Stutter Equivalence for Infinite State Systems

Zhendong Su

EECS Department, University of California, Berkeley
zhendong@cs.berkeley.edu

Abstract. In this paper, we study the state equivalences related to stuttering and how they relate to various temporal logics without the next-time operator. We first show that stutter closure of bisimilarity is not an abstract semantics for $\mathrm{STL}^{\mathcal{U}}$. Then we suggest a new logic $\mathrm{STL}^{\mathcal{AU}}$, which is a restricted subset of the logic $\mathrm{STL}^{\mathcal{U}}$. We show that stutter closure of bisimilarity is a full abstract semantics for $\mathrm{STL}^{\mathcal{AU}}$. Next, we suggest a new state equivalence *until-bisimilarity* and show that it is a full abstract semantics for $\mathrm{STL}^{\mathcal{U}}$. Finally we extend the results to other logics without the next-time operator.

1 Introduction

In formal verification, property preserving abstractions are very important for combating the *state-space explosion* problem. Thus, it is important to study when two states of an observation structure satisfy the same set of properties specifiable by logics [1].

A *state equivalence* $\simeq$ is a family of relations such that for each observation structure, it induces a equivalence relation on the states of that structure. A few common state equivalences are the *observational equivalence* $\approx$, which distinguishes any two states with different observations, the *state equivalence* $=$, which distinguishes any two different states, and the *universal equivalence*, which does not distinguish between any two states.

Bisimilarity is an important and well-studied state equivalence. It is fully characterized by a few state logics including STL, CTL, and CT_{μ}. It is usually the most stringent state equivalence one will consider. Properties specified by these temporal logics can be checked on the quotient structure with respect to bisimilarity.

In some systems, especially asynchronous systems, the system may stay in the same observable state for many rounds. This is called *stuttering*. For this kind of systems, sometimes we do not care how many rounds the system stays in the same observable state before making a transition to a state with different observable behavior. In this case, instead of considering the original transition system, it makes sense to consider its *stutter closure*, in which we add a transition that bypasses all these states with the same observations. We thus have a notion of the stutter closure of state equivalences, that is two states are *stutter closed X equivalent* if they are X equivalent in the stutter closure, where X stands for any state equivalence.

With this notion of stutter closure of state equivalences, it is natural for one to conjecture that the stutter closure of bisimilarity might be a full characterization of state logics without the next operator such as $\mathrm{STL}^{\mathcal{U}}$ and $\mathrm{CTL}_{-\bigcirc}$. The objective of this paper is to study this notion. It is quite counter-intuitive for us to find out that the stutter closure of bisimilarity is not an abstract semantics for $\mathrm{STL}^{\mathcal{U}}$, and thus not an abstract semantics for $\mathrm{CTL}_{-\bigcirc}$ either. However, we are able to show that the stutter closure of bisimilarity is a full abstraction of restricted subsets of $\mathrm{STL}^{\mathcal{U}}$ and $\mathrm{CTL}_{-\bigcirc}$. The restriction is somewhat natural since it is not difficult to show that the stutter closure of bisimilarity is an abstract semantics for LTL without the next-time operator, and the restriction in a sense mimics that LTL considers linear trajectories instead of branching trees. Another aspect of this work is the suggestion of a new state equivalence *until-bisimilarity* and proving that it is a full abstraction of $\mathrm{STL}^{\mathcal{U}}$ and $\mathrm{CTL}_{-\bigcirc}$.

The rest of the paper is structured as follows. We first provide some definitions. In particular, we define what are state equivalences and the stutter closure of state equivalences (Section 2). Next, we establish the relationship between stutter closure of bisimilarity and the logic $\mathrm{STL}^{\mathcal{U}}$ (Section 3). We show that stutter closure of bisimilarity is not an abstract semantics of $\mathrm{STL}^{\mathcal{U}}$, and suggest a subset of $\mathrm{STL}^{\mathcal{U}}$ for which the stutter closure of bisimilarity is its full abstraction. We then define a new state equivalence and show that it is a full abstract semantics for $\mathrm{STL}^{\mathcal{U}}$ (Section 4). Next, we consider the other logics without the next time operator and study their relations with stutter closure of state equivalences (Sections 5, 6, 7, and 8). Finally we conclude (Section 9).

2 State Equivalences and Their Stutter Closures

In this section, we define state equivalences and the stutter closures of them. These definitions are taken from [1].

