Resolution for a Temporal Logic of Robustness (Extended Version)

Clare Dixon[1] and John C. M^{c}Cabe-Dansted[2]

[1] Department of Computer Science, University of Liverpool,
Liverpool, L69 3BZ, UK
clare@csc.liv.ac.uk
[2] School of Computer Science and Software Engineering
The University of Western Australia, Australia
john@csse.uwa.edu.au

Abstract. The logic RoCTL* is an extension of the branching time temporal logic CTL* to represent robustness and reliability in systems. New operators are introduced dealing with obligation (where no failures occur) and robustness (where at most one additional failure occurs). The only known decision procedure for the temporal logic of robustness RoCTL* involves a reduction to the non-elementary QCTL* logic. Here we propose a CTL like restriction of RoCTL*, termed RoCTL, and investigate its application and complexity. We show that the fragment of RoCTL without the robust and prone operators, RoCTL$^-$, can be translated into CTL. We provide a satisfiability preserving translation for RoCTL$^-$ into CTL. By applying a known resolution calculus to the resulting formulae we obtain a resolution calculus for RoCTL$^-$ and show that the complexity of satisfiability of RoCTL$^-$ is EXPTIME.

1 Introduction

The RoCTL* logic [11] is an extension of CTL* introduced to represent issues relating to robustness and reliability in systems. It does this by explicitly representing success and failure relations in the underlying model structures and using these to define an *obligatory* operator and a *robustly* operator (and their duals *permissible* and *prone*). The obligatory operator specifies how the systems *should* behave by quantifying over paths in which no failures occur. The robustly operator specifies that something must be true on the current path and on all paths that deviate from the current path that have at most one more failure than the current path. This notation allows phrases such as "even with n additional failures" to be built up by chaining n simple unary operators together. One of the strengths of RoCTL* is its ability to express contrary-to-duty [9] obligations, which can be difficult for some Deontic logics.

Unfortunately the only known decision procedure for RoCTL* involves a reduction to QCTL* [11] which is non-elementary to decide. We therefore study a CTL like restriction, termed RoCTL. We show the fragment without robust and prone operators (termed RoCTL$^-$) can be translated into CTL. For RoCTL$^-$ we propose a translation into CTL thus allowing us to use a known CTL resolution based decision procedure [2, 18] to carry out RoCTL$^-$ proofs. The translation into CTL is shown to increase the length of the formula linearly and using this we show that the complexity of satisfiability for RoCTL$^-$ is EXPTIME. RoCTL$^-$ is still reasonably expressive. For example it can still be used to express certain contrary-to-duty obligations.

RoCTL can express any statement that can be expressed in CTL, and can additionally use a robustly or obligatory operator (or their duals permission and prone) in place of the *all paths* operator. The robustly operator quantifies over paths that deviate from the current path. As this set of paths depends on the current path, the robustly operator is not a state formula.

This paper provides proof procedures for RoCTL$^-$, a sub-logic of RoCTL*, via a satisfiability preserving translation into CTL. Decision procedures have been developed for the branching time temporal logic CTL based on resolution [2, 18] and tableau [8, 1]. The success and failure relations in the RoCTL model structures are represented by introducing a new proposition *viol* such that if *viol* holds in a state it represents following a failure relation, and if it doesn't hold it represents following a success relation. At the root or initial state *viol* may or may not hold.

This paper is structured as follows. In Section 2 we present the syntax and semantics of RoCTL with some examples formulated in RoCTL provided in Section 3. The syntax and semantics of CTL and a normal form for CTL (known as SNF$_{CTL}$) are provided in Section 4. In Section 5 we give translations from RoCTL$^-$ formulae into CTL. In Section 6 we provide examples of how to carry out the translation of RoCTL$^-$ formulae into the normal form. In Section 7 we provide details of the resolution calculus for CTL. In Section 8 we provide examples of the translation and application of the resolution rules applied to translated RoCTL$^-$ formulae. In Section 9 we show that the translation preserves satisfiability and in Section 10 provide results relating to the complexity of the translation. We provide concluding remarks and mention related work in Section 11.

2 Syntax and Semantics of RoCTL

This follows that in [11] except it is restricted to RoCTL.

