an equivalence relation on states.

The diagonal on S (i.e., the binary relation $\{(s,s) \mid s \in S\}$) is a consistent colouring, so $\leftrightarrows_b$ is reflexive. That $\leftrightarrows_b$ is symmetric is immediate from the required symmetry of colourings.

To prove that $\leftrightarrows_b$ is transitive, suppose $s \leftrightarrows_b t$ and $t \leftrightarrows_b u$. So there exist consistent colourings $\mathcal{C}$ and $\mathcal{D}$ with $\mathcal{C}(s) = \mathcal{C}(t)$ and $\mathcal{D}(t) = \mathcal{D}(u)$. Let $\mathcal{E}$ be the finest equivalence relation containing $\mathcal{C}$ and $\mathcal{D}$. Then $\mathcal{E}(s) = \mathcal{E}(t) = \mathcal{E}(u)$. It suffices to show that $\mathcal{E}$ is consistent.

First of all note that the $\mathcal{E}$-colour of a state is completely determined by its $\mathcal{C}$-colour, as well as by its $\mathcal{D}$-colour: $\mathcal{C}(p) = \mathcal{C}(q) \Rightarrow \mathcal{E}(p) = \mathcal{E}(q)$ and $\mathcal{D}(p) = \mathcal{D}(q) \Rightarrow \mathcal{E}(p) = \mathcal{E}(q)$ for all $p, q \in S$. Thus, if two states have the same sets of $\mathcal{C}$-coloured traces or the same sets of $\mathcal{D}$-coloured traces, they must also have the same sets of $\mathcal{E}$-coloured traces.

Suppose $\mathcal{E}(p) = \mathcal{E}(q)$. Then there must be a sequence of states $(p_i)_{0 \le i \le n}$ such that $p = p_0$, $q = p_n$ and for $0 \le i < n$ we have either $\mathcal{C}(p_i) = \mathcal{C}(p_{i+1})$ or $\mathcal{D}(p_i) = \mathcal{D}(p_{i+1})$. As $\mathcal{C}$ and $\mathcal{D}$ are consistent colourings, p_i and p_{i+1} have the same $\mathcal{C}$-coloured traces or the same $\mathcal{D}$-coloured traces. In either case they also have the same $\mathcal{E}$-coloured traces. This holds for $0 \le i < n$, so p and q have the same $\mathcal{E}$-coloured traces. Thus $\mathcal{E}$ is consistent. □

Lemma 3.7. *Let $\mathcal{C}$ be a consistent colouring and $s \in S$. Then the complete $\mathcal{C}$-coloured traces of s consist of the $\mathcal{C}$-coloured traces of s that are infinite, divergent, or maximal, in the sense that they cannot be extended.*

Proof. By definition, infinite and divergent $\mathcal{C}$-coloured traces of s are complete. Let σ be a maximal $\mathcal{C}$-coloured trace of s, and let π be a path from s such that $\mathcal{C}(\pi) = \sigma$. Let π' be an extension of π to a maximal path. As σ is a maximal $\mathcal{C}$-coloured trace, in the sense that it cannot be extended, we have $\mathcal{C}(\pi') = \sigma$. Hence σ is a complete $\mathcal{C}$-coloured trace of s.

Now let σ be a complete $\mathcal{C}$-coloured trace of s that is not infinite, nor a divergent $\mathcal{C}$-coloured trace of s. In that case $\sigma = \mathcal{C}(\pi)$ for π a finite maximal path from s. Let t be the last state of π. We have $\neg\exists a, t'.\ t \xrightarrow{a} t'$. Suppose, towards a contradiction, that σ is not maximal, i.e. there is a path π' from s such that $\mathcal{C}(\pi')$ is a proper extension of σ. Then there must be a state u on π' with $\mathcal{C}(u) = \mathcal{C}(t)$, such that u has a coloured trace σ'

of length > 1, which is a suffix of $\mathcal{C}(\pi')$. As $\mathcal{C}$ is consistent, σ' is also a coloured trace of t, contradicting $\neg\exists a, t'.\ t \xrightarrow{a} t'$. □

As for Kripke structures, for any colouring $\mathcal{C}$, the $\mathcal{C}$-coloured traces of a state s are the prefixes of the complete $\mathcal{C}$-coloured traces of s. Moreover, Lemma 3.7 says that the complete $\mathcal{C}$-coloured traces of a state s are completely determined by the $\mathcal{C}$-coloured traces of s together with the divergent $\mathcal{C}$-coloured traces of s. Hence, any colouring that is consistent and preserves divergence is also fully consistent. Therefore, $\underline{\leftrightarrow}_b^{\Delta}$ is finer than $\underline{\leftrightarrow}_b^{\lambda}$, which is finer than $\underline{\leftrightarrow}_b$.

The difference between $\underline{\leftrightarrow}_b^{\lambda}$ and $\underline{\leftrightarrow}_b^{\Delta}$ is that only the latter sees the difference between those maximal finite coloured traces that stem from finite paths (ending in *deadlock*) and those that stem from infinite paths (ending in *livelock*). For *deadlock-free* LTSs (having no states s with $\neg\exists a, s'.\ s \xrightarrow{a} s'$) the equivalences $\underline{\leftrightarrow}_b^{\lambda}$ and $\underline{\leftrightarrow}_b^{\Delta}$ coincide.

4. Translating between Kripke structures and labelled transition systems

We presuppose a set A of *actions* with a special element $\tau \in A$, and a set $\mathbf{AP}$ of *atomic propositions*. A *doubly labelled transition system* ($\mathrm{L}^2\mathrm{TS}$) is a structure $(S, \mathscr{L}, \rightarrow)$ that consists of a set of states S, a *labelling function* $\mathscr{L} : S \to 2^{\mathbf{AP}}$ and a *labelled transition relation* $\rightarrow \subseteq S \times A \times S$. From an $\mathrm{L}^2\mathrm{TS}$ one naturally obtains an LTS by omitting the labelling function $\mathscr{L}$, and a Kripke structure by replacing the labelled transition relation by one from which the labels are omitted. We call these the LTS or Kripke structure *associated* to the $\mathrm{L}^2\mathrm{TS}$. An $\mathrm{L}^2\mathrm{TS}$ $(S, \mathscr{L}, \rightarrow)$ is *consistent* if it satisfies the following three conditions:

(i) if $s \xrightarrow{a} t$, then $(\mathscr{L}(s) = \mathscr{L}(t)$ iff $a = \tau)$;
(ii) if $s \xrightarrow{a} t$, $s' \xrightarrow{a} t'$ and $\mathscr{L}(s) = \mathscr{L}(s')$, then $\mathscr{L}(t) = \mathscr{L}(t')$; and
(iii) if $s \xrightarrow{a} t$, $s' \xrightarrow{b} t'$, $\mathscr{L}(s) = \mathscr{L}(s')$ and $\mathscr{L}(t) = \mathscr{L}(t')$, then $a = b$.

Consistent $\mathrm{L}^2\mathrm{TS}$s were introduced in De Nicola & Vaandrager [5] for studying relationships between notions defined for Kripke structures and notions defined for LTSs. Condition (i) states that a transition is unobservable in the underlying Kripke structure (i.e., a transition between states with the same label) if and only if it is an unobservable transition in the underlying labelled transition system (i.e., a τ-transition). Condition (ii) expresses that the label of the target state of a transition is completely determined by the label of the source state and the label of the transition. Consequently, the label of a state t reachable from a state s is completely determined by the label of s and the sequence of labels of the transitions leading from s to t. Condition (iii) says that the label of a transition is fully determined by the labels of its source and target state.

Example 4.1. The three $\mathrm{L}^2\mathrm{TS}$s from Figure 3a are not consistent because they violate conditions (i), (ii), and (iii), respectively; the $\mathrm{L}^2\mathrm{TS}$ in Figure 3b is consistent.

Many semantic equivalences on LTSs, such as $\underline{\leftrightarrow}_b$, $\underline{\leftrightarrow}_b^{\lambda}$ and $\underline{\leftrightarrow}_b^{\Delta}$, are considered in the literature; for an overview see [8].

Definition 4.2. Any semantic equivalence $\sim$ on LTSs extends to $\mathrm{L}^2\mathrm{TS}$s by declaring, for all states s and t in an $\mathrm{L}^2\mathrm{TS}$, that $s \sim t$ iff $\mathscr{L}(s) = \mathscr{L}(t)$ and $s \sim t$ in the associated LTS.

Any semantic equivalence $\sim$ on Kripke structures extends to $\mathrm{L}^2\mathrm{TS}$s by declaring, for all states s and t in an $\mathrm{L}^2\mathrm{TS}$, that $s \sim t$ iff $s \sim t$ in the associated Kripke structure.

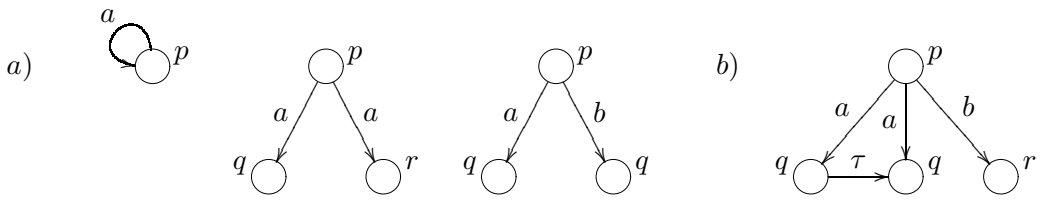

Figure 3: a) Three inconsistent L^{2}TSs and b) a consistent L^{2}TS.

