Open access • Book Chapter • DOI:10.1007/3-540-58201-0_82

Equivalences for Fair Kripke Structures — Source link

Adnan Aziz, Vigyan Singhal, Felice Balarin, Robert K. Brayton ...+1 more authors

Institutions: University of California

Published on: 11 Jul 1994 - International Colloquium on Automata, Languages and Programming

Topics: Kripke structure, Kripke semantics, CTL*, Bisimulation and Equivalence (formal languages)

Equivalences for fair Kripke structures

Adnan Aziz Vigyan Singhal Felice Balarin
Robert K. Brayton Alberto L. Sangiovanni-Vincentelli *
Email: {adnan,vigyan,felice,brayton,alberto}@cs.berkeley.edu
University of California, Berkeley, CA 94720, USA

Abstract. We extend the notion of bisimulation to Kripke structures with fairness. We define equivalences that preserve fairness and are akin to bisimulation. Specifically we define an equivalence and show that it is complete in the sense that it is the coarsest equivalence that preserves the logic CTL* interpreted with respect to the fair paths. We show that the addition of fairness might cause two Kripke structures, which can be distinguished by a CTL* formula, to become indistinguishable by any CTL formula. We also define another weaker equivalence that is the weakest equivalence preserving CTL interpreted on the fair paths. As a consequence of our proof, we also obtain characterizations of states in the fair structure in terms of CTL* and CTL formulae.

1 Introduction

Branching time propositional temporal logic has been found very useful in the automatic verification of concurrent finite-state systems [3]. The systems are modelled using labelled state transition structures called Kripke or temporal structures [5]. The properties that one wishes to verify can be expressed in terms of a branching-time temporal logic. One of the simplest such logics is CTL (Computational Tree Logic) described in [4]. While the problem of model-checking CTL formulas of a Kripke structure is of polynomial complexity, CTL suffers in expressiveness. The richer logic CTL*, described in [6], adds the power of linear-time propositional logic to CTL, and subsumes both CTL and PLTL (Propositional Linear Time Logic). However, the problem of model checking becomes PSPACE-complete [4].

The major limitation of CTL is that it cannot express correctness under fairness constraints. Fairness constraints allow us to reason about only those infinite paths in the Kripke structure which satisfy some fairness specification, which is evaluated over the infinite path. The logic FairCTL allows the specification of a CTL formula p along with a path formula ϕ. The fairness constraint ϕ is a Boolean combination of the set of infinitary linear time operators applied to propositional arguments [5]. The path quantifiers in the syntax of the formula now range over only those infinite paths which meet the fairness constraint ϕ. In [4], a more general specification $\mathrm{CTL}^{\mathrm{F}}$ is allowed, where the fairness is defined in terms of state labels. This allows us to distinguish between two different

* Supported by SRC Grant 93-DC-008 and NSF/DARPA Grant MIP-8719546

states which cannot be distinguished by any propositional temporal logic formulae. The notion of fairness used in our paper is the extension of [5], where we allow the infinitary linear time operators in ϕ to refer to state labels also. The model-checking problem for FairCTL (and $\mathrm{CTL}^{\mathrm{F}}$) can be solved in polynomial time.

Often, it is more natural to think of the fairness constraints as part of the system specification, instead of part of the property being verified. We will refer to Kripke structures with fairness constraints as fair Kripke structures, and the problem of checking a CTL (or CTL*) formula on a fair Kripke structure as the FairCTL (or FairCTL*) model checking. Since we allow the fairness constraints to be a Boolean combination of infinitary linear time operators applied to *state labels*, the fair Kripke structure specification is as powerful as any kind of ω-automata [8].

Browne, Clarke and Grümberg [2] characterized finite Kripke structures in temporal logic. They showed that any two Kripke structures that can be distinguished by a CTL* formula can also be distinguished by a CTL formula. They provide a CTL formula which characterizes Kripke structures up to bisimulation equivalence. Bisimulation equivalence is exactly the equivalence that preserves all CTL and CTL* formulas. In this paper, we solve an open problem proposed in [2] of characterizing equivalence classes for Kripke structures with fairness constraints.

We show that, unlike ordinary Kripke structures, there exists a pair of fair Kripke structures which can be distinguished by a CTL* formula, whereas no CTL formula can distinguish these two. In fact, these two structures are not even trace equivalent, which is surprising because in the case of ordinary Kripke structures bisimulation equivalence is the finest equivalence and trace equivalence is the coarsest equivalence in the linear time – branching time spectrum [7].

Since, for fair Kripke structures, the notion of equivalence is different for CTL and CTL* formulas, we provide two different extensions of bisimulation equivalence which deal with fairness constraints. $\mathcal{E}^{fair}$–bisimulation characterizes states in fair Kripke structures with respect to equivalence over CTL formulas, and $\mathcal{E}^{fair*}$–bisimulation characterizes states in fair Kripke structures with respect to equivalence over CTL* formulas.