RoCTL extends CTL by adding the following path operators:

- $\mathbf{O}\varphi$ (obligatory): a deontic operator, denoting that φ holds on every failure-free path;
- $\mathbf{P}\varphi$ (permissible): a deontic operator, denoting that φ holds on some failure free path;
- $\blacktriangle\varphi$ (robust): denoting that φ holds on the current path and on any path that differs from this path by a single deviating event;
- $\triangle\varphi$ (prone): denoting that φ holds on the current path or on a path that differs from this path by a single deviating event;

to the CTL path operators:

- $\mathbf{A}\varphi$ (all paths): a CTL path operator, denoting that φ holds on every path;
- $\mathbf{E}\varphi$ (some path): a CTL path operator, denoting that φ holds on some path.

Formulae are constructed from a set PROP $= \{p, q, r, \ldots\}$ of *primitive propositions*. The language of RoCTL contains **true** and **false** and the standard propositional connectives $\neg$ (not), $\vee$ (or), $\wedge$ (and) and $\Rightarrow$ (implies). For the temporal dimension we take the usual [12] set of future-time temporal connectives $\bigcirc$ (*next*), $\Diamond$ (*sometime* or *eventually*), $\Box$ (*always*), $\mathcal{U}$ (*until*) and $\mathcal{W}$ (*unless* or *weak until*). Each of these must be paired with a path operator.

The set of well-formed formulae of RoCTL, WFF, is defined as follows:

- **false**, **true** and any element of PROP is in WFF;
- if φ and ψ are in WFF and $\mathbf{H} \in \{\mathbf{A}, \mathbf{E}, \mathbf{O}, \mathbf{P}, \blacktriangle, \triangle\}$ then the following are in WFF:

$$\begin{array}{lllll} \neg\varphi & \varphi \vee \psi & \varphi \wedge \psi & \varphi \Rightarrow \psi & \\ \mathbf{H}\Diamond\varphi & \mathbf{H}\Box\varphi & \mathbf{H}\bigcirc\varphi & \mathbf{H}(\varphi\,\mathcal{U}\,\psi) & \mathbf{H}(\varphi\,\mathcal{W}\,\psi) \end{array}$$

The set of *state formulae* of RoCTL, is defined as follows:

- **false**, **true** and any element of PROP is in the set of state formulae;
- if φ and ψ are state formulae and $\mathbf{H} \in \{\mathbf{A}, \mathbf{E}, \mathbf{O}, \mathbf{P}\}$ then the following are also state formulae:

$$\begin{array}{lllll} \neg\varphi & \varphi \vee \psi & \varphi \wedge \psi & \varphi \Rightarrow \psi & \\ \mathbf{H}\Diamond\varphi & \mathbf{H}\Box\varphi & \mathbf{H}\bigcirc\varphi & \mathbf{H}(\varphi\,\mathcal{U}\,\psi) & \mathbf{H}(\varphi\,\mathcal{W}\,\psi) \end{array}$$

RoCTL$^-$ is the fragment of RoCTL without the robustly ($\blacktriangle$) and prone ($\triangle$) operators. Hence all well-formed RoCTL$^-$ formulae are state formulae.

A RoCTL structure, M, is a 4-tuple $\langle A, \xrightarrow{s}, \xrightarrow{f}, \alpha\rangle$ such that

- A is a set of states;
- $\xrightarrow{s}$ is a serial, binary success relation over A;
- $\xrightarrow{f}$ is a binary failure relation over A;
- α is a valuation (a map from A to the powerset of propositional variables).

Let $\rightarrow$ be an abbreviation for $\xrightarrow{s} \cup \xrightarrow{f}$. A *fullpath* is an infinite sequence of states $\sigma = \langle w_0, w_1, w_2, \ldots\rangle$ such that for all $i \geqslant 0$ $(w_i, w_{i+1}) \in\rightarrow$. Let $\sigma_{\geqslant i}$ be the fullpath $w_i, w_{i+1}, \ldots$, let σ_i be w_i and $\sigma_{\leqslant i}$ be $w_0, \ldots w_i$.