The following theorem was proved in [5] for finite consistent L^{2}TSs. Here we drop the finiteness restriction.

Theorem 4.3. *On a consistent L^{2}TS, $\approx_{dbs}$ equals $\leftrightarrows_b$, and $\approx_s$ equals $\leftrightarrows_b^\lambda$.*

Proof. Suppose $s \approx_{dbs} t$ [or $s \approx_s t$]. Then there is a colouring $\mathcal{C}$ on the states of the L^{2}TS that is [fully] consistent on the associated Kripke structure K and satisfies $\mathcal{C}(s) = \mathcal{C}(t)$. By definition, this entails $\mathscr{L}(s) = \mathscr{L}(t)$. It remains to show that $\mathcal{C}$ is [fully] consistent on the associated LTS L. So let $\mathcal{C}(p) = \mathcal{C}(q)$, and let σ be a [complete] coloured trace of p in L. Using symmetry, it suffices to show that σ is also a [complete] coloured trace of q in L. Let ρ be obtained by omitting all actions from the alternating sequence of states and actions σ. Using direction "only if" of clause (i) in the definition of a consistent L^{2}TS, ρ must be a [complete] coloured trace of p in K. As $\mathcal{C}$ is [fully] consistent on K, ρ must also be a [complete] coloured trace of q in K. Finally, using clauses (i) "only if" and (iii), σ must be a [complete] coloured trace of q in L.

Now suppose $s \leftrightarrows_b t$ [or $s \leftrightarrows_b^\lambda t$]. Then $\mathscr{L}(s) = \mathscr{L}(t)$ and there is a colouring $\mathcal{C}$ on the states of the L^{2}TS, with $\mathcal{C}(s) = \mathcal{C}(t)$, that is [fully] consistent on L. Let $\mathcal{D}$ be the colouring given by $\mathcal{D}(p) := (\mathcal{C}(p), \mathscr{L}(p))$ for all $p \in S$, so that $\mathcal{D}(p) = \mathcal{D}(q) \Leftrightarrow [\mathcal{C}(p) = \mathcal{C}(q) \wedge \mathscr{L}(p) = \mathscr{L}(q)]$. It suffices to show that $\mathcal{D}$ is [fully] consistent on K. The requirement $\mathcal{D}(p) = \mathcal{D}(q) \Rightarrow \mathscr{L}(p) = \mathscr{L}(q)$ is built into the definition of $\mathcal{D}$. So let $\mathcal{D}(p) = \mathcal{D}(q)$, and let ν be a [complete] $\mathcal{D}$-coloured trace of p in K. Using symmetry, it suffices to show that ν is also a [complete] $\mathcal{D}$-coloured trace of q in K. Using clause (i) "only if", there must be a [complete] $\mathcal{D}$-coloured trace ρ of p in L such that ν is obtained from ρ by omitting its actions. Let σ be the [complete] $\mathcal{C}$-coloured trace of s in K obtained from ρ by omitting the second component of each $\mathcal{D}$-colour of a state. As $\mathcal{C}(p) = \mathcal{C}(q)$ and $\mathcal{C}$ is [fully] consistent on L, σ must also be a [complete] $\mathcal{C}$-coloured trace of q in L. By applying clauses (i) "if" and (ii) one derives that ρ is a [complete] $\mathcal{D}$-coloured trace of q in L. Therefore, again using clause (i) "only if", ν must be a [complete] $\mathcal{D}$-coloured trace of q in K. □

Observation 4.4. For every Kripke structure K there exists a consistent L^{2}TS D such that K is the Kripke structure associated to D.

One way to obtain D is to label any transition $s \longrightarrow t$ by the pair $(\mathscr{L}(s), \mathscr{L}(t))$ (or simply by $\mathscr{L}(t)$) when $\mathscr{L}(s) \neq \mathscr{L}(t)$, or τ when $\mathscr{L}(s) = \mathscr{L}(t)$. An alternative is the label $(\mathscr{L}(s) - \mathscr{L}(t), \mathscr{L}(t) - \mathscr{L}(s))$, where $(\emptyset, \emptyset)$ is identified with τ.

Unlike the situation for Kripke structures (Observation 4.4) it is not the case that every LTS can be obtained as the LTS associated to a consistent L^{2}TS. A simple counterexample is presented in [5]. Thus, in encoding LTSs as L^{2}TSs, it is in general not possible to keep the set of states the same.

Definition 4.5. An *LTS-to-L^{2}TS transformation* η consist of a function taking any LTS L to a consistent L^{2}TS η(L), and in addition taking any state s in L to a state $\eta(s)$ in η(L). Such

a transformation should at least satisfy $s \leftrightarrows_b^\lambda t \Leftrightarrow \eta(s) \leftrightarrows_b^\lambda \eta(t)$, that is, it *preserves* ("$\Rightarrow$") and *reflects* ("$\Leftarrow$") divergence sensitive branching bisimulation equivalence, and likewise for $\leftrightarrows_b$, and $\leftrightarrows_b^\Delta$.

A common LTS-to-L^{2}TS transformation is presented in [5]. It takes an LTS $\mathrm{L} = (S, \rightarrow)$ to an L^{2}TS $\eta(\mathrm{L})$ by inserting a new state halfway along any transition $s \xrightarrow{a} t$ with $a \neq \tau$. This new state is labelled $\{a\}$, and each of the two transitions replacing $s \xrightarrow{a} t$ (from s to the new state and from there to t) is labelled a. Transitions $s \xrightarrow{\tau} t$ are untouched. One takes $\eta(s) = s$ for $s \in S$ and all such states from L are labelled with the same dummy symbol in $\eta(\mathrm{L})$. (Consult [5] for the formal definition and examples.) In [5] it is shown that this transformation preserves and reflects $\leftrightarrows_b^\lambda$; the same proof applies to $\leftrightarrows_b$ and $\leftrightarrows_b^\Delta$.

An LTS-to-L^{2}TS transformation η yields an LTS-to-Kripke-structure transformation that we also call η, namely the one transforming an LTS L into the Kripke structure associated to $\eta(\mathrm{L})$. In fact, using Theorem 4.3 and Observation 4.4, any LTS-to-Kripke-structure transformation η that preserves and reflects the required equivalences can be obtained in this way.

An LTS-to-L^{2}TS transformation η makes it possible to define when a state s in an LTS satisfies a $\mathsf{CTL}^*_{-\mathsf{X}}$ formula φ. Namely, one defines $s \models^\eta \varphi$ iff $\eta(s) \models \varphi$. This way, $\mathsf{CTL}^*_{-\mathsf{X}}$ can be used as temporal logic on LTSs.

Theorem 4.6. *Let s and t be states in an LTS, and let η be an LTS-to-L^{2}TS transformation. Then*

$$s \leftrightarrows_b t \text{ iff } s \models^\eta_{db} \varphi \Leftrightarrow t \models^\eta_{db} \varphi \text{ for all } \mathsf{CTL}^*_{-\mathsf{X}} \text{ state formulas } \varphi$$
$$s \leftrightarrows_b^\lambda t \text{ iff } s \models^\eta \varphi \Leftrightarrow t \models^\eta \varphi \text{ for all } \mathsf{CTL}^*_{-\mathsf{X}} \text{ state formulas } \varphi.$$

Proof. This is an immediate consequence of the requirement that η preserves and reflects $\leftrightarrows_b$ and $\leftrightarrows_b^\lambda$, in combination with Theorems 2.7, 2.8 and 4.3. □

5. Parallel composition

For a behavioural equivalence to be useful in a process algebraic setting, it is essential that it is a congruence for the operations under consideration. In this section we prove that $\leftrightarrows_b^\Delta$ and $\leftrightarrows_b$ are congruences for the *merge* or *interleaving operator* $\|$. This operator is often used to represent (asynchronous) parallel composition. However, $\leftrightarrows_b^\lambda$ fails to be a congruence for $\|$. We characterise the least discriminating congruence that makes all the distinctions of $\leftrightarrows_b^\lambda$ as $\leftrightarrows_b^\Delta$. In the following definition we provide the necessary and sufficient conditions for a binary operation *on* the set of states of an LTS to qualify as a merge.

Definition 5.1. A binary operation $\|$ on the states of an LTS is a *merge* if for all $s, t, u \in S$ and for all $a \in A$ it holds that $s \,\|\, t \xrightarrow{a} u$ iff

- there exists $s' \in S$ such that $s \xrightarrow{a} s'$ and $u = s' \,\|\, t$; or
- there exists $t' \in S$ such that $t \xrightarrow{a} t'$ and $u = s \,\|\, t'$.

The structural operational semantics of any process calculus that includes an operation for pure interleaving generates an LTS with merge. Moreover, any LTS can be augmented to an LTS with merge, for instance through a transition system specification [1] that includes all states of the original LTS as constants and a binary operation $\|$ with the usual structural operational rules for interleaving parallel composition. Henceforth we deal with LTSs with a merge $\|$.