The problem of FairCTL* model checking can be solved using the algorithm for CTL* model checking by introducing additional atomic propositions which evaluate state labels, and then transforming the formula using these additional propositions [4]. However, the characterization of states in Kripke structures for CTL* equivalence [2] does not solve the problem of characterizing states in *fair* Kripke structures. This is especially important when one considers fairness constraints as part of the *system* specification.

The remainder of this paper is organized as follows: In section 2 we give the definitions of fair-Kripke structures and CTL/CTL* syntax and semantics on such structures. In section 3, the relationship between bisimulation and CTL/CTL* model checking is reviewed. In section 4 we present the definitions

of $\mathcal{E}^{fair*}$–bisimulation and $\mathcal{E}^{fair}$–bisimulation, and prove completeness results for both equivalences. We conclude in section 5 with plans for future research and applications of our results.

2 Definitions

2.1 Fair Kripke Structures

A Kripke structure K is a triple $< S, T, \mathcal{L} >$, where

- S is a finite set of *states.*
- $T \subset S \times S$ is the *transition relation.*
- $\mathcal{L} : S \rightarrow 2^{AP}$ is the *labelling function* and AP is the underlying set of *atomic propositions.*

The infinite sequence of states $\sigma = [s_1 s_2 s_3 \ldots]$ is said to be a *path* starting at state s_1 if $\forall i(T(s_i, s_{i+1}))$. σ^k denotes the path $[s_k s_{k+1} s_{k+2} \ldots]$, i.e. the k-th suffix of σ. $[\sigma]_k$ denotes s_k i.e. the k-th state occurring on σ.

Fairness conditions express restrictions on the infinitary behavior of the system. Various formalisms exist for defining fair paths, e.g Büchi, Streett, Rabin, and Muller conditions [8]. An important observation is that in all cases fairness of the path is a function of the set of infinitary states. Muller conditions, defined below, can express arbitrary constraints on the set of infinitary states. Thus Muller fairness constraints are complete, and so without loss of generality, we will restrict our analysis to Kripke structures with Muller fairness conditions, which will be referred to as **fair-Kripke structures**, denoted by the 4-tuple $(S, T, \mathcal{L}, f)$.

Definition 1. A **Muller Fairness condition** (MFC) f on Kripke structure K is characterized by a class $\mathcal{C} = M_1, M_2, \ldots, M_n$ of subsets of S; the path σ is fair, if and only if the set of states occurring infinitely often in σ, (denoted by $inf(\sigma)$) is an element of $\mathcal{C}$. The sets M_i will be referred to as the **Muller fair** subsets.

Notation: $\mathcal{F}^f_{s_0}$ denotes the set of all paths starting at s_0 that satisfy the MFC f.
Remark: Muller conditions are known to be exponentially less succinct in expressing fairness than other common fairness constraints. We do not analyze complexity issues in this paper; hence this is of no concern. Also, to simplify analysis we will always assume that every state lies on a fair path. This is not a serious restriction; also note that under Muller fairness conditions, there are efficient procedures for deciding if there is a fair path from a state.

2.2 CTL/CTL* Model Checking on fair Kripke structures

There are two type of formulae in CTL and CTL*: state formulae (which are true or false in a specific state), and path formulae (which are true or false along a specific path). Let AP be the set of atomic proposition names. A state formula is given by the following syntax:

1. $\underline{a}$ if a $\in$ AP
2. If f_1 and f_2 are state formula, then so are $\neg f_1, f_1 \vee f_2$
3. If g is a path formula, then $\exists g$, $\forall g$ are state formulae.

A path formula is given by the following syntax:

1. A state formula
2. If g_1 and g_2 are path formula, then so are $\neg g_1, f_1 \vee g_2$.
3. If g_1 and g_2 are path formula, then so are $Xg_1, g_1 U g_2$.

CTL* is the set of state formulae that are generated by the above rules; CTL is a subset of CTL* in which the path formulae are restricted to be:

1. If f_1, and f_2 are state formula, then Xf_1 and $f_1 U f_2$ are path formula

Given a fair-Kripke structure $K = (S, R, \mathcal{L}, f)$ state and path formulae are interpreted over fair paths as defined below. The formulae f_1 and f_2 are state formulae, and g_1 and g_2 are path formulae.

1. $s_0 \models \underline{a}$ if and only if $a \in \mathcal{L}(s_0)$
2. $s_0 \models \neg f_1$ if and only if $s_0 \not\models f_1$, $s_0 \models f_1 \vee f_2$ if and only if $s_0 \models f_1$ or $s_0 \models f_2$
3. $s_0 \models \exists g_1$ if and only if there exists a **fair** path π starting at s_0 such that $\pi \models g_1$; similarly $s_0 \models \forall g_1$ if and only if for all **fair** paths π starting at s_0, $\pi \models g_1$
4. $\pi \models f_1$ if and only if s_0 is the first state of π and $s_0 \models f_1$
5. $\pi \models \neg g_1$ if and only if $\pi \not\models g_1$, $\pi \models g_1 \vee g_2$ if and only if $\pi \models g_1$ or $\pi \models g_2$
6. $\pi \models Xg_1$ if and only if $\pi^1 \models g_1$, $\pi \models g_1 U g_2$ if and only if there exists a $k \geq 0$ such that $\pi^k \models g_2$ and for all $0 \leq j < k$, $\pi^j \models g_1$

Notation: Given a path formula g_1, we will use the abbreviation Gg_1 to denote the CTL* path formula $\neg(\texttt{TRUE}\, U\, \neg g_1)$, where TRUE is a logical tautology.