Definition 1. *A fullpath is* failure free *if and only if for all $i \in \mathbb{N}$ we have $w_i \xrightarrow{s} w_{i+1}$. Let $SF(w)$ be the set of fullpaths in M starting at state w and $S(w)$ be the set of all failure free fullpaths in M starting with w.*

Definition 2. *For two fullpaths σ and π, π is an* i-deviation *from σ if and only if $\sigma_{\leqslant i} = \pi_{\leqslant i}$ and $\pi_{\geqslant i+1} \in S(\pi_{i+1})$. π is a deviation from σ if there exists a non-negative integer i such that π is an i-deviation from σ. A function δ from a fullpath to a set of fullpaths is defined as: π is a member of $\delta(\sigma)$ if and only if π is a deviation from σ where σ and π are fullpaths.*

Let $\sigma_{\leqslant i}$ be a finite path and π be a fullpath such that $\sigma_i = \pi_0$. We denote the path formed from following $\sigma_{\leqslant i}$ and then π by $\langle \sigma_{\leqslant i} : \pi \rangle$.

The semantics of RoCTL formulae are defined on a fullpath $\sigma = \langle w_0, w_1, \ldots \rangle$ in a RoCTL structure M as follows. Recall $\sigma_i = w_i$ so $\sigma_0 = w_0$.

$$\begin{aligned}
M, \sigma \models p &\text{ iff } p \in \text{PROP} \text{ and } p \in \alpha(\sigma_0) \\
M, \sigma \models \neg\varphi &\text{ iff } M, \sigma \not\models \varphi \\
M, \sigma \models \varphi \wedge \psi &\text{ iff } M, \sigma \models \varphi \text{ and } M, \sigma \models \psi \\
M, \sigma \models \bigcirc\varphi &\text{ iff } M, \sigma_{\geqslant 1} \models \varphi \\
M, \sigma \models \Box\varphi &\text{ iff } \forall i \in \mathbb{N}, M, \sigma_{\geqslant i} \models \varphi \\
M, \sigma \models \Diamond\varphi &\text{ iff } \exists i \in \mathbb{N}, M, \sigma_{\geqslant i} \models \varphi \\
M, \sigma \models \varphi \mathcal{U} \psi &\text{ iff } \exists i \in \mathbb{N} \text{ s.t. } M, \sigma_{\geqslant i} \models \psi \text{ and } \forall j \in \mathbb{N} \text{ s.t. } j < i,\ M, \sigma_{\geqslant j} \models \varphi \\
M, \sigma \models \varphi \mathcal{W} \psi &\text{ iff } M, \sigma \models \Box\varphi \text{ or } M, \sigma \models \varphi \mathcal{U} \psi \\
M, \sigma \models \mathbf{A}\varphi &\text{ iff } \forall \pi \in SF(\sigma_0)\ M, \pi \models \varphi \\
M, \sigma \models \mathbf{O}\varphi &\text{ iff } \forall \pi \in S(\sigma_0)\ M, \pi \models \varphi \\
M, \sigma \models \blacktriangle\varphi &\text{ iff } M, \sigma \models \varphi \text{ and } \forall \pi \in \delta(\sigma)\ M, \pi \models \varphi
\end{aligned}$$

The definitions for other Boolean operators are as we would expect from classical logic. The semantics of other operators can be derived via equivalent formulae where $\mathbf{E}\varphi \equiv \neg\mathbf{A}\neg\varphi$, $\mathbf{P}\varphi \equiv \neg\mathbf{O}\neg\varphi$ and $\triangle\varphi \equiv \neg\blacktriangle\neg\varphi$. We say that a RoCTL formula φ is satisfiable if and only if for some structure M and some path σ, $M, \sigma \models \varphi$.

In the following let a literal be a proposition or a negated proposition.

3 RoCTL Examples

In this section we provide some problems formulated in RoCTL. Examples 2 and 3 have been adapted from the RoCTL* examples in [11].

Example 1. A heart beat link should remain connected, but if the link becomes disconnected, it should remain disconnected. This contrary-to-duty obligation can be formalised in RoCTL if the second obligation is stronger than the first, for example as follows:

$$\mathbf{O}\,\Box c \wedge \mathbf{O}\,\Box \mathbf{A} \bigcirc \mathbf{O}\,\Box\,(\neg c \Rightarrow \mathbf{A}\,\Box \neg c)$$

In this example c is used to represent the system remaining connected. Thus $\mathbf{O}\,\Box c$ represents "It is obligatory that it will always be the case that the system is connected."

Example 2. In the coordinated attack problem we have two generals A and B. General A wants to organise an attack with B. A communication protocol will be presented such that a coordinated attack will occur if no more than one message is lost.

We use the following proposition symbols for $i = A, B$:

- s_i general i sends a message;
- r_i general i receives a message;
- f_i general i commits to an attack.