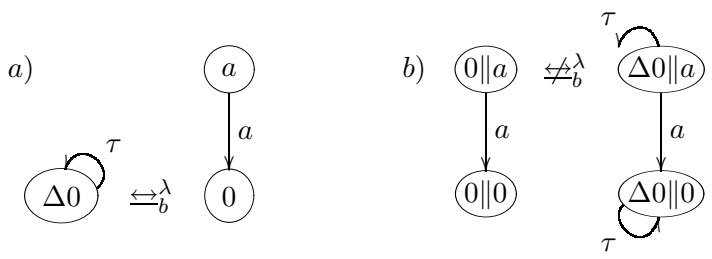

Figure 4: $\leftrightarrows_b^\lambda$ is not a congruence for parallel composition

Theorem 5.2. *The relation $\leftrightarrows_b^\Delta$ is a congruence for $\|$, i.e., if $s \leftrightarrows_b^\Delta t$ and $u \leftrightarrows_b^\Delta v$, then $s \parallel u \leftrightarrows_b^\Delta t \parallel v$.*

Proof. Let $\mathcal{R}$ be the reflexive and transitive closure of the relation

$$\{(p\|q,\, p'\|q') \mid p \leftrightarrows_b^\Delta p' \;\&\; q \leftrightarrows_b^\Delta q'\} \ .$$

Let $\mathcal{C}$ be the function that assigns to each state its equivalence class with respect to $\mathcal{R}$. It suffices to prove that $\mathcal{C}$ is a consistent divergence preserving colouring. So suppose $\mathcal{C}(r) = \mathcal{C}(r')$. Using Lemmas 3.3 and 3.5 it suffices to show that r and r' have the same $\mathcal{C}$-coloured traces of length three and the same divergent $\mathcal{C}$-coloured traces of length one. It is straightforward, but notationally cumbersome, to establish this in the special case that $r = p \parallel q$ and $r' = p' \parallel q'$ with $p \leftrightarrows_b^\Delta p'$ and $q \leftrightarrows_b^\Delta q'$. The general case then follows by induction on the length of a chain of pairs from the relation displayed above showing that the pair (r, r') is in its reflexive and transitive closure. □

A similar proof shows that also $\leftrightarrows_b$ is a congruence for $\|$. However, $\leftrightarrows_b^\lambda$ is not.

Example 5.3. Consider an LTS with merge that contains a state 0 without outgoing transitions, a state $\Delta 0$ with a τ-loop (an outgoing τ-labelled transition to itself) and no other outgoing transitions, and a state a with $a \xrightarrow{a} 0$ and no other outgoing transitions. (Note that such an LTS is, e.g., generated by the structural operational semantics of CCS with recursion.) Then $0 \leftrightarrows_b^\lambda \Delta 0$. Figure 4a shows the fragment consisting of the states 0, $\Delta 0$ and a of the LTS under consideration. Figure 4b shows a fragment where the merge is applied. Observe that $0 \parallel a \not\leftrightarrows_b^\lambda \Delta 0 \parallel a$. The reason is that $\Delta 0 \parallel a$ has a maximal path that stays in its initial state, whereas $0 \parallel a$ has not. This problem does not apply to $\leftrightarrows_b$ because $0 \parallel a \leftrightarrows_b \Delta 0 \parallel a$. It does not apply to $\leftrightarrows_b^\Delta$ because $0 \not\leftrightarrows_b^\Delta \Delta 0$.

The example above involves a deadlock state, namely 0. This is unavoidable, as on LTSs without deadlock $\leftrightarrows_b^\lambda$ coincides with $\leftrightarrows_b^\Delta$ (cf. Section 3) and hence is a congruence for $\|$.

The standard solution to the problem of an equivalence $\sim$ failing to be a congruence for a desirable operator Op is to replace it by the coarsest congruence for Op that is included in $\sim$ [13]. Applying this technique to the current situation, the coarsest congruence for $\|$ included in $\leftrightarrows_b^\lambda$ turns out to be $\leftrightarrows_b^\Delta$.

Theorem 5.4. *$\leftrightarrows_b^\Delta$ is the coarsest congruence for $\|$ that is included in $\leftrightarrows_b^\lambda$.*[4]

[4]Strictly speaking, we merely show that $\leftrightarrows_b^\Delta$ is the coarsest congruence for $\|$ that is included in $\leftrightarrows_b^\lambda$ and satisfies the Fresh Atom Principle (FAP). This principle, described in [9], is satisfied by a semantic equivalence $\sim$ on LTSs when $\sim$ on an LTS L can always be obtained as the restriction of $\sim$ on any given larger LTS of which L is a subLTS, and whose transition labels may be drawn from a larger set of actions

Proof. We have already seen that $\leftrightarrows_b^\Delta$ is a congruence for $\|$, and that it is included in $\leftrightarrows_b^\lambda$. To show that it is the coarsest, we need to show that if $\sim$ is any congruence for $\|$ that is included in $\leftrightarrows_b^\lambda$, then $\sim$ is included in $\leftrightarrows_b^\Delta$. So let $\sim$ be such a congruence and assume $s \sim t$. We need to show that $s \leftrightarrows_b^\Delta t$. Let a be an action that does not occur in any path from s or t. Since $\sim$ is a congruence for $\|$, we have $s \,\|\, a \sim t \,\|\, a$, where a is the state from Example 5.3. As $\sim$ is included in $\leftrightarrows_b^\lambda$ we obtain $s \,\|\, a \leftrightarrows_b^\lambda t \,\|\, a$. Let $\mathcal{C}$ be a fully consistent colouring with $\mathcal{C}(s\|a) = \mathcal{C}(t\|a)$. Define the colouring $\mathcal{D}$ by $\mathcal{D}(p) = \mathcal{C}(p\|a)$ for p a state reachable from s or t, and $\mathcal{D}(p) = p$ otherwise. Then $\mathcal{D}(s) = \mathcal{D}(t)$. It suffices to show that $\mathcal{D}$ is consistent and preserves divergence, implying $s \leftrightarrows_b^\Delta t$.

So suppose $\mathcal{D}(p) = \mathcal{D}(q)$ with $p \neq q$. Then $\mathcal{C}(p\|a) = \mathcal{C}(q\|a)$.

First we show that p and q have the same $\mathcal{D}$-coloured traces. Let σ be a $\mathcal{D}$-coloured trace of p. Then σ is also a $\mathcal{C}$-coloured trace of $p \,\|\, a$. As $p \,\|\, a$ and $q \,\|\, a$ have the same complete $\mathcal{C}$-coloured traces, they surely have the same $\mathcal{C}$-coloured traces (for the coloured traces of a state are the prefixes of its complete coloured traces). Hence σ is a $\mathcal{C}$-coloured trace of $q \,\|\, a$. As p is reachable from s or t, the action a cannot occur in σ. Therefore, σ must also be a $\mathcal{D}$-coloured trace of q. By symmetry, any $\mathcal{D}$-coloured trace of q is also a $\mathcal{D}$-coloured trace of p, and hence p and q have the same $\mathcal{D}$-coloured traces.

Next, we show that p and q have the same divergent $\mathcal{D}$-coloured traces. So let σ be a divergent $\mathcal{D}$-coloured trace of p. Then σ is also a divergent $\mathcal{C}$-coloured trace of $p \,\|\, a$. Hence σ is a complete $\mathcal{C}$-coloured trace of $p \,\|\, a$ and thus also of $q \,\|\, a$. As the action a cannot occur in σ, it is not possible that σ stems from a finite maximal path from $q \,\|\, a$. Therefore, σ must be a divergent $\mathcal{C}$-coloured trace of $q \,\|\, a$, and hence a divergent $\mathcal{D}$-coloured trace of q. Again invoking symmetry, p and q have the same divergent $\mathcal{D}$-coloured traces.

It follows that $\mathcal{D}$ is consistent and preserves divergence; thus $s \leftrightarrows_b^\Delta t$. □

So if one is in search of a semantics such that, for s and t states in an LTS,

- if there is a $\mathsf{CTL}^*_{-\mathsf{X}}$ state formula φ such that $s \models^\eta \varphi$ but $t \not\models^\eta \varphi$, then s and t should be distinguished,
- if s and t can be distinguished after placing them in a context $\_ \,\|\, u$ for some u, then they should be distinguished to start with, and
- no two states should be distinguished unless this is required by the previous two conditions,

then branching bisimulation semantics with explicit divergence is the answer, for $s \leftrightarrows_b^\Delta t$ iff for all u and all $\varphi \in \Phi$ we have $s \,\|\, u \models^\eta \varphi \Leftrightarrow t \,\|\, u \models^\eta \varphi$.

6. Adding deadlock detection to $\mathsf{CTL}^*_{-\mathsf{X}}$

We saw above that there are important properties of states s in an LTS that can be expressed in terms of a context $\_ \,\|\, u$ and a $\mathsf{CTL}^*_{-\mathsf{X}}$ formula φ, namely as $s\|u \models^\eta \varphi$, but that cannot be directly expressed in terms of $\mathsf{CTL}^*_{-\mathsf{X}}$. This is somewhat unsatisfactory, and therefore we propose an extension of $\mathsf{CTL}^*_{-\mathsf{X}}$ in which this type of property can be expressed directly. We add a path modality ∞ that is valid on a path π iff π is infinite. This path modality,

than those of L. FAP allows us to use the state a that figures in the proof of Theorem 5.4, regardless of whether such a state, or the fresh action a, occurs in the given LTS or not. FAP is satisfied by virtually all semantic equivalences documented in the literature, and can be used as a sanity check for meaningful equivalences [9].

or actually an equally expressive one, was studied prior by Kaivola & Valmari [11] in the context of Linear Temporal Logic without the next state operator—see Section 9.