Let $\simeq_1$ and $\simeq_2$ be two state equivalences, we say that they $\simeq_1$ is *as distinguishing as* the state equivalence $\simeq_2$, written as $\simeq_2 \sqsubseteq \simeq_1$, if for all observation structures K, the equivalence $\simeq_1^K$ refines the equivalence $\simeq_2^K$, i.e., each $\simeq_2^K$ equivalence class is a union of $\simeq_1^K$ equivalence classes. We say that $\simeq_1$ and $\simeq_2$ are *equally distinguishing* if $\simeq_1 \sqsubseteq \simeq_2$ and $\simeq_2 \sqsubseteq \simeq_1$. The state equivalences $\simeq_1$ and $\simeq_2$ are *incomparable* if $\simeq_1 \not\sqsubseteq \simeq_2$ and $\simeq_2 \not\sqsubseteq \simeq_1$. The state equivalence $\simeq_1$ is *more distinguishing* than the state equivalence $\simeq_2$ if $\simeq_2 \sqsubseteq \simeq_1$ and $\simeq_1 \not\sqsubseteq \simeq_2$.

A very important state equivalence is called *bisimilarity*. It is less distinguishing than state equivalence, but more distinguishing than observation equivalence. Bisimilarity is the state equivalence induced by the coarsest stable refinement of observation equivalence. Below we give an alternative definition of bisimilarity.

Definition 1 (Bisimilarity). *Let $K = (\Sigma, \sigma^I, \rightarrow, A, \langle\!\langle\cdot\rangle\!\rangle)$ be an observation structure. The state equivalence π on the states of K is a* bisimulation *of K if (1) the partition Σ/π is a stable partition of K and (2) π refines the observational equivalence. Thus, for all states s and t of K, if $s\pi t$ then*

(1) $\langle\!\langle s\rangle\!\rangle = \langle\!\langle t\rangle\!\rangle$;

(2) if $s \to s'$, then there is a state t' such that $t \to t'$ and $s'\pi t'$;
(3) if $t \to t'$, then there is a state s' such that $s \to s'$ and $s'\pi t'$.

Two states s and t of K are bisimilar *iff there is a bisimulation π of K such that $s\pi t$.*

Alternatively, bisimilarity can be characterized by the so-called *i-step bisimilarity* when we view it as games between two players [1].

Definition 2 (i-step bisimilarity). *The state equivalences $\approx^i$, called i-*step bisimilarity *for each natural number i, are defined inductively. The state equivalence $\approx^0$ coincides with observational equivalence; that is, $\approx^0 = \approx$. For each natural number i, for every observation structure $K = (\Sigma, \sigma^I, \to, A, \langle\!\langle \cdot \rangle\!\rangle)$, and for all states s and t of K, let $s \approx^{i+1}_K t$ iff*

(1) $\langle\!\langle s \rangle\!\rangle = \langle\!\langle t \rangle\!\rangle$;
(2) if $s \to s'$, then there is a state t' such that $t \to t'$ and $s' \approx^i_K t'$;
(3) if $t \to t'$, then there is a state s' such that $s \to s'$ and $s' \approx^i_K t'$.

Intuitively, two states are bisimilar iff for all natural number i, the two states are i-step bisimilar. The following proposition makes the intuition precise.

Proposition 1. *Bisimilarity $\simeq^B$ equals the intersection $\bigcup_{i \in \mathbb{N}} \approx^i$ of the i-step bisimilarity equivalences.*

A reactive module *stutters* when its observable states stays unchanged for some number of update rounds. An asynchronous module may stutter in every update round. For many of the properties the number of rounds for which a module stutters before updating its observation is irrelevant, we can combine many of these rounds into a single rounds. This suggests that we add a transition from state s to state t if there is a trajectory from s to t on which the observation stays unchanged.

Definition 3 (Stutter Closure). *Let $K = (\Sigma, \sigma^I, \to, A, \langle\!\langle \cdot \rangle\!\rangle)$ be an observation structure. For two states s and t of K, let $s \to^S t$ if there is an source-s K-trajectory $\overline{s}_{0..m}$ such that (1) for all $0 \le i < m$, $\langle\!\langle s_i \rangle\!\rangle = \langle\!\langle s \rangle\!\rangle$, and (2) $s_m = t$. The relation $\to^S$ is called the* stutter-closed transition relation *of K. The* stutter closure *K^S is the observation structure $(\Sigma, \sigma^I, \to^S, A, \langle\!\langle \cdot \rangle\!\rangle)$.*

Remark 1. Notice that it is not necessarily the case that the stutter closure of an observation structure K is again an observation structure. Thus, when we discuss properties about stutter closures, it only makes sense to work with structures whose stutter closure is again an observation structure. In the rest of the discussion, we consider only observations structures whose stutter closure is again an observation structure.