3 Equivalences preserving CTL/CTL*

Given a Kripke structure $K = (S, T, \mathcal{L})$, the usual definition of bisimulation is the coarsest relation on $S \times S$ satisfying

$$\begin{aligned}\mathcal{E}^{bis}(s,t) \leftrightarrow\ & (\mathcal{L}(s) \equiv \mathcal{L}(t)) \wedge \\ & \forall s'(T(s,s') \rightarrow \exists t'(T(t,t') \wedge \mathcal{E}^{bis}(s',t'))) \wedge \\ & \forall t'(T(t,t') \rightarrow \exists s'(T(s,s') \wedge \mathcal{E}^{bis}(s',t'))) \end{aligned} \quad (1)$$

It is clear that $\mathcal{E}$ is an equivalence relation; soundness of this definition follows from the observation that

1. there exists a relation satisfying the above (namely the identity), and
2. given any two distinct relations $\mathcal{E}_1, \mathcal{E}_2$ satisfying the above, there exists a relation containing both $\mathcal{E}_1$ and $\mathcal{E}_2$.

In the absence of fairness conditions on the paths through the Kripke structure, Browne, Clarke, and Grümberg prove the following completeness result [2]:

Theorem 2. *Let s,t be states in K. Then $\mathcal{E}^{bis}(s,t)$ if and only if there is no CTL formula ϕ such that $s \models \phi \wedge t \not\models \phi$.*

As a corollary, they note that states in a Kripke structure that can be differentiated by a formula of CTL* can also be differentiated by a formula of CTL. Furthermore, they construct CTL formulae that characterize states and structures up to bisimulation equivalence.

4 Equivalences on fair Kripke structures

In the presence of fairness conditions, states that have the same branching structure may have different infinitary behavior. In the fair-Kripke structure defined in figure 1, the Muller fairness condition is $\{U_1, V_1\}$ (shown in the dotted boxes), and the set of AP's is $\{a, b\}$. States s_0 and t_0 have identical finite branching structure, but state t_0 models the CTL formula $\exists Ga$ (there exists a path such that always a), while $s_0 \not\models \exists Ga$.

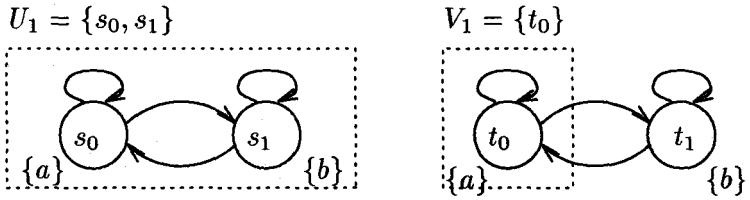

Fig. 1. States that agree on all CTL formulae in the absence of fairness

In this section we define two equivalences on the states of fair-Kripke structures. We prove completeness results with respect to CTL* and CTL, using arguments analogous to those in [2]. Essentially, our equivalences incorporate fairness constraints by requiring that states be equivalent on all fair paths. We show that it suffices to examine a restricted class of paths, namely the *rational* paths defined below.

Definition 3. Let σ be a path through a Kripke structure K. Define σ to be a **rational path** if $\exists N, M$ such that $\forall i\ (i > N \Rightarrow [\sigma]_i = [\sigma]_{(i \bmod M+N)})$.

Thus rational paths are those which end in a cycle.
Notation: Given an equivalence relation $\mathcal{E}$ on the state space of a Kripke structure, extend it to an equivalence $\mathcal{E}^\omega$ on paths through the Kripke structure as follows:

$$\mathcal{E}^\omega(\sigma,\tau) \Leftrightarrow \forall i\,(\mathcal{E}([\sigma]_i,[\tau]_i))$$

In the sequel, we will simply use $\mathcal{E}$ to denote $\mathcal{E}^\omega$.