Definition 6.1. The syntax of CTL^*_∞ is given by

$$\varphi ::= \ p \ \mid \ \neg\varphi \ \mid \ \bigwedge \Phi' \ \mid \ \exists\psi \qquad\qquad \psi ::= \ \varphi \ \mid \ \neg\psi \ \mid \ \bigwedge \Psi' \mid \ \psi \,\mathsf{U}\, \psi \mid \ \infty$$

with $p \in \mathbf{AP}$, $\varphi \in \Phi$, $\Phi' \subseteq \Phi$, $\psi \in \Psi$ and $\Psi' \subseteq \Psi$.
Validity is defined as in Definition 2.2, but adding the clause

– $\pi \models \infty$ iff the path π is infinite.

We write $\exists^\infty\psi$ for $\exists(\infty \wedge \psi)$; this formula holds in a state s if there exists an infinite path π from s such that $\pi \models \psi$. Likewise $\forall^\infty\psi = \forall(\infty \to \psi)$ holds in s if for all infinite paths π from s we have that $s \models \psi$. These constructs are *dual*, in the sense that $s \models \neg\exists^\infty\psi$ iff $s \models \forall^\infty\neg\psi$.

The negation of ∞ holds for a maximal path π iff π is finite, and hence ends in a deadlock. It is tempting to simply extend $\mathsf{CTL}^*_{-\mathsf{X}}$ with a state formula δ such that $s \models \delta$ iff $\neg\exists s'.\ s \longrightarrow s'$. This would make it possible to express ∞ as $\neg\mathsf{F}\delta$. However, this would make the resulting logic too expressive: the two states in the Kripke structure $\circ \longrightarrow \circ$ (with the empty labelling) are branching bisimulation equivalent with explicit divergence, yet they would be distinguished by this extension of $\mathsf{CTL}^*_{-\mathsf{X}}$, as only the last state satisfies δ.

CTL^*_∞ is an extension of $\mathsf{CTL}^*_{-\mathsf{X}}$. There is no need for a similar extension of CTL^*, for δ can be expressed as $\neg\exists\mathsf{X}\top$. In particular, CTL^*_∞ is not more expressive than CTL^*.

The definition of branching bisimulation equivalence with explicit divergence lifts easily to Kripke structures: $s \leftrightarrows^\Delta_b t$, for s and t states in a Kripke structure, iff there exists a consistent and divergence preserving colouring $\mathcal{C}$ such that $\mathcal{C}(s) = \mathcal{C}(t)$. Here *divergence preserving* is defined as in Section 3; by Lemma 3.5, this time applied to Kripke structures, a consistent colouring preserves divergence iff, for any states s and t, $\mathcal{C}(s) = \mathcal{C}(t)$ implies

$$\begin{array}{c}\text{for any infinite path } \pi \text{ from } s \text{ with } \mathcal{C}(\pi) = \mathcal{C}(s)\\ \text{there is an infinite path } \rho \text{ from } t \text{ with } \mathcal{C}(\rho) = \mathcal{C}(t).\end{array}$$

Theorem 6.2. *$s \leftrightarrows^\Delta_b t$ iff $s \models \varphi \Leftrightarrow t \models \varphi$ for all CTL^*_∞ state formulas φ.*

Proof. "Only if" goes as in the proof of Theorem 2.7, reading $\models$ for $\models_{db}$, requiring $\mathcal{C}$ to be *consistent and divergence preserving*, and, in the second paragraph, requiring the paths π and ρ to be maximal and $\mathcal{C}(\pi)$ to be a *complete* coloured trace of s and t. Here we use that if a colouring is consistent and divergence preserving, then two states with the same colour must also have the same complete coloured traces. This follows from Lemma 3.7, this time applied to Kripke structures.

There is one extra case to check. Suppose $\mathcal{C}(\pi) = \mathcal{C}(\rho)$ and $\pi \models \infty$, but $\rho \not\models \infty$. Then the last state t of ρ has the same colour $\mathcal{C}(t)$ as one of the states s of π. Let π' be the (infinite) suffix of π starting at s. Then $\mathcal{C}(\pi') = \mathcal{C}(s) = \mathcal{C}(t)$, yet there is no infinite path from t, contradicting that $\mathcal{C}$ is divergence preserving.

"If" goes as in the proof of Theorem 2.7, but this time we also have to show that $\mathcal{C}$ preserves divergence. So let s and t be states and π an infinite path from s with $\mathcal{C}(\pi) = \mathcal{C}(s) = \mathcal{C}(t) = C$. Let

$$\mathcal{U} = \{u \mid \text{there is a path from } t \text{ to } u \text{ and } \mathcal{C}(u) \neq C\}.$$

For every $u \in \mathcal{U}$ pick a CTL^*_∞ formula $\varphi_u \in C - \mathcal{C}(u)$. Now $s \models \exists^\infty \mathsf{G}(\bigwedge_{u\in\mathcal{U}} \varphi_u)$ and, as $\mathcal{C}(s) = \mathcal{C}(t)$, also $t \models \exists^\infty \mathsf{G}(\bigwedge_{u\in\mathcal{U}} \varphi_u)$. Thus, there is an infinite path ρ from t such that $t' \models \bigwedge_{u\in\mathcal{U}} \varphi_u$ for all states t' in ρ. It follows that $t' \notin \mathcal{U}$. Hence $\mathcal{C}(t') = C$ and thus $\mathcal{C}(\rho) = C$. □

7. Adding deadlock detection to $\mathsf{CTL}_{-\mathsf{X}}$

$\mathsf{CTL}_{-\mathsf{X}}$ is the sublogic of $\mathsf{CTL}^*_{-\mathsf{X}}$ that only allows path formulas of the form $\varphi \,\mathsf{U}\, \varphi'$ and $\neg(\varphi \,\mathsf{U}\, \varphi')$, where φ and φ' are state formulas. Equivalently, it can be defined as only allowing path formulas of the form $\varphi \,\mathsf{U}\, \varphi'$ and $\mathsf{G}\varphi$, for we have

$$s \models \exists \mathsf{G}\varphi \text{ iff } s \models \exists\neg(\top \,\mathsf{U}\, \neg\varphi)$$

$$s \models \exists\neg(\varphi \,\mathsf{U}\, \varphi') \text{ iff } s \models \exists[(\neg\varphi') \,\mathsf{U}\, \neg(\varphi \vee \varphi')] \vee \exists\mathsf{G}\neg\varphi' \,.$$

Theorems 2.7 and 2.8 are also valid when using $\mathsf{CTL}_{-\mathsf{X}}$ instead of $\mathsf{CTL}^*_{-\mathsf{X}}$, for their proofs use no other temporal constructs than $\exists(\varphi \,\mathsf{U}\, \varphi')$ and $\exists\mathsf{G}\varphi$.

A natural proposal for CTL_∞ would be to add the path quantifier $\exists^\infty$ to $\mathsf{CTL}_{-\mathsf{X}}$, thus yielding the syntax

$$\varphi \;::=\; p \mid \neg\varphi \mid \bigwedge \Phi' \mid \exists(\varphi \,\mathsf{U}\, \varphi) \mid \exists^\infty(\varphi \,\mathsf{U}\, \varphi) \mid \exists\mathsf{G}\varphi \mid \exists^\infty\mathsf{G}\varphi \,.$$

However, we can economise on that, for

$$s \models \exists^\infty(\varphi \,\mathsf{U}\, \varphi') \text{ iff } s \models \exists(\varphi \,\mathsf{U}\, (\varphi' \wedge \exists^\infty\mathsf{G}\top))$$

$$s \models \exists\mathsf{G}\varphi \text{ iff } s \models \exists^\infty\mathsf{G}\varphi \vee \exists(\varphi \,\mathsf{U}\, (\forall\mathsf{G}\varphi))$$

where $\forall\mathsf{G}\varphi$ is an abbreviation for $\neg\exists(\top \,\mathsf{U}\, \neg\varphi)$. Hence CTL_∞ can be given by the syntax

$$\varphi ::= p \mid \neg\varphi \mid \bigwedge \Phi' \mid \exists(\varphi \,\mathsf{U}\, \varphi) \mid \exists^\infty\mathsf{G}\varphi \,.$$

It follows immediately from the proof of Theorem 6.2 that this language is sufficiently expressive to characterise branching bisimulation equivalence with explicit divergence:

Theorem 7.1. *$s \leftrightarrows_b^\Delta t$ iff $s \models \varphi \Leftrightarrow t \models \varphi$ for all CTL_∞ formulas φ.* □

It is tempting to simply write $\exists^\infty\mathsf{G}$ as $\exists\mathsf{G}$; that is, to keep the same syntax as for $\mathsf{CTL}_{-\mathsf{X}}$ but define its semantics in such a way that $\exists(\varphi \,\mathsf{U}\, \varphi')$ asks merely for a finite path, whereas $\exists\mathsf{G}\varphi$ asks for an infinite one. This *deadlock sensitive* interpretation of $\mathsf{CTL}_{-\mathsf{X}}$ is an alternative for the interpretation of [5]. It is consistent with the classical interpretation of CTL [7, 3], as for total Kripke structures there is no difference between $\exists^\infty$ and $\exists$.