Below we list requirements of the system, giving the informal English requirements of the system on the right, and the formalization of those requirements on the left.

$\mathbf{A}\,\Box\,(s_A \Rightarrow \mathbf{O} \bigcirc r_B)$: If A sends a message, B should receive it at the next step (and will receive the message if no failure occurs).

$\mathbf{A}\,\Box\,(\neg s_A \Rightarrow \neg\mathbf{E} \bigcirc r_B)$: If A does not send a message now, B will not receive a message at the next step.

$\mathbf{A}\,\Box(f_A \Rightarrow \mathbf{A}\,\Box f_A)$: If A commits to an attack, A cannot withdraw.
$\mathbf{A}\,\Box(f_A \Rightarrow \neg s_A)$: If A has committed to an attack it is too late to send messages.
$\mathbf{A}\,(\neg f_A\,\mathcal{W}\,r_A)$: A cannot commit to an attack until A has received a message (from B).
$\mathbf{A}(\neg r_A\,\mathcal{W}\,s_B)$: A cannot receive a message until B sends one.

Similar constraints to the above also apply to B. Below we add a constraint requiring A to be the general planning the attack.

$\mathbf{A}\,(\neg s_B\,\mathcal{W}\,r_B)$: General B will not send a message until B has received a message.

No protocol exists to satisfy the original coordination problem, since an unbounded number of messages can be lost. Here we only attempt to ensure correct behaviour if one or fewer messages are lost.

$\mathbf{A}\,(s_A\,\mathcal{U}\,r_A)$: General A will send plans until a response is received.
$\mathbf{A}\,\Box\,(r_A \Rightarrow f_A)$: Once general A receives a response, A will commit to an attack.
$\mathbf{A}\,(\neg r_B\,\mathcal{W}\,(r_B \wedge (s_B \wedge \mathbf{A}\bigcirc s_B \wedge \mathbf{A}\bigcirc\mathbf{A}\bigcirc f_B)))$: Once general B receives plans, B will send two messages to A and then commit to an attack.

Having the formal statement of the policy above and the semantics of RoCTL we may want to prove, for example that the policy $\hat{\varphi}$ is consistent and that it implies correct behaviour even if a single failure occurs:

$$\hat{\varphi} \Rightarrow \mathbf{O}\,\Box\blacktriangle\Diamond(f_A \wedge f_B)\,.$$

Example 3. We have a cat that does not eat the hour after it has eaten. If the cat bowl is empty we might forget to fill it. We must ensure that the cat never goes hungry, even if we forget to fill the cat bowl one hour. At the beginning of the first hour, the cat bowl is full. We have the following variables:

b "The cat bowl is full at the beginning of this hour"
d "This hour is feeding time"

We can translate the statements above into RoCTL statements:

1. $\mathbf{A}\,\Box(d \Rightarrow \mathbf{A}\bigcirc\neg d)$: If this hour is feeding time, the next is not.
2. $\mathbf{A}\,\Box((d \vee \neg b) \Rightarrow \triangle\bigcirc\neg b)$: If it is feeding time or the cat bowl was empty, a single failure may result in an empty bowl at the next step
3. $\mathbf{A}\,\Box((\neg d \wedge b) \Rightarrow \mathbf{A}\bigcirc b)$: If the bowl is full and it is not feeding time, the bowl will be full at the beginning of the next hour.
4. $\mathbf{O}\,\Box\blacktriangle\,\Box\,(d \Rightarrow b)$: It is obligatory that, even if a single failure occurs, it is always the case that the bowl must be full at feeding time.
5. b: The cat bowl starts full.

Having the formalised the policy it can be proven that the policy is consistent and that the policy implies $\mathbf{O}\,\Box\blacktriangle\,\Box\mathbf{O}\bigcirc b$, indicating that the bowl must be filled at every step (in case we forget at the next step), unless we have already failed twice. The formula $\mathbf{A}\,\Box\mathbf{O}\bigcirc b \Rightarrow \mathbf{O}\,\Box\blacktriangle\,\Box\,(d \Rightarrow b)$ can also be derived, indicating that following a policy requiring us to always attempt to fill the cat bowl ensures that we will not starve the cat even if we make a single mistake. Thus following this simpler policy is sufficient to discharge our original obligation.