Definition 4 (Stutter Closure of State Equivalences). *Let $\simeq$ be a state equivalence, and let K be an observation structure. For two states s and t of K, $s \cong_K t$, for the stutter closure $\cong$ of $\simeq$, if $s \simeq_{K^S} t$. The induced state equivalence $\cong$ is called the* stutter closure *of $\simeq$. The state equivalence $\simeq$ is* stutter-insensitive *if $\cong = \simeq$.*

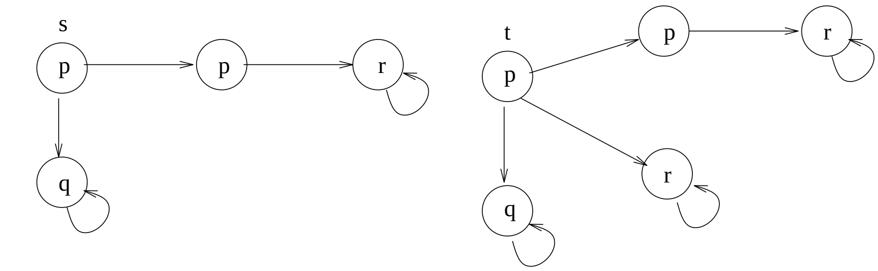

Fig. 1. An observation structure.

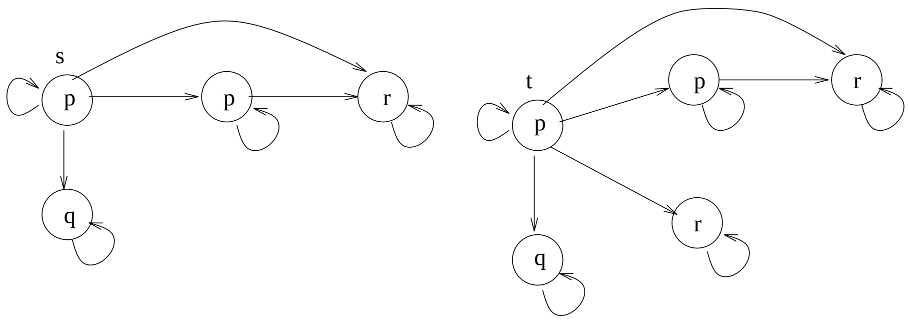

Fig. 2. The stutter closure of the observation structure in Figure 1.

We denote by $\cong^B$ the stutter closure of bisimilarity ($\mathcal{SB}$).

Definition 5 (i-step Stutter-closed Bisimilarity). *Let K be an observation structure, two states s and t are i-step stutter-closed bisimilar iff they are i-step bisimilar in K^S, the stutter closure of K.*

3 $\mathcal{SB}$ and STL$^{\mathcal{U}}$

In this section, we study the relation between the stutter closure of bisimilarity and the state logic STL$^{\mathcal{U}}$.

3.1 $\mathcal{SB}$ is not an Abstract Semantics of STL$^{\mathcal{U}}$

It is very tempting to think that the stutter closure of bisimilarity is an abstract semantics for STL$^{\mathcal{U}}$. However this is not the case.

Consider the observation structure in Figure 1 and its stutter closure in Figure 2. Notice that the states s and t are stutter-closed bisimilar. However for the STL$^{\mathcal{U}}$ formula $\phi = (p\exists\mathcal{U}q)\exists\mathcal{U}r$, we have $t \models_K \phi$, but $s \not\models_K \phi$. Thus, the stutter closure of bisimilarity is not an abstract semantics for STL$^{\mathcal{U}}$.

3.2 $\mathcal{SB}$ is a Full Abstraction of STL$^{A\mathcal{U}}$

In this part, we define a temporal logic STL$^{A\mathcal{U}}$ which is a restricted subset of STL$^{\mathcal{U}}$ and show that $\mathcal{SB}$ is a full abstract semantics for this logic.

Definition 6 (STL$^{A\mathcal{U}}$)**.** *The logic* STL$^{A\mathcal{U}}$ *is a subset of* STL$^{\mathcal{U}}$*. Formulas of the logic are described by the grammar*

$$\phi ::= p \mid \phi_1 \vee \phi_2 \mid \neg\phi \mid p\exists\mathcal{U}\phi$$

where p ranges over atomic formulas over observations.

Proposition 2. *The state equivalence stutter-closed bisimilarity is a full abstract semantics for* STL$^{A\mathcal{U}}$*.*

Proposition 2 follows from Lemma 1 and 2.

Lemma 1. *Stutter-closed bisimilarity is an abstract semantics for* STL$^{A\mathcal{U}}$*.*

Proof. Let K be an observation structure. We wish to show that for any STL$^{A\mathcal{U}}$ formula ϕ for any two states s and t with $s \cong^B t$, $s \models_K \phi$ iff $t \models_K \phi$. We prove the statement by an induction on the structure of ϕ.