8. The deadlock extension of Kripke structures

Following De Nicola & Vaandrager [5] we have applied $\mathsf{CTL}^*_{-\mathsf{X}}$ to non-total Kripke structures by using maximal instead of infinite paths in the definition of validity. As remarked in Section 2, the same effect can be obtained by transforming a non-total Kripke structure into a total one by adding a self-loop $s \longrightarrow s$ to every deadlock state s, and applying the standard $\mathsf{CTL}^*_{-\mathsf{X}}$ semantics to the resulting total Kripke structure. However, the latter does not apply to CTL^*_∞, because the self-loop $s \longrightarrow s$ invalidates the formula $\exists\neg\infty$ that holds in any deadlock state s. Here we define another transformation on Kripke structures that makes every Kripke structure total, and allows the encoding of CTL^*_∞ in terms of $\mathsf{CTL}^*_{-\mathsf{X}}$.

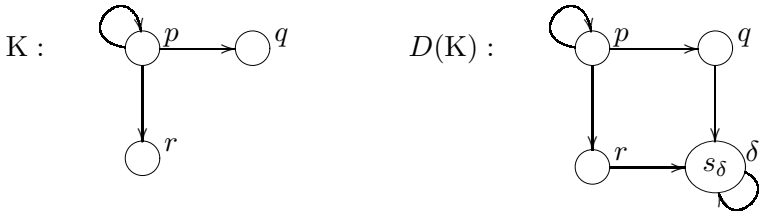

Figure 5: Deadlock extension of a Kripke structure

Definition 8.1. The *deadlock extension* $D(\mathrm{K})$ of a Kripke structure K is obtained by the addition of a fresh state s_δ, labelled by the fresh atomic proposition δ, together with a transition from s_δ and from every deadlock state in K to s_δ.

An example of this transformation is depicted in Figure 5.

Theorem 8.2. *Let* K *be a Kripke structure, with states* s *and* t*. Then* $s \leftrightarrows_b^\Delta t$ *within the Kripke structure* K *iff* $s \leftrightarrows_b^\Delta t$ *within the Kripke structure* $D(\mathrm{K})$*.*

Proof. "If": Let $\mathcal{D}$ be a consistent and divergence preserving colouring on $D(\mathrm{K})$. Note that $\mathcal{D}(s_\delta) \neq \mathcal{D}(s)$ for any state $s \neq s_\delta$ in $D(\mathrm{K})$. Let $\mathcal{C}$ be the restriction of $\mathcal{D}$ to the states of K. Then the $\mathcal{C}$-coloured traces of a state s in K equal the $\mathcal{D}$-coloured traces of s in $D(\mathrm{K})$, but with the colour $\mathcal{D}(s_\delta)$ omitted from the end of such traces. It follows that $\mathcal{C}$ is consistent. It preserves divergence by Lemma 3.5.

"Only if": Let $\mathcal{C}$ be a consistent and divergence preserving colouring on K. Extend it to a colouring $\mathcal{D}$ on $D(\mathrm{K})$ by assigning a fresh colour δ to the extra state s_δ of $D(\mathrm{K})$. It suffices to check that $\mathcal{D}$ is consistent and divergence preserving.

Claim. From any state s in K with the same colour as a deadlock state t in K there must be a path π to a deadlock state such that $\mathcal{C}(\pi) = \mathcal{C}(t)$.

Proof of claim. As t has no $\mathcal{C}$-coloured traces of length two, neither does s, and as t has no divergent $\mathcal{C}$-coloured traces, neither does s. Thus, all paths from s are finite and only pass through states with colour $\mathcal{C}(t)$.

Application of the claim. The $\mathcal{D}$-coloured traces of length two of a state $s \neq s_\delta$ in $D(\mathrm{K})$ are the $\mathcal{C}$-coloured traces of length two of the state s in K, together with the trace $\mathcal{C}(t)\delta$ in case s has the same colour as a deadlock state t in K. Thus $\mathcal{D}$ is consistent by Lemma 2.5, and preserves divergence by Lemma 3.5. □

The "if"-direction of the theorem, with a similar proof, also applies to $\approx_s$ and $\approx_{dbs}$, but the "only if"-direction does not. As a counterexample, let K be a Kripke structure with a deadlock state d (having no outgoing transitions) and a livelock state l (with a self-loop as its only one outgoing transition); neither state satisfies any atomic propositions. In K we have $d \approx_s l$, and hence $d \approx_{dbs} l$, but in $D(\mathrm{K})$ we have $d \not\approx_{dbs} l$, and hence $d \not\approx_s l$.

Considering that Kripke structures of the form $D(\mathrm{K})$ are total, and that on total Kripke structures $\approx_s$ and $\leftrightarrows_b^\Delta$ coincide, it is in fact impossible to define a transformation like D for which Theorem 8.2 holds for both $\leftrightarrows_b^\Delta$ and $\approx_s$.

Now let η be an arbitrary LTS-to-L^{2}TS-transformation, yielding an LTS-to-Kripke-structure transformation that is also called η (see Section 4). Then $D \circ \eta$ is not a valid LTS-to-Kripke-structure transformation as intended in [5], for it fails to preserve $\leftrightarrows_b^\lambda$ / $\approx_s$ and $\leftrightarrows_b$ / $\approx_{dbs}$ (cf. Definition 4.5). Yet, it satisfies

$$s \leftrightarrows_b^\Delta t \;\Leftrightarrow\; D \circ \eta(s) \approx_s D \circ \eta(t)$$

(because $s \leftrightarrows_b^\Delta t \Leftrightarrow \eta(s) \leftrightarrows_b^\Delta \eta(t) \Leftrightarrow D \circ \eta(s) \leftrightarrows_b^\Delta D \circ \eta(t)$ and on total Kripke structures $\leftrightarrows_b^\Delta$ and $\approx_s$ coincide), and as such it is a suitable transformation for defining validity of $\mathsf{CTL}^*_{-\mathsf{X}}$ formula on states in LTSs. We obtain:

Corollary 8.3. *Let s and t be states in an LTS, and let η be an LTS-to-L^{2}TS transformation. Then $s \leftrightarrows_b^\Delta t$ iff $s \models^{D\circ\eta} \varphi \Leftrightarrow t \models^{D\circ\eta} \varphi$ for all $\mathsf{CTL}^*_{-\mathsf{X}}$ state formulas φ.* □

Thus, one way to make $\mathsf{CTL}^*_{-\mathsf{X}}$ suitable for dealing with deadlock behaviour on LTSs is to stick to total Kripke structures and translate LTSs to Kripke structures by a translation $D \circ \eta$ instead of a transformation η as proposed in [5]. This way branching bisimulation equivalence with explicit divergence becomes the natural counterpart of stuttering equivalence on Kripke structures, and we have the modal characterisation of Corollary 8.3.

An alternative is to stick to more natural transformations η meeting the criteria on Definition 4.5, apply the definition of validity of $\mathsf{CTL}^*_{-\mathsf{X}}$ formulas to non-total Kripke structures as in [5], and extend $\mathsf{CTL}^*_{-\mathsf{X}}$ to CTL^*_∞ as indicated in Section 6.

Below we show that these solutions lead to equally expressive logics on LTSs.

Definition 8.4. Given a set of atomic propositions, let CTL^*_δ be the logic $\mathsf{CTL}^*_{-\mathsf{X}}$ extended with an extra atomic proposition δ. The mappings $\mathscr{D}$ from CTL^*_∞ to CTL^*_δ formulas and $\mathscr{E}$ from CTL^*_δ to CTL^*_∞ formulas are defined inductively by

$$\begin{array}{rlrl}
\mathscr{D}(p) &= p & \mathscr{E}(p) &= p \\
\mathscr{D}(\neg\varphi) &= \neg\delta \wedge \neg\mathscr{D}(\varphi) & \mathscr{E}(\neg\varphi) &= \neg\mathscr{E}(\varphi) \\
\mathscr{D}(\bigwedge_{i\in I}\varphi_i) &= \bigwedge_{i\in I}\mathscr{D}(\varphi_i) & \mathscr{E}(\bigwedge_{i\in I}\varphi_i) &= \bigwedge_{i\in I}\mathscr{E}(\varphi_i) \\
\mathscr{D}(\exists\psi) &= \exists\mathscr{D}(\psi) & \mathscr{E}(\exists\psi) &= \exists\mathscr{E}(\psi) \\
\mathscr{D}(\neg\psi) &= \neg\delta \wedge \neg\mathscr{D}(\psi) & \mathscr{E}(\neg\psi) &= \neg\mathscr{E}(\psi) \\
\mathscr{D}(\bigwedge_{i\in I}\psi_i) &= \bigwedge_{i\in I}\mathscr{D}(\psi_i) & \mathscr{E}(\bigwedge_{i\in I}\psi_i) &= \bigwedge_{i\in I}\mathscr{E}(\psi_i) \\
\mathscr{D}(\psi\,\mathsf{U}\,\psi') &= \mathscr{D}(\psi)\,\mathsf{U}\,\mathscr{D}(\psi') & \mathscr{E}(\psi\,\mathsf{U}\,\psi') &= (\mathscr{E}(\psi)\,\mathsf{U}\,\delta_{\psi'}) \vee (\mathscr{E}(\psi)\,\mathsf{U}\,\mathscr{E}(\psi')) \\
\mathscr{D}(\infty) &= \neg\mathsf{F}\delta & \mathscr{E}(\delta) &= \neg\top.
\end{array}$$

Here $\delta_{\psi'} = \begin{cases} \delta \text{ if } s_\delta \models \exists\psi' \\ \neg\top \text{ otherwise} \end{cases}$, and $\psi\,\mathsf{U}\,\delta$ abbreviates $\neg\infty \wedge \mathsf{G}\psi$.