4 CTL

CTL [6] is a branching time temporal logic which is the fragment of CTL* [7] such that every path operator is paired with a temporal operator. Well formed formulae of CTL are constructed from the same elements as RoCTL but without the operators $\mathbf{O}$, $\mathbf{P}$, $\blacktriangle$ and $\triangle$.

- **false**, **true** and any element of PROP is in WFF;
- if φ and ψ are in WFF and $\mathbf{H} \in \{\mathbf{A}, \mathbf{E}\}$ then the following are in WFF:

$$\begin{array}{lllll} \neg\varphi & \varphi \vee \psi & \varphi \wedge \psi & \varphi \Rightarrow \psi & \\ \mathbf{H}\Diamond\varphi & \mathbf{H}\,\Box\varphi & \mathbf{H}\bigcirc\varphi & \mathbf{H}(\varphi\,\mathcal{U}\,\psi) & \mathbf{H}(\varphi\,\mathcal{W}\,\psi) \end{array}$$

CTL formulae are interpreted over structures $\mathcal{M}$ such that $\mathcal{M} = \langle S, R, L\rangle$ where S is a set of states, R is a binary relation, and L is a valuation (a map from S to the powerset of propositional variables). A *fullpath*, σ, over R, is a sequence of states $\sigma = \langle w_0, w_1, w_2, \ldots\rangle$ such that for all $i \geqslant 0$, $(w_i, w_{i+1}) \in R$. Using the same terminology as for RoCTL. where $SF(w)$ is the set of fullpaths in M starting at state w, the semantics of CTL formulae are as follows. We omit the semantics for Boolean operators as they are standard.

$$
\begin{array}{rcl}
\mathcal{M}, \sigma \models \bigcirc\varphi & \text{iff} & \mathcal{M}, \sigma_{\geqslant 1} \models \varphi \\
\mathcal{M}, \sigma \models \Box\varphi & \text{iff} & \forall i \in \mathbb{N}, \mathcal{M}, \sigma_{\geqslant i} \models \varphi \\
\mathcal{M}, \sigma \models \Diamond\varphi & \text{iff} & \exists i \in \mathbb{N}, \mathcal{M}, \sigma_{\geqslant i} \models \varphi \\
\mathcal{M}, \sigma \models \varphi \mathcal{U} \psi & \text{iff} & \exists i \in \mathbb{N} \text{ s.t. } \mathcal{M}, \sigma_{\geqslant i} \models \psi \text{ and } \forall j \in \mathbb{N} \text{ s.t. } j < i,\ \mathcal{M}, \sigma_{\geqslant j} \models \varphi \\
\mathcal{M}, \sigma \models \varphi \mathcal{W} \psi & \text{iff} & \mathcal{M}, \sigma \models \Box\varphi \text{ or } \mathcal{M}, \sigma \models \varphi \mathcal{U} \psi \\
\mathcal{M}, \sigma \models \mathbf{A}\varphi & \text{iff} & \forall \pi \in SF(\sigma_0)\ \mathcal{M}, \pi \models \varphi \\
\mathcal{M}, \sigma \models \mathbf{E}\varphi & \text{iff} & \exists \pi \in SF(\sigma_0)\ \mathcal{M}, \pi \models \varphi
\end{array}
$$

CTL formulae are evaluated over CTL structures and do not have the O or $\blacktriangle$ operator, otherwise the semantics of CTL are the same as the semantics for RoCTL defined above.

4.1 A Normal Form for CTL

Next we present a normal form for CTL known as SNF$_{CTL}$. Any CTL formula φ can be translated into this normal form giving φ' such that φ is satisfiable if and only if φ' is satisfiable [18]. For the purposes of the normal form we introduce a symbol **start** such that **start** holds only at the initial moment in time.