$\phi = p$ for some atomic formula p.
 Since $\langle\langle s\rangle\rangle = \langle\langle t\rangle\rangle$, $s \models_K p$ iff $t \models_K p$.
$\phi = \phi_1 \vee \phi_2$.
 $s \models_K \phi$ iff $s \models_K \phi_1$ or $s \models_K \phi_2$ iff $t \models_K \phi_1$ or $t \models_K \phi_2$ iff $t \models_K \phi$.
$\phi = \neg\phi_1$.
 $s \models_K \phi$ iff $s \not\models_K \phi_1$ iff $t \not\models_K \phi_1$ iff $t \models_K \phi$.
$\phi = p\exists\mathcal{U}\phi_1$.
 Assume $s \cong^B t$. Suppose $s \models_K \phi$. Then there exists a source s trajectory $s_0 = s, \ldots, s_k$ such that $s_i \models_K p$ for $0 \leq i < k$ and $s_k \models_K \phi_1$. Since $s \cong^B t$, there exists a source t trajectory $t_0 = t, \ldots, t_k$ in K_S, the stutter closure of K, with $s_i \cong^B t_i$ for $0 \leq i \leq k$. Thus there exists a source t trajectory $u_0 = t, \ldots, u_l = t_k$ in K such that $u_i \models_K p$ and $u_l \models_K \phi_1$. Hence $t \models_K \phi$. Symmetrically, we can show that if $t \models_K \phi$ then $s \models_K \phi$. Thus, $s \models_K \phi$ iff $t \models_K \phi$.

Lemma 2. *For any observation structure K, any two non $\mathcal{SB}$ states can be distinguished by a* STL$^{A\mathcal{U}}$ *formula.*

Proof. Let K be an observation structure. We show that for any natural number i, any two states s and t which are not i-step stutter-closed bisimilar can be distinguished by a STL$^{A\mathcal{U}}$ formula ϕ, i.e., $s \models_K \phi$ but $t \not\models_K \phi$. The proof is by induction on i.

1. Base case: $i = 0$. We can simply let $\phi = \langle\langle s\rangle\rangle$ since 0-step stutter-closed bisimilarity coincides with the observational equivalence $\approx$.

2. Inductive case: $i = k+1$. Assume s and t are not $(k+1)$-step stutter-closed bisimilar. Further we can assume that s and t are k-step stutter-closed bisimilar, otherwise, by induction, there is a STL$^{A\mathcal{U}}$ formula ϕ such that $s \models_K \phi$ but $t \not\models_K \phi$.
   Since s and t are not $(k+1)$-step stutter-closed bisimilar, then either (1) there exists a state s' with $s \rightarrow_K s'$ and for all t' with $t \rightarrow_{K^S} t'$, we have s' and t' are not k-step stutter-closed bisimilar; or (2) there exists a state t' with $t \rightarrow_K t'$ and for all s' with $s \rightarrow_{K^S} s'$, we have t' and s' are not k-step stutter-closed bisimilar. W.L.O.G., assume (1) holds. Notice that there are only finitely many t' with $t \rightarrow_{K^S} t'$ and $\langle\!\langle t' \rangle\!\rangle = \langle\!\langle s' \rangle\!\rangle$, since K^S is an observation structure. Denote the set of such t''s by S, i.e., $S = \{t' \mid t \rightarrow_{K^S} t' \wedge \langle\!\langle t' \rangle\!\rangle = \langle\!\langle s' \rangle\!\rangle\}$. Consider the following STL$^{A\mathcal{U}}$ formula

$$\phi = \langle\!\langle s \rangle\!\rangle \exists\mathcal{U}(\langle\!\langle s' \rangle\!\rangle \wedge (\bigwedge_{t' \in S} \psi(s', t')))$$

   where $\psi(s', t')$ is any STL$^{A\mathcal{U}}$ such that $s' \models_K \psi(s', t')$ but $t' \not\models_K \psi(s', t')$. Such formulas exist by induction.
   Clearly $s \models_K \phi$. However, $t \not\models_K \phi$. Since if it were, then there exists a source-t trajectory $t_0 = t, \ldots, t_k$ such that $\langle\!\langle t_i \rangle\!\rangle = \langle\!\langle s \rangle\!\rangle$ for $0 \leq i < k$ and $t_k \models_K (\langle\!\langle s' \rangle\!\rangle \wedge \bigwedge_{t' \in S} \psi(s', t'))$. Thus $t_k \in S$ since $\langle\!\langle t_k \rangle\!\rangle = \langle\!\langle s' \rangle\!\rangle$. Hence we have $t_k \models_K \psi(s', t_k)$, a contradiction.