We remark that checking whether $s_\delta \models \exists\psi'$ is simple: just substitute $\top$ for δ and $\bot$ for all other atomic propositions in ψ', while simplifying subformulas $\psi_1\,\mathsf{U}\,\psi_2$ to ψ_2. The latter is justified because the unique infinite path starting from s_δ has only itself as suffix.

Theorem 8.5. *Let* K *be a Kripke structure and s a state in* K*. Then for any CTL^*_∞ state formula φ we have $s \models \varphi$ in* K *iff $s \models \mathscr{D}(\varphi)$ in D(K), and for any CTL^*_δ state formula φ we have $s \models \varphi$ in D(K) iff $s \models \mathscr{E}(\varphi)$ in* K*.*

Proof. For a state formula φ, let $[\![\varphi]\!]_\mathrm{K}$ denote the set of states s in K with $s \models \varphi$. Likewise, for a path formula ψ, $[\![\psi]\!]_\mathrm{K}$ denotes the set of maximal paths π in K with $\pi \models \varphi$. Note that there is a bijective correspondence between the maximal paths in K and those in D(K) not starting in s_δ. A straightforward structural induction shows that $[\![\varphi]\!]_\mathrm{K} = [\![\mathscr{D}(\varphi)]\!]_{D(\mathrm{K})}$ for any CTL^*_∞ state formula φ and, up to the aforementioned bijective correspondence, $[\![\psi]\!]_\mathrm{K} = [\![\mathscr{D}(\psi)]\!]_{D(\mathrm{K})}$ for any CTL^*_∞ path formula ψ.

For the second statement, let π_δ be the unique path in D(K) starting in s_δ. A straightforward structural induction shows that $[\![\varphi]\!]_{D(\mathrm{K})} - \{s_\delta\} = [\![\mathscr{E}(\varphi)]\!]_\mathrm{K}$ for any CTL^*_δ state formula φ and, up to the above bijective correspondence, $[\![\psi]\!]_{D(\mathrm{K})} - \{\pi_\delta\} = [\![\mathscr{E}(\psi)]\!]_\mathrm{K}$ for any CTL^*_δ path formula ψ. □

In CTL^*_∞ the path modality ∞ is equally expressive as the path modality $\psi\,\mathsf{U}\,\delta$ of Definition 8.4, saying of a path that it is finite and all its suffixes satisfy ψ. This is because $\pi \models \psi\,\mathsf{U}\,\delta \;\Leftrightarrow\; \pi \models \neg\infty \wedge \mathsf{G}\psi$ and $\pi \models \infty \;\Leftrightarrow\; \pi \models \neg\mathsf{F}\delta \;\Leftrightarrow\; \pi \models \neg\top\,\mathsf{U}\,\delta$. In this light, the encoding $\mathscr{D}$ of CTL^*_∞ into CTL^*_δ merely adds a conjunct $\neg\delta$ here and there. These conjuncts are not optional; they enable, for instance, the correct translation of the CTL^*_∞ path formula $\mathsf{G}p$ by the CTL^*_δ formula $\neg\delta \wedge \mathsf{G}(\delta \vee p)$.

Recall that in Section 6 we considered extending $\mathsf{CTL}^*_{-\mathsf{X}}$ with a state formula δ such that $s \models \delta$ iff $\neg\exists s'.\ s \longrightarrow s'$. We then argued that this would make the resulting logic too expressive. Note that in our current proposal the atomic proposition δ only holds in the fresh state s_δ of the deadlock extension $D(\mathrm{K})$ of a Kripke structure K and not in any of the original states of K. As a consequence, in CTL^*_∞, which does not have the next state modality X, we can express the property that deadlock is unavoidable (when all paths from an original state of K lead to deadlock), but we still cannot express the property of *being deadlocked* (i.e., the property that holds in an original state of K iff no further transitions are possible).

Theorem 8.6. *Also the logics* CTL_δ *and* CTL_∞ *are equally expressive.*

Proof. This follows because $\mathscr{D}$ can be restricted to a mapping from CTL_∞ to CTL_δ formula and $\mathscr{E}$ to a mapping from CTL_∞ to CTL_δ formula. In particular,

$$\mathscr{D}(\exists(\varphi\,\mathsf{U}\,\varphi')) = \exists(\mathscr{D}(\varphi)\,\mathsf{U}\,\mathscr{D}(\varphi')) \qquad \mathscr{D}(\exists\mathsf{G}^\infty\varphi) = \exists\mathsf{G}(\neg\delta \wedge \mathscr{D}(\varphi))$$

$$\mathscr{E}(\exists(\varphi\,\mathsf{U}\,\varphi')) = \begin{cases} \exists(\mathscr{E}(\varphi)\,\mathsf{U}\,\mathscr{E}(\varphi')) \vee \exists(\mathscr{E}(\varphi)\,\mathsf{U}\,(\neg\exists^\infty\mathsf{G}\top \wedge \exists\mathsf{G}\mathscr{E}(\varphi))) & \text{if } s_\delta \models \varphi' \\ \exists(\mathscr{E}(\varphi)\,\mathsf{U}\,\mathscr{E}(\varphi')) & \text{otherwise} \end{cases}$$

and

$$\mathscr{E}(\exists\mathsf{G}\varphi) = \begin{cases} \exists\mathsf{G}^\infty\mathscr{E}(\varphi) & \text{if } s_\delta \models \varphi' \\ \exists\mathsf{G}\,\mathscr{E}(\varphi) & \text{otherwise.} \end{cases}$$

□

9. Linear temporal logic with deadlock detection

Linear Temporal Logic [14] (LTL) is the sublogic of CTL^* that allows propositional variables $p \in \mathbf{AP}$ but no other state formulas to be used as path formulas. Path formulas are applied to states by an implicit universal quantification: $s \models \psi$ iff $s \models \forall\psi$. In this section we explore the programme of this paper in the setting of $\mathsf{LTL}_{-\mathsf{X}}$ (LTL without the next state modality), and compare the results with the branching time case.

First we characterise the equivalence induced on the states of a Kripke structure $(S, \mathscr{L}, \rightarrow)$ by validity of $\mathsf{LTL}_{-\mathsf{X}}$ formulas. We can conveniently use the notion of complete coloured traces in this characterisation, observing that $\mathscr{L}$ is a colouring in the sense of Definition 2.3. We write $s \approx_{\mathscr{L}} t$ if the states s and t have the same complete $\mathscr{L}$-coloured traces. Now two states satisfy the same $\mathsf{LTL}_{-\mathsf{X}}$ formulas iff they have the same complete $\mathscr{L}$-coloured traces.

Theorem 9.1. $s \approx_{\mathscr{L}} t$ *iff* $s \models \psi \Leftrightarrow t \models \psi$ *for all* $\mathsf{LTL}_{-\mathsf{X}}$ *formulas* ψ.

Proof. "Only if": Note that, to show that $s \approx_{\mathscr{L}} t$ implies $s \models \psi \Leftrightarrow t \models \psi$, it suffices to prove that if $\mathscr{L}(\pi) = \mathscr{L}(\rho)$ then $\pi \models \psi \Leftrightarrow \rho \models \psi$. We proceed by structural induction on ψ.

From $\mathscr{L}(\pi) = \mathscr{L}(\rho)$ it follows that the first states of π and ρ have the same colour, and hence if $\psi = p$ with $p \in \mathbf{AP}$ then $\pi \models \psi \Leftrightarrow \rho \models \psi$. The cases $\psi = \neg\psi'$ and $\psi = \bigwedge \Psi'$ follow immediately from the induction hypothesis.

Finally, let $\psi = \psi' \mathsf{U} \psi''$ and suppose that $\pi \models \psi$. Then there exists a suffix π' of π such that $\pi' \models \psi''$ and $\pi'' \models \psi'$ for all $\pi \trianglerighteq \pi'' \rhd \pi'$. As $\mathscr{L}(\pi) = \mathscr{L}(\rho)$, there must be a suffix ρ' of ρ such that $\mathscr{L}(\pi') = \mathscr{L}(\rho')$ and for every path ρ'' such that $\rho \trianglerighteq \rho'' \rhd \rho'$ there exists a path π'' with $\pi \trianglerighteq \pi'' \rhd \pi'$ such that $\mathscr{L}(\pi'') = \mathscr{L}(\rho'')$. By induction, this implies $\rho' \models \psi''$ and $\rho'' \models \psi'$ for all $\rho \trianglerighteq \rho'' \rhd \rho'$. Hence $\rho \models \psi$.