4.1 Equivalences preserving CTL* on fair Kripke structures

Definition 4. Given a fair-Kripke structure $K = (S, T, \mathcal{L}, f)$, states s and t are said to be $\mathcal{E}^{fair*}$**-bisimilar** if they lie in the coarsest equivalence $\mathcal{E}$ that satisfies

$$\begin{aligned}\mathcal{E}(s,t) \Leftrightarrow (\mathcal{L}(s) \equiv \mathcal{L}(t)) \wedge \\ &\text{(for all fair rational paths } \sigma \text{ starting at } s \\ &\quad \text{there exists a fair rational path } \tau \text{ starting at } t \text{ such that } \mathcal{E}(\sigma,\tau)) \wedge \\ &\text{(for all fair rational paths } \tau \text{ starting at } t \\ &\quad \text{there exists fair rational path } \sigma \text{ starting at } s \text{ such that } \mathcal{E}(\sigma,\tau)) \quad (2)\end{aligned}$$

The soundness of this definition follows in a manner analogous to that for equation 1.
This definition is complete in the sense that we have the following theorem:

Theorem 5. *Let s, t be states in K. Then $\mathcal{E}^{fair*}(s,t)$ if and only if there is no fair CTL* formula ϕ such that $s \models \phi \wedge t \not\models \phi$.*

Proof. The forward direction of the theorem, namely $\mathcal{E}^{fair*}(s,t) \Rightarrow$ for every CTL* formula ϕ, $s \models \phi \leftrightarrow t \models \phi$ follows by a straightforward induction on the length of CTL* formula.

To show the converse, namely $\neg\mathcal{E}^{fair*}(s,t) \Rightarrow$ there exists a formula ϕ of CTL* such that $s \models \phi \wedge t \not\models \phi$ we first define $E_0, E_1, \ldots$:

- $E_0(s,t)$ if and only if $\mathcal{L}(s) \equiv \mathcal{L}(t)$.
- $E_{k+1}(s,t)$ if and only if
  - For every fair rational path σ starting at s there is a fair rational path τ starting at t such that $E_k(\sigma,\tau)$.
  - For every fair rational path τ starting at t there is a fair rational path σ starting at s such that $E_k(\sigma,\tau)$.

Observe that since $E_{l+1}(s,t) \Rightarrow E_l(s,t)$, it follows that $E_0 \supseteq E_1 \supseteq E_2 \ldots$. Also every equivalence in the sequence contains the equality relation. (The binary relation where an element is related only to itself). Since the state space is finite the sequence converges to a fixed point in some finite number of step, i.e. there is some k such that $E_{k+1} = E_k$, which we will refer to as E_∞.

We now characterize states up to E_l equivalence by CTL* equivalence. This is done by induction on l. Specifically we demonstrate

- If $\neg(E_l(s,t))$ then there is a CTL* formula $d_l(s,t)$ such that $\forall v\,[E_l(s,v) \Rightarrow v \models d_l(s,t)]$, and $t \not\models d_l(s,t)$.
- For every state $s \in S$, there is a formula of CTL* $C_l(s)$ such that for every $t \in S\,[t \models C_l(s) \Leftrightarrow E_l(s,t)]$.

$d_l(s,t)$ is a formula that distinguishes between t and states E_l-equivalent to s and $C_l(s)$ is a formula that characterizes E_l-equivalence to state s within the fair-Kripke structure.

If we let $C_l(s)$ be a conjunction of $C_{l-1}(s)$ and $d_l(s,t)$ for every t which is not E_l-related to s, the second assertion follows immediately. Now it is necessary to show how to construct $d_l(s,t)$ by induction on l.

Base Case:($l = 0$)

Let $\{p_i\}$ be the set of atomic propositions in $\mathcal{L}(s)$ and $\{q_j\}$ be the set of atomic propositions in AP $- \mathcal{L}(s)$. Now let $C_0(s) = \bigwedge_i \underline{p_i} \wedge \bigwedge_j \neg \underline{q_j}$. It is clear that this formula is only true in states with exactly the same labelling as s. Thus the base case is established.

Induction:

Assume the result is true for l. We will show it for $l+1$.

Let s,t be any states in the structure such that $\neg(E_{l+1}(s,t))$. This can only happen if there is a fair rational path from s for which there is no E_l-corresponding fair rational path out of t, or there is a fair rational path from t for which there is no E_l-corresponding fair rational path out of s. In the latter case, we will use the argument below to find a $d_{l+1}(t,s)$ such that $t \models d_{l+1}(t,s)$ and $s \not\models d_{l+1}(t,s)$. We can negate this formula to obtain the desired $d_{l+1}(t,s)$. Let a fair rational path from s with no corresponding path from τ be $\sigma = s_1 s_2 \ldots s_N (s_{N+1} \ldots s_{N+k})^\omega$, where $s = s_1$ for notational convenience. First define the CTL* formulae $\mathtt{cycle}^i_{l+1}(s,t)$, for $i \in \{1,\ldots,k\}$

$$\mathtt{cycle}^i_{l+1}(s,t) = (C_l(s_{N+1+(i-1) \bmod k}) \wedge X(C_l(s_{N+1+(i) \bmod k}) \wedge X(C_l(s_{N+1+(i+1) \bmod k}) \cdots \; XC_l(s_{N+1+(i+k-2) \bmod k})) \cdots)$$

Let $\mathtt{cycle}_{l+1}(s,t)$ be the path formula given below:

$$\mathtt{cycle}_{l+1}(s,t) = \mathtt{cycle}^1_{l+1}(s,t) \vee \mathtt{cycle}^2_{l+1}(s,t) \ \ldots \ \mathtt{cycle}^k_{l+1}(s,t)$$

A path will model $\mathtt{cycle}_{l+1}(s,t)$ if and only if the k-th prefix of the path is E_l-equivalent to a cyclic permutation of the k-th prefix of σ.