4 A Full Abstraction of STL$^{\mathcal{U}}$

In this section, we introduce a new state equivalence *until-bisimilarity*. It is denoted by $\simeq^{\mathcal{U}B}$. We show that $\simeq^{\mathcal{U}B}$ is a full abstract semantics of STL$^{\mathcal{U}}$.

Definition 7 (Until-Bisimilar). *Let K be an observation structure, two states s and t are* until-bisimilar, *denoted by $s \simeq_K^{\mathcal{U}B} t$, iff*

(1) $\langle\!\langle s \rangle\!\rangle = \langle\!\langle t \rangle\!\rangle$;
(2) for every states s' with $s \rightarrow s'$, there exists a source t trajectory $t_0 = t, \ldots, t_k$, such that $t_i \simeq_K^{\mathcal{U}B} s$ for $0 < i < k$ and $t_k \simeq_K^{\mathcal{U}B} s'$;
(3) for every states t' with $t \rightarrow t'$, there exists a source s trajectory $s_0 = s, \ldots, s_k$, such that $s_i \simeq_K^{\mathcal{U}B} t$ for $0 < i < k$ and $s_k \simeq_K^{\mathcal{U}B} t'$.

As in the case of bisimilarity, we can have a similar notion of *i-step until-bisimilarity.*

Definition 8. *We define i-*step until-bisimilarity *denoted by $\sim^i$ inductively. The state equivalence $\sim^0$ is the same as the observational equivalence, i.e., $\sim^0 = \approx$. For any observation structure K and natural number i, two states s and t of K are $(i+1)$-step until bisimilar, that is $s \sim^{i+1} t$ iff*

(1) $\langle\!\langle s \rangle\!\rangle = \langle\!\langle t \rangle\!\rangle$;

(2) for every state s' such that $s \to s'$, there exists a source t trajectory $t_0 = t, \ldots, t_k$ such that $t_i \sim^i s$ for $0 < i < k$ and $t_k \sim^i s'$;
(3) for every state t' such that $t \to t'$, there exists a source s trajectory $s_0 = s, \ldots, s_k$ such that $s_i \sim^i t$ for $0 < i < k$ and $s_k \sim^i t'$.

Proposition 3. *Until-Bisimilarity $\simeq^{\mathcal{U}B}$ equals the intersection $\bigcap_{i\in\mathbb{N}} \sim^i$ of the i-step until-bisimilarity. In other words, for any observation structure K, for any states s and t of K, $s \simeq^{\mathcal{U}B}_K t$ iff $s \sim^i t$ for all i.*

In the rest of the section, we show that until-bisimilarity is a fully abstract semantics of $\mathrm{STL}^{\mathcal{U}}$.

Proposition 4. *The state equivalence until-bisimilarity $\simeq^{\mathcal{U}B}$ is a fully abstract semantics for $\mathrm{STL}^{\mathcal{U}}$.*

Proposition 4 follows from Lemma 3 and 4.

Lemma 3. *Until-bisimilarity is an abstract semantics for $\mathrm{STL}^{\mathcal{U}}$.*

Proof. Let K be an observation structure. We wish to show that for any two states s and t with $s \simeq^{\mathcal{U}B}_K t$, for any $\mathrm{STL}^{\mathcal{U}}$ formula ϕ, $s \models_K \phi$ iff $t \models_K \phi$. We prove the statement by an induction on the structure of ϕ.

$\phi = p$ for some atomic formula p.
Since $\langle\!\langle s \rangle\!\rangle = \langle\!\langle t \rangle\!\rangle$, $s \models_K p$ iff $t \models_K p$.
$\phi = \phi_1 \vee \phi_2$.
$s \models_K \phi$ iff $s \models_K \phi_1$ or $s \models_K \phi_2$ iff $t \models_K \phi_1$ or $t \models_K \phi_2$ iff $t \models_K \phi$.
$\phi = \neg\phi_1$.
$s \models_K \phi$ iff $s \not\models_K \phi_1$ iff $t \not\models_K \phi_1$ iff $t \models_K \phi$.
$\phi = \phi_1 \exists\mathcal{U} \phi_2$.
Assume $s \simeq^{\mathcal{U}B} t$. Suppose $s \models_K \phi$. Then there exists a source s trajectory $s_0 = s, \ldots, s_k$ such that $s_i \models_K \phi_1$ for $0 \leq i < k$ and $s_k \models_K \phi_2$. Since $s \simeq^{\mathcal{U}B} t$, for each transition $s_i \to s_{i+1}$ with $0 \leq i < k$ there exists a source t_i trajectory $u_0 = t_i, \ldots, u_l$ with $u_j \simeq^{\mathcal{U}B} s_i$ for $0 \leq j < l$ and $u_l \simeq^{\mathcal{U}B} s_{i+1}$. Thus by conjoining all these trajectories, we get a source t trajectory $t_0 = t, \ldots, t_m$. By induction, we have $t_i \models_K \phi_1$ for $0 \leq i < m$ and $t_m \models_K \phi_2$. Thus, $t \models_K \phi$. Symmetrically, we can show that if $t \models_K \phi$ then $s \models_K \phi$. Thus, $s \models_K \phi$ iff $t \models_K \phi$.