Some clauses are labelled by indices *ind* which are taken from a set *Ind*. Formulae in SNF$_{CTL}$ are of the general form $\mathbf{A}\Box \bigwedge_i C_i$ where each C_i is known as a *clause* and must be one of the following forms.

$$
\begin{array}{lll}
\mathbf{start} \Rightarrow \bigvee_{b=1}^{r} l_b & & \text{(an } \textit{initial} \text{ clause)} \\
\mathbf{true} \Rightarrow \bigvee_{b=1}^{r} l_b & & \text{(a } \textit{global} \text{ clause)} \\
\bigwedge_{a=1}^{g} k_a \Rightarrow \mathbf{A}\bigcirc \bigvee_{b=1}^{r} l_b & & \text{(an } \mathbf{A} \textit{ step} \text{ clause)} \\
\bigwedge_{a=1}^{g} k_a \Rightarrow \mathbf{E}\bigcirc \bigvee_{b=1}^{r} l_{b\langle ind\rangle} & & \text{(a } \mathbf{E} \textit{ step} \text{ clause)} \\
\bigwedge_{a=1}^{g} k_a \Rightarrow \mathbf{A}\Diamond l & & \text{(an } \mathbf{A} \textit{ sometime} \text{ clause)} \\
\bigwedge_{a=1}^{g} k_a \Rightarrow \mathbf{E}\Diamond l_{\langle ind\rangle} & & \text{(a } \mathbf{E} \textit{ sometime} \text{ clause)}
\end{array}
$$

Here k_a, l_b, and l are literals, $\langle ind\rangle$ is an index that is present on $\mathbf{E}$ step clauses and on $\mathbf{E}$ sometime clauses. This index indicates a particular next relation and arises, for example, from the translation of formulae such as $\mathbf{E}(\varphi \mathcal{U} \psi)$. During the translation to the normal form such formulae are translated into several $\mathbf{E}$ step clauses and a $\mathbf{E}$ sometime clause (which ensures that ψ must actually hold). To indicate that all these clauses refer to the same path they are annotated with an index. The outer '$\mathbf{A}\Box$' operator that surrounds the conjunction of clauses is usually omitted. Similarly, for convenience the conjunction is dropped and we consider just the set of clauses C_i.

CTL formulae are interpreted over structures $\mathcal{M}$ such that $\mathcal{M} = \langle S, R, L\rangle$ where S is a set of states, R is a binary relation, and L is a valuation (a map from S to the powerset of propositional variables). As SNF$_{CTL}$ formulae contain indices we extend CTL structures (see [18]) $\mathcal{M}$ to be $\mathcal{M} = \langle S, R, L, [\_], \mathbf{w}\rangle$, where S, R and L are as previously, $\mathbf{w} \in S$ and $[\_] : Ind \to (S \times S)$ and for every $ind \in Ind$, $[ind]$ is a total functional relation such that if $(w_i, w_{i+1}) \in [ind]$ then $(w_i, w_{i+1}) \in R$. An infinite path $\sigma^{\langle ind\rangle}$ is an infinite sequence of states $w_0, w_1, w_2, \ldots$ such that for all $i \geqslant 0$, $(w_i, w_{i+1}) \in [ind]$. The semantics of

SNF$_{CTL}$ is then defined as shown below as an extension of the semantics of CTL defined earlier.

$$\begin{array}{rl}
\mathcal{M}, \sigma \models \mathbf{start} & \text{iff } \sigma_0 = \mathbf{w} \\
\mathcal{M}, \sigma \models \mathbf{E}\bigcirc\psi_{\langle ind\rangle} & \text{iff } \exists\pi^{\langle ind\rangle} \in SF(\sigma_0) \text{ s.t. } \mathcal{M}, \pi^{\langle ind\rangle}_{\geqslant 1} \models \psi \\
\mathcal{M}, \sigma \models \mathbf{E}\,\square\psi_{\langle ind\rangle} & \text{iff } \exists\pi^{\langle ind\rangle} \in SF(\sigma_0) \text{ s.t. } \forall i \in \mathbb{N}, \mathcal{M}, \pi^{\langle ind\rangle}_{\geqslant i} \models \psi \\
\mathcal{M}, \sigma \models \mathbf{E}\Diamond\psi_{\langle ind\rangle} & \text{iff } \exists\pi^{\langle ind\rangle} \in SF(\sigma_0) \text{ s.t. } \exists i \in \mathbb{N}, \text{ and } \mathcal{M}, \pi^{\langle ind\rangle}_{\geqslant i} \models \psi \\
\mathcal{M}, \sigma \models \mathbf{E}\varphi\,\mathcal{U}\,\psi_{\langle ind\rangle} & \text{iff } \exists\pi^{\langle ind\rangle} \in SF(\sigma_0) \text{ s.t. } \exists i \in \mathbb{N} \text{ and } \mathcal{M}, \pi^{\langle ind\rangle}_{\geqslant i} \models \psi \\
& \text{and } \forall j \in \mathbb{N} j < i, \mathcal{M}, \pi^{\langle ind\rangle}_{\geqslant j} \models \varphi \\
\mathcal{M}, \sigma \models \mathbf{E}\varphi\,\mathcal{W}\,\psi_{\langle ind\rangle} & \text{iff } \exists\pi^{\langle ind\rangle} \in SF(\sigma_0), \text{ s.t. } \mathcal{M}, \sigma \models \mathbf{E}\,\square\varphi_{\langle ind\rangle} \text{ or} \\
& \mathcal{M}, \sigma \models \mathbf{E}\varphi\,\mathcal{U}\,\psi_{\langle ind\rangle}
\end{array}$$