Now define $\mathtt{path}_{l+1}(s,t)$ as below:

$$\begin{aligned}\mathtt{path}_{l+1}(s,t) = (C_l(s_1) \wedge X(C_l(s_2) \wedge X(C_l(s_3) \wedge \cdots X(C_l(s_N) \wedge \\ [XC_l(s_{N+1}) \wedge X(C_l(s_{N+2}) \ldots X(C_l(s_{N+k}))] \wedge \\ [X\,G\,(\mathtt{cycle}_{l+1}(s,t))]) \cdots)\end{aligned}$$

Let $d_{l+1}(s,t) = \exists \mathtt{path}_{l+1}(s,t)$. Note that $\sigma^{N+1} \models \mathtt{cycle}_{l+1}(s,t)$. Furthermore, $\sigma \models (C_l(s_1) \wedge X(C_l(s_2) \wedge X(C_l(s_3) \wedge \cdots X(C_l(s_{N+k})) \cdots)$; hence $s \models d_{l+1}(s,t)$.

Given that $\pi \models \mathtt{path}_{l+1}(s,t)$, we can prove that π is E_l-equivalent to σ. First observe that for each $i \in \{1,\ldots,N+k\}$, $\pi^i \models C_l(s_i)$. Further, it is true that for $i \geq 1$, $\pi^{N+i} \models \mathtt{cycle}_{l+1}(s,t)$. Using these facts, one can show by induction that for $i \geq 1$, $\pi^{N+i} \models \mathtt{cycle}^{((i-1) \bmod k)+1}_{l+1}(s,t)$. This implies that for each $i \geq 1$, $\pi^{N+i} \models C_l(s_{N+1+(i-1) \bmod k})$.

We now reason that $E_\infty(s,t) \Rightarrow \mathcal{E}^{fair*}(s,t)$, and so states that are E_∞ equivalent cannot be differentiated by any formula of CTL*, implying that states that are not $\mathcal{E}^{fair*}(s,t)$ equivalent can be differentiated.

Since E_∞ is a fixed point, and is reached at some finite stage, there exists some k such that $E_k = E_{k+1} = E_\infty$. Hence E_∞ satisfies the following:

- $E_{k+1}(s,t)(= E_\infty(s,t))$ if and only if for every fair path from s there is an $E_k(= E_\infty)$-equivalent path from t, and vice versa.

Thus E_∞ lies in $\mathcal{E}^{fair*}$, and so $E_\infty = \mathcal{E}^{fair*}$. ∎

Remark: In definition 4 states were taken to be equivalent over rational fair paths. The following lemma demonstrates that equivalence over rational fair paths implies equivalence over all fair paths, establishing a more intuitive characterization of $\mathcal{E}^{fair*}$-bisimulation. The lemma also establishes that $\mathcal{E}^{fair*}$ can be polytime reduced to deciding trace equivalence for ω-automata with acceptance conditions corresponding to the fairness conditions.

Lemma 6. Let K be a given fair-Kripke structure. Let $\mathcal{E}$ be an equivalence relation on the states satisfying equation 2 i.e. satisfying the following:

$$\begin{aligned}\mathcal{E}(s,t) \Leftrightarrow\ & (\mathcal{L}(s) \equiv \mathcal{L}(t)) \wedge \\ & \text{(for all fair rational paths } \sigma \text{ starting at } s \\ & \quad \text{there exists a fair rational path } \tau \text{ starting at } t \text{ such that } \mathcal{E}(\sigma,\tau)) \wedge \\ & \text{(for all fair rational paths } \tau \text{ starting at } t \\ & \quad \text{there exists fair rational path } \sigma \text{ starting at } s \text{ such that } \mathcal{E}(\sigma,\tau)) \quad (3)\end{aligned}$$

Then $\mathcal{E}$ preserves equivalence across all fair paths, i.e. for all fair paths σ starting at s there exists a fair path τ starting at t such that $\mathcal{E}(\sigma,\tau)$), and for all fair paths τ starting at t there exists a fair path σ starting at s such that $\mathcal{E}(\sigma,\tau)$).

Proof. Let $\{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_n\}$ be the equivalence classes of $\mathcal{E}$. Define an alphabet $\Sigma = \{c_1, c_2, \ldots, c_n\}$ corresponding to the equivalence classes. Define the ω-language L_s over Σ as $L_s = \{x \in \Sigma^\omega \mid \exists \sigma \in \mathcal{F}_s^f$ such that $\forall i\, [\sigma]_i \in \mathcal{C}([x]_i)\}$, where $\mathcal{C} : \{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_n\} \rightarrow \Sigma$ maps equivalence classes to their corresponding alphabets. It is clear that L_s is ω-regular. (The fair-Kripke structure can be viewed as a Muller automaton, and the output at a state is the symbol of Σ corresponding to its equivalence class.) Similarly, define the ω-regular language $L_t = \{y \in \Sigma^\omega \mid \exists \tau \in \mathcal{F}_t^f$ such that $\forall i\, [\tau]_i \in \mathcal{C}([y]_i)\}$.