Lemma 4. *Let K be an observation structure. Any two non-until-bisimilar states s and t of K can be distinguished by an $\mathrm{STL}^{\mathcal{U}}$ formula ϕ, i.e., $s \models_K \phi$ but $t \not\models_K \phi$.*

Proof. Let K be an observation structure. We show that for any natural number i, any two states s and t which are not i-step until-bisimilar can be distinguished by an $\mathrm{STL}^{\mathcal{U}}$ formula ϕ, i.e., $s \models_K \phi$ but $t \not\models_K \phi$. The proof is by induction on i.

1. Base case: $i = 0$. We can simply let $\phi = \langle\!\langle s \rangle\!\rangle$ since 0-step until-bisimilarity coincides with the observational equivalence $\approx$.

2. Inductive case: $i = k+1$. Assume s and t are not $(k+1)$-step until-bisimilar. Further we assume that s and t are k-step until-bisimilar, otherwise, by induction, there is a STL$^{\mathcal{U}}$ formula ϕ such that $s \models_K \phi$ but $t \not\models_K \phi$.
   Since s and t are not $(k+1)$-step until-bisimilar, then either (1) there exists a state s' with $s \rightarrow_K s'$ and for all source t trajectory $t_0 = t, \ldots, t_k$ with $\langle\!\langle t_i \rangle\!\rangle = \langle\!\langle t \rangle\!\rangle$ for $0 \leq i < k$ and $\langle\!\langle t_k \rangle\!\rangle = \langle\!\langle s' \rangle\!\rangle$ either one of the following holds
   (a) t_k and s' are not i-step until-bisimilar;
   (b) there exists $0 < i < k$ such that t_i and s are not i-step until-bisimilar.

   or (2) there exists a state t' with $t \rightarrow_K t'$ and for all source s trajectory $s_0 = s, \ldots, s_k$ with $\langle\!\langle s_i \rangle\!\rangle = \langle\!\langle t \rangle\!\rangle$ for $0 \leq i < k$ and $\langle\!\langle s_k \rangle\!\rangle = \langle\!\langle t' \rangle\!\rangle$ either one of the following holds
   (a) s_k and t' are not i-step until-bisimilar;
   (b) there exists $0 < i < k$ such that s_i and t are not i-step until-bisimilar.

   W.L.O.G., assume (1) holds. Notice that there are only finitely many such trajectories since K^S is an observation structure itself. Denote by S_1 the set of states on the trajectories for which (a) is violated, and by S_2 for which (b) is violated. Let $\phi_1 = \bigwedge_{u \in S_2} \psi(s, u)$ and $\phi_2 = \bigwedge_{u \in S_1} \psi(s', u)$, where $\psi(u, v)$ is any STL$^{\mathcal{U}}$ formula such that $u \models_K \psi(u, v)$ but $v \not\models_K \psi(u, v)$. Such formulas exist by induction. Now consider the formula $\phi = (\langle\!\langle s \rangle\!\rangle \wedge \phi_1) \exists\mathcal{U} (\langle\!\langle s' \rangle\!\rangle \wedge \phi_2)$. Clearly $s \models_K \phi$ and $t \not\models_K \phi$.

Remark 2. In both of the proofs of Proposition 2 and Proposition 4, we assumed that K^S to be an observation structure. For STL$^{A\mathcal{U}}$ this is a natural assumption. For STL$^{\mathcal{U}}$, it is also a natural and not very strong assumption. Since when we use STL$^{\mathcal{U}}$ formulas to describe system properties, we do not care how many rounds the system stutters. Thus it is natural to require the stutter closure again an observation structure.

5 CTL without the Next-Time Operator

In this section, we extend the results from previous sections to two subsets of CTL without the next-time operator. One is analogous to STL$^{A\mathcal{U}}$ and the other is analogous to STL$^{\mathcal{U}}$.

The logic CTL$^{A}_{-\bigcirc}$ is defined by the grammar

$$\phi ::= p \mid \neg\phi \mid \phi \vee \phi \mid p \exists\mathcal{U} \phi \mid \exists\Box p$$

where p ranges over atomic formulas on observations.

The logic CTL$_{-\bigcirc}$ is defined by the grammar

$$\phi ::= p \mid \neg\phi \mid \phi \vee \phi \mid \phi \exists\mathcal{U} \phi \mid \exists\Box \phi$$

where p ranges over atomic formulas on observations.