A set of SNF$_{CTL}$ clauses C are said to be satisfied in a model $\mathcal{M}$ if for each $C_i \in C$, $\mathcal{M}, w_0 \models C_i$ where w_0 is the root node of the model $\mathcal{M}$.

5 Translating RoCTL$^-$ into CTL

Next we provide a satisfiability preserving translation of RoCTL$^-$ into CTL. Without loss of generality we assume that the RoCTL$^-$ formula to be translated into CTL is in *negation normal form*; it is simple to show that we may convert any RoCTL$^-$ formula into negation normal form by pushing negations through to atoms using standard equivalences (see e.g. [8, 11]).

We replace temporal subformulae in the scope of other temporal operators by new propositions and add new formulae enforcing that the replaced subformulae hold when the new proposition is satisfied everywhere in the RoCTL structure. This reduces the nesting of the temporal operators in the original formula so that they aren't in the scope of any other temporal operator. The newly added formulae will have the replaced temporal formulae in the scope of the $\mathbf{A}\,\square$ operators. In the resulting formulae we also replace subformulae that are not literals in the scope of permissible and obligatory operators by new propositions again adding formulae enforcing the replaced subformulae hold when the new proposition is satisfied. This means that formula involving permissible and obligatory operators only apply to literals rather than complex subformulae. Finally we apply the translation, τ to non-CTL formulae. As RoCTL$^-$ formulae are interpreted in structures with two types of relation, success and failure, during the translation we introduce a new propositional variable *viol* which holds in states w_{j+1} in the CTL model structures which correspond to states w_{j+1} in the RoCTL model structures where $(w_j, w_{j+1}) \in \xrightarrow{f}$. Other new propositions are introduced to re-name complex subformulae as described above. First we introduce some definitions.

Definition 3. *The depth of a RoCTL$^-$ formula, φ, denoted depth(φ) is defined as follows where $\mathbf{H} \in \{\mathbf{A}, \mathbf{E}, \mathbf{O}, \mathbf{P}\}$ and φ, ψ are RoCTL$^-$ formulae.*

$$\begin{array}{l}
depth(p) = 0 \text{ where } p \in \textsc{prop} \\
depth(\neg\varphi) = depth(\varphi) \\
depth(\varphi \wedge \psi) = depth(\varphi \vee \psi) = depth(\varphi \Rightarrow \psi) = max(depth(\varphi), depth(\psi)) \\
depth(\mathbf{H}\bigcirc\varphi) = depth(\mathbf{H}\,\square\varphi) = depth(\mathbf{H}\Diamond\varphi) = 1 + depth(\varphi) \\
depth(\mathbf{H}\varphi\,\mathcal{U}\,\psi) = depth(\mathbf{H}\varphi\,\mathcal{W}\,\psi) = 1 + max(depth(\varphi), depth(\psi))
\end{array}$$

In the following we assume that Boolean combinations involving **true** and **false** are simplified using the usual equivalences.

Translation of RoCTL$^-$ Formulae into CTL

Let the original RoCTL$^-$ formula (in negation normal form) be φ and let $\varphi_R = \mathbf{true}$.