"If": Suppose that $s \not\approx_{\mathscr{L}} t$. Then, without loss of generality, there exists a maximal path ρ from t such that for all maximal paths π from s it holds that $\mathscr{L}(\pi) \neq \mathscr{L}(\rho)$; we define an $\mathsf{LTL}_{-\mathsf{X}}$ formula ψ such that $s \models \psi$, while $t \not\models \psi$.

First, we define for every colour C, which is a subset of $\mathbf{AP}$, a formula $\psi(C)$ with the property that $\pi \models \psi(C)$ iff the first state of π has colour C. (A possible definition of $\psi(C)$ would be $\bigwedge_{p\in C} p \wedge \bigwedge_{p\notin C} \neg p$; however, one can economise on the cardinality of this conjunction by including only one conjunct for every other colour D that actually occurs in the underlying Kripke structure—this way we meet the cardinality restriction imposed in Section 2.) For every maximal path π from s such that $\mathscr{L}(\rho)$ is not a prefix of $\mathscr{L}(\pi)$, let

$$\psi_\pi = (\cdots((\psi(C_0)) \mathsf{U} (\psi(C_1))) \mathsf{U} \cdots) \mathsf{U} (\psi(C_k)) \ ,$$

where $C_0, C_1, \ldots, C_k$ is the shortest prefix of $\mathscr{L}(\rho)$ that is not also a prefix of $\mathscr{L}(\pi)$. For every maximal path π from t such that $\mathscr{L}(\rho)$ *is* a prefix of $\mathscr{L}(\pi)$, let

$$\psi_\pi = \neg(\cdots((\psi(D_0)) \mathsf{U} (\psi(D_1))) \mathsf{U} \cdots) \mathsf{U} (\psi(D_k)) \ ,$$

where $D_0, D_1, \ldots, D_k$ is the shortest prefix of $\mathscr{L}(\pi)$ that is not also a prefix of $\mathscr{L}(\rho)$. Note that in either case we have $\rho \models \psi_\pi$ while $\pi \not\models \psi_\pi$. Now, define ψ by

$$\psi = \neg \bigwedge \{\psi_\pi \mid \pi \text{ a maximal path from } s\} \ .$$

It is not hard to check that in a Kripke structure with less then κ states, for κ an infinite cardinal, less than κ of the formulas ψ_π are different. Now, since ρ is a path from t such that $\rho \not\models \psi$, it follows that $t \not\models \psi$. On the other hand, since $\pi \not\models \psi_\pi$, it follows that $\pi \models \psi$ for all paths π from s, and hence $s \models \psi$. □

In order to lift this notion of equivalence from Kripke structures to LTSs, consider a *trivial colouring* $\mathscr{T}$, assigning the same colour to all states in an LTS, and write $s =^{\lambda}_{T} t$ if s and t have the same complete $\mathscr{T}$-coloured traces. In [8], $=^{\lambda}_{T}$ was called *divergence sensitive trace equivalence*. The following counterpart of Theorem 4.3 indicates that $=^{\lambda}_{T}$ is on LTSs what $\approx_{\mathscr{L}}$ is on Kripke structures:

Theorem 9.2. *On a consistent L^2TS $\approx_{\mathscr{L}}$ equals $=^{\lambda}_{T}$.*

Proof. If π is a path from a state s and ρ a path from t in a consistent $\mathrm{L}^2\mathrm{TS}$ $(S, \mathscr{L}, \rightarrow)$, then

$$\mathscr{L}(\pi) = \mathscr{L}(\rho) \Leftrightarrow \mathscr{L}(s) = \mathscr{L}(t) \wedge \mathscr{T}(\pi) = \mathscr{T}(\rho)$$

where $\mathscr{L}(\pi)$ denotes the $\mathscr{L}$-coloured trace in the associated Kripke structure (thus, forgetting the actions) and $\mathscr{T}(\pi)$ denotes the trivially coloured trace in the associated LTS (thus, keeping the visible actions, but forgetting the colours). This is an immediate consequence of the definition of consistency, and it immediately implies the theorem. □

In order to make LTS-to-L^{2}TS transformations useful for applying LTL on LTSs they should be required to preserve and reflect $=_T^\lambda$—the transformation of [5] trivially has this property. We then obtain:

Corollary 9.3. *Let s and t be states in an LTS, and let η be an LTS-to-L^{2}TS transformation preserving and reflecting $=_T^\lambda$. Then $s =_T^\lambda t$ iff $s \models^\eta \psi \Leftrightarrow t \models^\eta \psi$ for all $\mathsf{LTL}_{-\mathsf{X}}$ formulas ψ.*

The very same counterexample as used in Section 5 shows that $=_T^\lambda$ fails to be a congruence for $\|$: we have $0 =_T^\lambda \Delta 0$, yet $0\|a \neq_T^\lambda \Delta 0\|a$. We proceed to characterise the coarsest congruence for $\|$ that is included in $=_T^\lambda$. We write $s =_T^{\Delta\lambda} t$ if s and t have the same complete $\mathscr{T}$-coloured traces as well as the same divergent $\mathscr{T}$-coloured traces; by analogy with the branching bisimulation variants we propose to call $=_T^{\Delta\lambda}$ *trace equivalence with explicit divergence.*

Theorem 9.4. *$=_T^{\Delta\lambda}$ is the coarsest congruence for $\|$ that is included in $=_T^\lambda$.*

Proof. Let $T(s)$ denote the set of $\mathscr{T}$-coloured traces of a state s, $T^\lambda(s)$ its set of complete $\mathscr{T}$-coloured traces, and $T^\Delta(s)$ its set of divergent ones. Clearly $T^\Delta(s) \subseteq T^\lambda(s) \subseteq T(s)$. Note that $T(s)$ is completely determined by $T^\lambda(s)$, namely as its set of initial prefixes. Furthermore, let $T^*(s)$ denote the set of finite $\mathscr{T}$-coloured traces of s and $T^\infty(s)$ its set of infinite ones. Also $T^*(s)$ and $T^\infty(s)$ are completely determined by $T^\lambda(s)$, and $T^\infty(s) \subseteq T^\lambda(s)$. For any two sets of sequences S and T, let $S\|T$ denote the set of those sequences which can be obtained by interleaving a sequence of S with a sequence of T. Now we have

$$\begin{aligned}
T(s\|t) &= T(s)\|T(t)\\
T^*(s\|t) &= T^*(s)\|T^*(t)\\
T^\infty(s\|t) &= T^\infty(s)\|T(t) \cup T(s)\|T^\infty(s)\\
T^\Delta(s\|t) &= T^\Delta(s)\|T^*(t) \cup T^*(s)\|T^\Delta(s)\\
T^\lambda(s\|t) &= T^\infty(s\|t) \cup T^\Delta(s\|t) \cup T^\lambda(s)\|T^\lambda(t).
\end{aligned}$$

This implies that $=_T^{\Delta\lambda}$ is a congruence. By construction it is included in $=_T^\lambda$.

Now let $\sim$ be any congruence for $\|$ that is included in $=_T^\lambda$, and assume $s \sim u$. We need to show that $s =_T^{\Delta\lambda} u$. We know already that $T^\lambda(s) = T^\lambda(u)$. So let $\sigma \in T^\Delta(u)$. By symmetry, it suffices to show that $\sigma \in T^\Delta(s)$. Let a be an action that does not occur in any path from s. Since $\sim$ is a congruence for $\|$, we have $s \parallel a \sim t \parallel a$, where a is the state from Example 5.3. As $\sim$ is included in $=_T^\lambda$ we obtain $s \parallel a =_T^\lambda t \parallel a$. Since $\sigma \in T^\Delta(u)$ and the empty trace ε is in $T^*(a)$, we have $\sigma \in T^\Delta(u\|a) \subseteq T^\lambda(u\|a) = T^\lambda(s\|a)$. Since $\varepsilon \notin T^\lambda(a)$ it must be that $\sigma \in T^\Delta(s\|a)$ and hence $\sigma \in T^\Delta(s)$. □

So far the situation is analogous with the branching time case. However, from here on the development is different. Adding the ∞-modality to $\mathsf{LTL}_{-\mathsf{X}}$ does not merely add the expressiveness to the logic to make it characterise $=_T^{\Delta\lambda}$. Instead LTL_∞ (obtained from $\mathsf{LTL}_{-\mathsf{X}}$ by adding the ∞-modality) characterises a strictly finer equivalence. We define *$\mathscr{L}$-coloured deadlock traces* as $\mathscr{L}$-coloured traces that stem from finite maximal paths, i.e. paths ending in a deadlock state, and for s, t states in a Kripke structure $(S, \mathscr{L}, \rightarrow)$ we write $s \approx_{\mathscr{L}}^{\Delta\delta} t$ if s and t have the same complete $\mathscr{L}$-coloured traces, the same divergent $\mathscr{L}$-coloured traces, and the same $\mathscr{L}$-coloured deadlock traces. Likewise, for s, t states in an LTS we write $s =_T^{\Delta\delta} t$ if s and t have the same complete $\mathscr{T}$-coloured traces, the same divergent $\mathscr{T}$-coloured traces, and the same $\mathscr{T}$-coloured deadlock traces. In [8], $=_T^{\Delta\delta}$ was called *divergence sensitive completed trace equivalence*. In light of the proof of Theorem 9.2 it is straightforward to establish that on a consistent L^{2}TS the preorders $\approx_{\mathscr{L}}^{\Delta\delta}$ and $=_T^{\Delta\delta}$ coincide.