We can show that the stutter closure of bisimilarity is also a full abstract semantics of CTL$^{A}_{-\bigcirc}$, and the until-bisimilarity is a full abstract semantics of CTL$_{-\bigcirc}$.

Proposition 5. *The stutter closure of bisimilarity is a full abstract semantics for* $\mathrm{CTL}^{A}_{-\bigcirc}$.

Proposition 6. *The state equivalence until-bisimilarity is a full abstract semantics for* $\mathrm{CTL}_{-\bigcirc}$.

The proofs for the above two propositions are straight forward, with only simple applications of König's Lemma, thus omitted from the paper.

6 LTL without the Next-Time Operator

In this section, we study the relationship between stutter closure of bisimilarity and LTL without the next time operator. We denote the logic LTL without the next-time operator by $\mathrm{LTL}_{-\bigcirc}$. It is defined by the grammar

$$\phi ::= p \mid \phi \vee \phi \mid \neg\phi \mid \phi\mathcal{U}\phi$$

where p ranges over atomic formulas on observations.

Proposition 7. *The state equivalence stutter closure of bisimilarity is an abstract semantics for* $\mathrm{LTL}_{-\bigcirc}$.

Definition 9 (Stutter Trace Equivalence). *Let $\underline{a}$ and $\underline{b}$ be two ω-trajectories. We say that $\underline{a}$ and $\underline{b}$ are* stutter trace equivalent, *iff*

(1) $\langle\!\langle a_0\rangle\!\rangle = \langle\!\langle b_0\rangle\!\rangle$; *and*
(2) For i such that $\langle\!\langle a_k\rangle\!\rangle = \langle\!\langle a_0\rangle\!\rangle$ for $0 \le k < i$ and $\langle\!\langle a_i\rangle\!\rangle \neq \langle\!\langle a_0\rangle\!\rangle$, there exists a j such that $\langle\!\langle b_k\rangle\!\rangle = \langle\!\langle b_0\rangle\!\rangle$ for $0 \le k < j$ and $\langle\!\langle b_j\rangle\!\rangle \neq \langle\!\langle b_0\rangle\!\rangle$. Also $\underline{a}_{i..\infty}$ and $\underline{b}_{j..\infty}$ are stutter trace equivalent; and
(3) For i such that $\langle\!\langle b_k\rangle\!\rangle = \langle\!\langle b_0\rangle\!\rangle$ for $0 \le k < i$ and $\langle\!\langle b_i\rangle\!\rangle \neq \langle\!\langle b_0\rangle\!\rangle$, there exists a j such that $\langle\!\langle a_k\rangle\!\rangle = \langle\!\langle a_0\rangle\!\rangle$ for $0 \le k < j$ and $\langle\!\langle a_j\rangle\!\rangle \neq \langle\!\langle a_0\rangle\!\rangle$. Also $\underline{a}_{j..\infty}$ and $\underline{b}_{i..\infty}$ are stutter trace equivalent.

Proposition 8. *Two stutter equivalent ω trajectories satisfy the same set of* $\mathrm{LTL}_{-\bigcirc}$ *formulas.*

Proof. The proof is a simple induction on the structure of the formula.

From Proposition 8 it follows immediately that any two stutter closed bisimilar states satisfy the same set of $\mathrm{LTL}_{-\bigcirc}$ formulas. Hence the stutter closure of bisimilarity is an abstract semantics for $\mathrm{LTL}_{-\bigcirc}$.

7 CTL* without the Next-Time Operator

In this section, we study the relationship between stutter closure of bisimilarity and CTL* without the next time operator. Let denote the logic by $\mathrm{CTL}^{*}_{-\bigcirc}$.

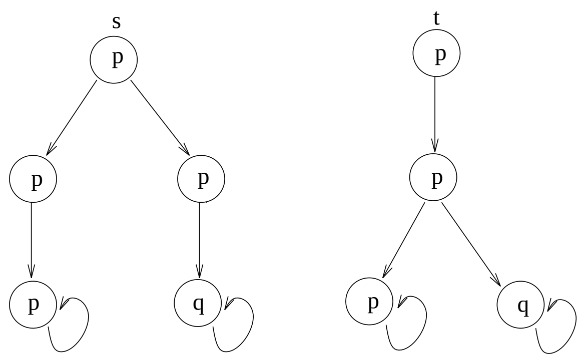

Fig. 3. An observation structure.

It is defined by the following two-sorted grammar with state formulas ϕ and trajectory formulas ψ

$$\phi ::= p \mid \neg\phi \mid \phi \vee \phi \mid \exists\psi$$
$$\psi ::= \phi \mid \neg\psi \mid \psi \vee \psi \mid \psi\mathcal{U}\psi$$

where p ranges over atomic formulas on observations.