It is clear that given any fair path σ starting at s, there is a fair path τ starting at t which is $\mathcal{E}$-equivalent to σ, and vice versa, if and only if $L_s = L_t$.

Claim: If W_1 and W_2 are two ω-regular languages over the same alphabet, and they agree on all rational words (i.e. words that are ultimately periodic), then they are in fact equal.

The claim follows from the following observation. Let W be the symmetric difference of W_1 and W_2, i.e. $W = (W_1 \cap W_2') \cup (W_1' \cap W_2)$. Then W is ω-regular, and so is non-empty if and only is it contains a rational word. Since W_1 and W_2 contain exactly the same set of rational words, W is empty, and so $W_1 = W_2$.

Since L_1 and L_2 agree on all rational words (because s and t agree on all rational paths), it follows that $L_1 = L_2$, and so s and t must agree on all paths, proving the lemma. ∎

4.2 Equivalences preserving CTL on fair Kripke structures

The logic CTL is a subset of the logic CTL* where nesting of path operators is not allowed, i.e. every path operator must be immediately followed by a path quantifier. Since it is a subset of CTL*, it follows from theorem 5 that states that are $\mathcal{E}^{fair*}$ equivalent must agree on all CTL formulae. However the converse is not true. Consider the the states s_1 and t_1 in figure 2.

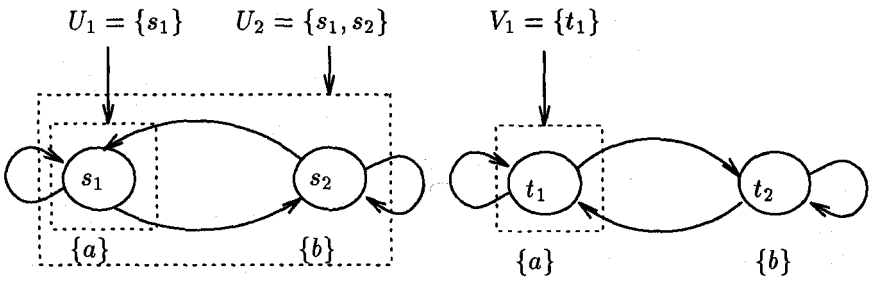

Fig. 2. States that agree on all CTL formulae but can be differentiated by CTL*

1. The set of atomic propositions is $\{a, b\}$, the set of AP's true at s_1 and t_1 is $\{a\}$, the set of AP's true at s_2 and t_2 is $\{b\}$.
2. The fairness conditions are of Muller type. The sets $U_1 = \{s_1\}$,$U_2 = \{s_1, s_2\}$, $V_1 = \{t_1\}$ are the fair Muller sets, i.e. fair paths are those in which the infinitary set of states is exactly one of U_1, U_2, V_1.

State s_1 can not be differentiated from t_1 by any CTL formula, since the only difference is the fact that there are paths from s_1 on which b happens infinitely often, and CTL can not express $\exists GF\phi$ i.e. there exists a path such that infinitely often ϕ is true. More formally the equivalence of s_1 and t_1 with respect to all CTL formula can be proved by using induction on the length of the formula.
Remark: It is surprising that the set of output traces from s_1 is not equal to the set of output traces from t_1. (Consider for example the trace $(ab)^\omega$). This in contrast to the fact that in the absence of fairness constraints states that are bisimilar equivalent must have the same set of traces.

We can still characterize states that agree on all CTL formula as shown in the following theorem.

Theorem 7. Given a fair-Kripke structure $K = (S, T, \mathcal{L}, f)$, define states s, t to be $\mathcal{E}^{fair}$-bisimilar if they lie in the coarsest equivalence $\mathcal{E}$ satisfying:
$\mathcal{E}(s, t)$ if and only if

1. $\mathcal{L}(s) \equiv \mathcal{L}(t)$
2. For every fair rational path $\sigma = (s_1 s_2 \ldots s_N) \cdot (s_{N+1} s_{N+2} \ldots s_{N+k})^\omega$ there exists a fair rational path τ such that $\forall i (1 \leq i \leq N \rightarrow \mathcal{E}(s_i, [\tau]_i))$ and $\forall i > N$ $[\tau]_i$ is $\mathcal{E}$-equivalent to some state in $inf(\sigma)$.

3. For every fair rational path τ from t_1, there should be a fair rational path σ from s_1 which corresponds to τ in the above sense.

Then $\mathcal{E}^{fair}$ is the coarsest equivalence preserving all of fair-CTL.