Theorem 9.5. *$s \approx^{\Delta\delta}_{\mathscr{L}} t$ iff $s \models \psi \Leftrightarrow t \models \psi$ for all LTL_∞ formulas ψ.*

Proof. Let $\mathscr{L}^\delta(\pi)$ be the $\mathscr{L}$-coloured trace of a path π as given in Definition 2.3, but with a symbol δ tagged at the end iff π is finite and maximal (i.e. ending in deadlock). Then $s \approx^{\Delta\delta}_{\mathscr{L}} t$ iff for every path π from s there is a path ρ from t such that $\mathscr{L}^\delta(\pi) = \mathscr{L}^\delta(\rho)$, and vice versa.

"Only if": To show that $s \approx^{\Delta\delta}_{\mathscr{L}} t$ implies $s \models \psi \Leftrightarrow t \models \psi$, it suffices to prove that if $\mathscr{L}^\delta(\pi) = \mathscr{L}^\delta(\rho)$ then $\pi \models \psi \Leftrightarrow \rho \models \psi$. This proceeds exactly as in the proof of Theorem 9.1, except that there is one extra case to consider, namely that $\psi = \infty$: Suppose $\pi \models \infty$. Then $\mathscr{L}^\delta(\pi)$ does not end in δ, so $\mathscr{L}^\delta(\rho)$ does not end in δ, so $\rho \models \infty$.

"If": Suppose that $s \not\approx^{\Delta\delta}_{\mathscr{L}} t$. Then, without loss of generality, there exists a maximal path ρ from t such that for all maximal paths π from s it holds that $\mathscr{L}^\delta(\pi) \neq \mathscr{L}^\delta(\rho)$. As in the proof of Theorem 9.1 we define an $\mathsf{LTL}_{-\mathsf{X}}$ formula ψ such that $s \models \psi$, while $t \not\models \psi$. For π a maximal path from s such that $\mathscr{L}(\pi) \neq \mathscr{L}(\rho)$, we define the formula ψ_π exactly as in the proof of Theorem 9.1. In case $\mathscr{L}(\pi) = \mathscr{L}(\rho)$ but $\mathscr{L}^\delta(\pi) \neq \mathscr{L}^\delta(\rho)$ we take ψ_π to be ∞ or $\neg\infty$. The definition of ψ remains the same. □

Corollary 9.6. *Let s and t be states in an LTS, and let η be an LTS-to-L^2TS transformation preserving and reflecting $=^{\Delta\delta}_T$. Then $s =^{\Delta\delta}_T t$ iff $s \models^\eta \psi \Leftrightarrow t \models^\eta \psi$ for all LTL_∞ formulas ψ.*

The deadlock extension of Definition 8.1 gives the same result.

Theorem 9.7. *Let s and t be states in an LTS, and let η be an LTS-to-L^2TS transformation preserving and reflecting $=^{\Delta\delta}_T$. Then $s =^{\Delta\delta}_T t$ iff $s \models^{D\circ\eta} \psi \Leftrightarrow t \models^{D\circ\eta} \psi$ for all $\mathsf{LTL}_{-\mathsf{X}}$ formulas ψ.*

Proof. Just like Corollary 8.3, this follows immediately from the observations that $s \approx^{\Delta\delta}_{\mathscr{L}} t$ within a Kripke structure K iff $s \approx^{\Delta\delta}_{\mathscr{L}} t$ within the Kripke structure $D(\mathrm{K})$ (cf. Theorem 8.2), and that on total Kripke structures the equivalence relations $\approx^{\Delta\delta}_{\mathscr{L}}$ and $\approx_{\mathscr{L}}$ coincide. □

Kaivola & Valmari [11] study equivalences on LTSs with the property that under all plausible transformations of LTSs into Kripke structures two equivalent states (transformed into states of Kripke structures) satisfy the same formulas in either $\mathsf{LTL}_{-\mathsf{X}}$ or LTL_∞. They characterise the coarsest such congruences for a selection of standard process algebra operators—including the merge, but also a partially synchronous parallel composition as well as nondeterministic choice—as *NDFD*-equivalence (for $\mathsf{LTL}_{-\mathsf{X}}$) and *CFFD*-equivalence (for LTL_∞). In turns out that neither $=^{\Delta\lambda}_T$ nor $=^{\Delta\delta}_T$ are congruences for the partially synchronous parallel composition, or for nondeterministic choice. Hence to satisfy the requirement of being a congruence for these operators, *NDFD*-equivalence is necessarily finer than $=^{\Delta\lambda}_T$, and *CFFD*-equivalence is necessarily finer than $=^{\Delta\delta}_T$. The question of raising the expressiveness of $\mathsf{LTL}_{-\mathsf{X}}$ to the level where it characterises NDFD- or CFFD-equivalence directly remains open.

10. Conclusion

In this paper we enabled $\mathsf{CTL}_{-\mathsf{X}}$ and $\mathsf{CTL}^*_{-\mathsf{X}}$ to be used as logics on labelled transition systems (LTSs) while taking deadlock behaviour into account. This could be accomplished by adding a modality to $\mathsf{CTL}^*_{-\mathsf{X}}$, by adapting the semantics of the G-modality (in $\mathsf{CTL}_{-\mathsf{X}}$), or by adapting the translations from [5] from LTSs to Kripke structures. We have shown that these approaches all lead to equally expressive logics on LTSs. Our work allows the

rich tradition of verification by equivalence checking to be combined with the full expressive power of $\mathsf{CTL}^*_{-\mathsf{X}}$. Taking advantage of this possibility is left for further research.

Acknowledgements. We are grateful to the referees for their many helpful suggestions.

References

[1] L. Aceto, W.J. Fokkink & C. Verhoef (2001): *Structural operational semantics.* In J.A. Bergstra, A. Ponse & S.A. Smolka, editors: *Handbook of Process Algebra*, Elsevier, pp. 197-292.

[2] J.A. Bergstra, A. Ponse & S.A. Smolka, editors (2001): *Handbook of Process Algebra*, Elsevier.

[3] M.C. Browne, E.M. Clarke & O. Grumberg (1988): *Characterizing finite Kripke structures in propositional temporal logic. Theoretical Computer Science* 59, pp. 115–131.

[4] R. De Nicola & F.W. Vaandrager (1990): *Action versus State based Logics for Transition Systems.* In I. Guessarian, editor: Proceedings LITP Spring School on Theoretical Computer Science: *Semantics of Systems of Concurrent Processes*, La Roche Posay, France 1990. LNCS 469, Springer, pp. 407-419.

[5] R. De Nicola & F.W. Vaandrager (1995): *Three logics for branching bisimulation. Journal of the ACM* 42(2), pp. 458–487.

[6] E.A. Emerson & E.M. Clarke (1982): *Using branching time temporal logic to synthesize synchronization skeletons. Science of Computer Programming* 2(3), pp. 241–266.

[7] E.A. Emerson & J.Y. Halpern (1986): *'Sometimes' and 'Not Never' revisited: on branching time versus linear time temporal logic. Journal of the ACM* 33(1), pp. 151–178.

[8] R.J. van Glabbeek (1993): *The linear time - branching time spectrum II.* In E. Best, editor: *Proceedings CONCUR'93*, LNCS 715, Springer, pp. 66–81.

[9] R.J. van Glabbeek (2005): *A characterisation of weak bisimulation congruence.* In A. Middeldorp, V. van Oostrom, F. van Raamsdonk & R. de Vrijer, editors: *Processes, Terms and Cycles: Steps on the Road to Infinity: Essays Dedicated to Jan Willem Klop on the Occasion of His 60th Birthday*, LNCS 3838, Springer, pp. 26–39.

[10] R.J. van Glabbeek & W.P. Weijland (1996): *Branching time and abstraction in bisimulation semantics. Journal of the ACM* 43(3), pp. 555–600.

[11] R. Kaivola & A. Valmari (1992): *The weakest compositional semantic equivalence preserving Nexttime-less Linear Temporal Logic.* In W.R. Cleaveland, editor: *Proceedings CONCUR'02*, LNCS 630, Springer, pp. 207–221.

[12] D. Kozen (1983): *Results on the propositional mu-calculus. Theoretical Computer Science* 27, pp. 333–354.

[13] R. Milner (1989): *Communication and Concurrency.* Prentice Hall, Englewood Cliffs.

[14] A. Pnueli (1977): *The Temporal Logic of Programs.* In *Proceedings FOCS'77*, IEEE Computer Society Press, pp. 46-57.

[15] Y.S. Ramakrishna & S. Smolka (1997): *Partial-order reduction in the weak modal mu-calculus.* In A. Mazurkiewicz & J. Winkowski, editors: *Proceedings CONCUR'97*, LNCS 1243, Springer, pp. 5–24.

[16] N. Trčka (2007): *Silent Steps in Transition Systems and Markov Chains.* PhD thesis, Eindhoven University of Technology.