Proposition 9. *The stutter closure of bisimilarity is a full abstract semantics for* $\mathrm{CTL}^{*A}_{-\bigcirc}$ *which restricts the first part of* $\mathcal{U}$ *to be an atomic formula.*

Proposition 10. *The state equivalence until-bisimilarity is a full abstract semantics for* $\mathrm{CTL}^{*}_{-\bigcirc}$.

8 SAL and ω-Automata

In this section, we study the distinguishing powers of stutter closure of bisimilarity and that induced by SAL which is trace equivalence.

Proposition 11. *The state equivalence trace equivalence induced by* SAL *and stutter closure of bisimilarity are incomparable.*

Proof. Consider the observation structure of Figure 3 and its stutter closure in Figure 4. The states s and t are trace equivalent, however not stutter-closed bisimilar.

Now consider the observation structure of Figure 1 and its stutter closure in Figure 2. The states s and t are stutter-closed bisimilar, however not trace equivalent.

However, if we restrict SAL to trace automata which are stutter closed, i.e., we only consider automata A with $A^S = A$, where A^S is the stutter closure of A. Actually it is sufficient to consider reflexive trace automata, that is trace

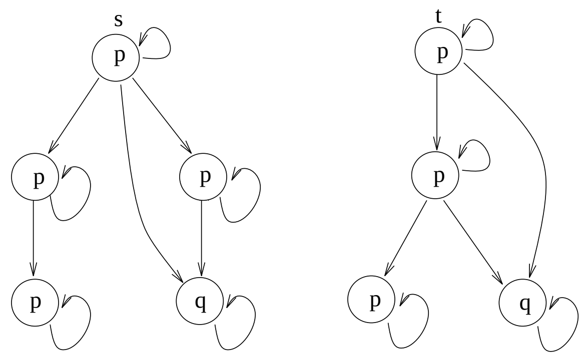

Fig. 4. The stutter closure of the observation structure in Figure 3.

automata with self loops on every state. With this restriction, we can easily show that stutter closure of bisimilarity is an abstract semantics for this restricted version of SAL. Let denote this restricted version of SAL by SAL^R.

Proposition 12. *Stutter closure of bisimilarity is an abstract semantics for* SAL *restricted to reflexive trace automaton.*

From the examples in Figure 1, we observe that the stutter closure of bisimilarity is more distinguishing than the state equivalence induced by SAL^R.

Proposition 13. *Stutter closure of bisimilarity is more distinguishing than the state equivalence induced* SAL^R.

The results also hold for ω-automata. We have the following.

Proposition 14. *Stutter closure of bisimilarity is an abstract semantics for ω-automata restricted to reflexive ω-trace automata.*

Proposition 15. *Stutter closure of bisimilarity is more distinguishing than the state equivalence induced reflexive ω-trace automata.*

9 Conclusions

In this paper, we have studied the relation between stutter closure and various temporal logics. We have given a full logical characterization of the distinguishing power of the stutter closure of bisimilarity and suggested a new state equivalence, i.e., the notion of until-bisimilarity. In particular, we have shown that (1) the stutter closure of bisimilarity is a full abstract semantics for a restricted subset of $\mathrm{STL}^{\mathcal{U}}$ called $\mathrm{STL}^{A\mathcal{U}}$; (2) until-bisimilarity is a full abstract semantics for $\mathrm{STL}^{\mathcal{U}}$. Finally we have extended the results to more standard logics such as CTL and LTL without the next operator.

There are some possible extensions to this work.

– First it would be interesting to consider state preorders instead of state equivalences and to see how stutter closure and the state equivalences induced by these state preorders relate. Similarly, we can define the notion of stutter closure of similarity. The results in the paper should carry naturally to this new notion.
– Second, it would be interesting to study algorithms for and the complexity of computing the until-bisimilarity. Many of the properties we are interested can be specified and probably are naturally specified in either $\mathrm{STL}^{\mathcal{U}}$ or $\mathrm{CTL}_{-\bigcirc}$. Since until-bisimilarity is less distinguishing than bisimilarity, the quotient state space is potentially smaller than that of bisimilarity.
– Third, in the paper, we did not consider fairness. It would be interesting to incorporate fairness constraints into the definitions of state equivalences and study properties of these notions. Notice however, if we only consider region constraints, such as Büchi or Streett constraints, the definitions of the stutter closure of bisimilarity and until-bisimilarity do have these kind of fairness incorporated.

Acknowledgments

We thank Tom Henzinger for the introduction to the problem and guidance in the project.

References

1. R. Alur and T. Henzinger. *Computer Aided Verification.* Draft, 1998.