Proof. The proof is similar to that for CTL*. First define $E_0, E_1, \ldots$

- $E_0(s_1, t_1)$ if and only if $\mathcal{L}(s_1) \equiv \mathcal{L}(t_1)$.
- $E_{l+1}(s_1, t_1)$ if and only if
  1. for every fair rational path $\sigma = (s_1 s_2 \ldots s_N) \cdot (s_N s_{N+1} \ldots s_{N+k})^\omega$ there exists a fair rational path τ such that $\forall i (1 \leq i \leq N \rightarrow E_l(s_i, [\tau]_i))$, and $\forall i > N$, $[\tau]_i$ is E_l-equivalent to some state in $inf(\sigma)$.
  2. for every fair rational path τ from t_1, there is a fair simple path σ from s_1 which corresponds to τ in the above sense

Note that E_∞ satisfies the definition of bisimulation as given in 1: By definition, $E_\infty(s,t) \Rightarrow \mathcal{L}(s) \equiv \mathcal{L}(t)$. Also, $T(s,s') \Rightarrow \exists t'(T(t,t') \wedge E_\infty(s',t'))$, since s' can be continued to an infinite path for which there must correspond an infinite path from T, the second state of which must be E_∞-equivalent to s. A symmetric argument for t shows that s and t are bisimilar.

We now characterize states up to E_l equivalence by CTL formulae. This is done by induction on l. Specifically we will demonstrate:

- If $\neg(E_l(s,t))$ then there is a CTL formula $d_l(s,t)$ such that $\forall v\, [E_l(s,v) \Rightarrow v \models d_l(s,v)]$, and $t \not\models d_l(s,t)$.
- For every state $s \in S$, there is a formula of CTL $C_l(s)$ such that for every $t \in S[t \models C_l(s) \Leftrightarrow E_l(s,t)]$

$d_l(s,t)$ is a formula that distinguishes between t and states E_l equivalent to s and $C_l(s)$ is a formula that characterizes E_l-equivalence to state s within the fair-Kripke structure.

If we let $C_l(s)$ be a conjunction of $C_{l-1}(s)$ and $d_l(s,t)$ for every t which is not E_l-related to s, the second assertion follows immediately. Now it is necessary to show how to construct $d_l(s,t)$ by induction on l.

Base Case:(l=0)
Let $\{p_i\}$ be the set of atomic propositions in $\mathcal{L}(s)$ and $\{q_j\}$ be the set of atomic propositions in AP $- \mathcal{L}(s)$. Now let $C_0(s) = \bigwedge_i \underline{p_i} \wedge \bigwedge_j \neg \underline{q_j}$. It is clear that this formula is only true in states with exactly the same labelling as s. Thus the base case is established.

Induction:
Assume the result is true for l. We will show it for $l+1$.

Let s, t be any states in the structure such that $\neg(E_{l+1}(s,t))$. This can only happen if there is a fair rational path from s with no E_l-corresponding fair rational path from t, or there is a fair rational path from t for which there is no E_l-corresponding fair rational path out of s. In the latter case, we will use the argument below to find a $d_{l+1}(t,s)$ such that $t \models d_{l+1}(t,s)$ and $s \not\models d_{l+1}(t,s)$. We can negate this formula to obtain the desired $d_{l+1}(t,s)$.

Let $\sigma = s_1 s_2 \ldots s_N (s_{N+1} \ldots s_{N+k})^\omega$ be a fair rational path from s with no E_l-corresponding fair rational path from t, where $s_1 = s$ for notational convenience.

Define $d_{l+1}(s,t)$ as below:

$$d_{l+1}(s,t) = C_l(s_1) \wedge \exists X(C_l(s_2) \wedge \exists X(C_l(s_3) \wedge \exists(X \ldots \exists X(C_l(s_{N+1}) \wedge \exists G(C_l(s_{N+1}) \vee C_l(s_{N+2}) \vee \ldots \vee C_l(s_{N+k}))\ldots)$$

By construction, $s \models d_{l+1}(s,t)$. Also, since there is no path from t which corresponds to σ, $t \not\models d_{l+1}(s,t)$. Hence the inductive step follows.

Observe that if states s,t are not E_∞ equivalent, then there is some k such that $\neg(E_k(s,t))$. As a result, $s \models C_k(s)$ and $t \not\models C_k(s)$ and so states that are not E_∞-equivalent can be differentiated by CTL.

We now reason that $E_\infty(s,t) \Rightarrow$ for any CTL formula ϕ, $s \models \phi \leftrightarrow t \models \phi$. We use induction on the length of the formula.

Base Case: $\phi = \underline{a}$ where $a \in$ AP. Then since $E_i \rightarrow E_0$, it follows $\mathcal{L}(s) \equiv \mathcal{L}(t)$, and so $s \models \mathbf{a} \Leftrightarrow t \models \mathbf{a}$. Hence the base case is proved.

Inductive Step:

1. $\phi = \neg(\phi_1)$ Straightforward - follows from elementary propositional logic.
2. $\phi = (\phi_1 \vee \phi_2)$ Straightforward - follows from elementary propositional logic.
3. $\phi = \exists X(\phi_1)$ Observe that $E_\infty(s,t) \Rightarrow \forall s'(T(s,s') \Rightarrow \exists t'(T(t,t') \wedge E_\infty(s',t')))$. This follows from the fact that s' can be continued to a fair rational path, and so there must be a corresponding fair rational path from t. t' can be taken to be the state following t in this path. From this observation and the induction hypothesis, it follows that $\exists s'(T(s,s') \wedge s' \models \phi_1) \Leftrightarrow \exists t'(T(t,t') \wedge t' \models \phi_1)$, and hence induction goes through.
4. $\phi = \exists(\phi_1 U \phi_2)$ Suppose $s \models \phi$. Then from the semantics of CTL, it follows that there exists a path $\sigma = s s_1 s_2 \ldots$ such that $\exists N(\forall i(i < N \Rightarrow [\sigma]_i \models \phi_1) \wedge [\sigma]_N \models \phi_2)$. Reasoning as above, there must exist a finite path $t t_1 t_2 \ldots t_N$ such that $\forall i \leq N(E_\infty(s_i,t_i))$. Hence by the induction hypothesis $\forall i < N(t_i \models \phi_1)$ and $(t_N \models \phi_2)$. This finite path can be extended to an infinite path, since every state is assumed to lie on a fair path, and this infinite path satisfies $(\phi_1 U \phi_2)$. Thus $t \models \phi$. The converse, namely to show $t \models \phi \Rightarrow s \models \phi$, follows by symmetry.
5. $\phi = \exists G(\phi_1)$ Suppose $s \models \phi$. Then there is a fair rational path σ such that $\forall i([\sigma]_i \models \phi)$. Since σ is rational, it can be expressed as a sequence $s s_1 s_2 \ldots s_N (s_{N+1} s_{N+2} \ldots s_{N+k})^\omega$. Because s is E_∞-equivalent to t, it follows that there is a rational fair path τ such that
   - $\forall i \leq N : E_\infty([\sigma]_i, [\tau]_i)$, and
   - $\forall i > N : \exists s_j \in inf(\sigma)$ such that $E_\infty(s_j, [\tau]_i)$

   Claim: $\tau \models G(\phi_1)$

   Proof: Every state on the path τ is E_∞-equivalent to a state on σ. Since $\sigma \models G(\phi_1)$, it follows that every state on σ satisfies ϕ_1. Since every state on the path τ is E_∞-equivalent to a state on σ, and the induction hypothesis requires that states that are E_∞-equivalent agree on all CTL formula of

length less than $| \phi |$, it follows that all states on τ satisfy ϕ_1. Thus $t \models \phi$, and the claim is proved.

Hence by induction, states that are E_∞-equivalent satisfy exactly the same set of CTL formula.

This completes the proof of theorem 7. ∎

5 Conclusion and Future Work

We have defined state equivalences on Kripke structures that incorporate fairness. These equivalences were shown to be complete in the sense that they are the weakest equivalences preserving branching time logics interpreted on the structures. Furthermore we characterized the equivalence classes by formulae from the logic.

We have developed approximations to the complete equivalence that can be efficiently computed for Büchi, Rabin, and Streett fairness conditions. These are used in a hierarchical procedure for minimizing systems of interacting state machines[1]. We plan to continue developing generalized notions of equivalence that are property specific, and can be used to reduce or abstract components in large designs.

References

1. A. Aziz, V. Singhal, G. M. Swamy, and R. K. Brayton. Minimizing Interacting Finite State Machines. Technical Report UCB/ERL M93/68, Electronics Research Lab, Univ. of California, Berkeley, CA 94720, September 1993.
2. M. C. Browne, E. M. Clarke, and O. Grümberg. Characterizing Finite Kripke Structures in Propositional Temporal Logic. *Theoretical Computer Science*, 59:115–131, 1988.
3. E. M. Clarke, J. R. Burch, O. Grümberg, D. E. Long, and K. L. McMillan. Automatic Verification of Sequential Circuit Designs. *Phil. Trans. of the Royal Society of London*, 339:105–120, 1992.
4. E. M. Clarke, E. A. Emerson, and A. P. Sistla. Automatic Verification of Finite-State Concurrent Systems Using Temporal Logic Specifications. *ACM Transactions on Programming Languages and Systems*, 8(2):244–263, 1986.
5. E. A. Emerson. Temporal and Modal Logic. In J. van Leeuwen, editor, *Formal Models and Semantics*, volume B of *Handbook of Theoretical Computer Science*, pages 996–1072. Elsevier Science, 1990.
6. E. A. Emerson and J. Y. Halpern. "Sometimes" and "Not Never" Revisited: on Branching versus Linear Time Temporal Logic. *Journal of the ACM*, 33(1):151–178, 1986.
7. Robert J. van Glabbeek. *Comparative Concurrency Sematics and Refinement of Actions*. PhD thesis, Centrum voor Wiskunde en Informatica, Vrije Universiteit te Amsterdam, Amsterdam, May 1990.
8. Shmuel Safra. *Complexity of Automata on Infinite Objects*. PhD thesis, The Weizmann Institute of Science, Rehovot, Israel, March 1989.