1. In φ repeatedly replace sub-formulae with main operator $\mathbf{A}, \mathbf{E}, \mathbf{O}, \mathbf{P}$ of depth 1, ψ , in the scope of another temporal operator by a new proposition t_i until $depth(\varphi) \leqslant 1$ and let $\varphi_R = \varphi_R \wedge \mathbf{A}\,\square(t_i \Rightarrow \psi)$.
2. For any subformula of φ or φ_R where $\mathbf{H} \in \{\mathbf{O}, \mathbf{P}\}$, of the following forms $\mathbf{H}\bigcirc\psi_1$, $\mathbf{H}\,\square\psi_1$, $\mathbf{H}\Diamond\psi_1$, $\mathbf{H}\psi_1\,\mathcal{U}\,\psi_2$, $\mathbf{H}\psi_1\,\mathcal{W}\,\psi_2$, where ψ_1 (respectively ψ_2) is not a literal, replace ψ_1 (respectively ψ_2) by a new proposition t_j and conjoin $\mathbf{A}\,\square(t_j \Rightarrow \psi_1)$ (respectively $\mathbf{A}\,\square(t_j \Rightarrow \psi_2)$) to φ_R.

3. Apply the translation τ to $\varphi \wedge \varphi_R \wedge \mathbf{A}\,\Box \mathbf{E}\bigcirc\neg viol$ where τ is defined as follows.

$$\begin{aligned}
\tau(\varphi) &= \varphi \text{ for any CTL formula } \varphi \\
\tau(\varphi \wedge \psi) &= \tau(\varphi) \wedge \tau(\psi) \text{ if either } \varphi \text{ or } \psi \text{ is not a CTL formula} \\
\tau(\varphi \vee \psi) &= \tau(\varphi) \vee \tau(\psi) \text{ if either } \varphi \text{ or } \psi \text{ is not a CTL formula} \\
\tau(\mathbf{A}\,\Box(l \Rightarrow \varphi)) &= \mathbf{A}\,\Box(l \Rightarrow \tau(\varphi)) \text{ if } l \text{ is a literal and } \varphi \text{ is not a CTL formula} \\
\\
\tau(\mathbf{P}\bigcirc l) &= \mathbf{E}\bigcirc(\neg viol \wedge l) \\
\tau(\mathbf{P}\,\Box l) &= l \wedge \mathbf{E}\bigcirc\mathbf{E}\,\Box(\neg viol \wedge l) \\
\tau(\mathbf{P}\Diamond l) &= l \vee \mathbf{E}\bigcirc\mathbf{E}(\neg viol\,\mathcal{U}\,(\neg viol \wedge l)) \\
\tau(\mathbf{P} l_1\,\mathcal{U}\,l_2) &= l_2 \vee (l_1 \wedge \mathbf{E}\bigcirc\mathbf{E}((\neg viol \wedge l_1)\,\mathcal{U}\,(\neg viol \wedge l_2))) \\
\tau(\mathbf{P} l_1\,\mathcal{W}\,l_2) &= l_2 \vee (l_1 \wedge \mathbf{E}\bigcirc\mathbf{E}((\neg viol \wedge l_1)\,\mathcal{W}\,(\neg viol \wedge l_2))) \\
\\
\tau(\mathbf{O}\bigcirc l) &= \mathbf{A}\bigcirc(viol \vee l) \\
\tau(\mathbf{O}\,\Box l) &= l \wedge \mathbf{A}\bigcirc\mathbf{A}((viol \vee l)\,\mathcal{W}\,viol) \\
\tau(\mathbf{O}\Diamond l) &= l \vee \mathbf{A}\bigcirc\mathbf{A}\Diamond(l \vee viol) \\
\tau(\mathbf{O} l_1\,\mathcal{U}\,l_2) &= l_2 \vee (l_1 \wedge \mathbf{A}\bigcirc\mathbf{A}((viol \vee l_1)\,\mathcal{U}\,(viol \vee l_2))) \\
\tau(\mathbf{O} l_1\,\mathcal{W}\,l_2) &= l_2 \vee (l_1 \wedge \mathbf{A}\bigcirc\mathbf{A}((viol \vee l_1)\,\mathcal{W}\,(viol \vee l_2)))
\end{aligned}$$

6 Example Translations

In this section we show how to translate some examples from RoCTL$^-$ into CTL. First we consider the heart beat example from Section 3 and then translate a simple unsatisfiable formula using both permissible and obligatory operators.

6.1 Heartbeat Example

We show how to translate the heart beat example (Example 1 from Section 3) into CTL. As we assume the problem is in negation normal form let

$$\varphi = \mathbf{O}\,\Box c \wedge \mathbf{O}\,\Box \mathbf{A}\bigcirc\mathbf{O}\,\Box\,(c \vee \mathbf{A}\,\Box\neg c)\,.$$

First (step 1) we rename nested temporal subformulae and obtain

$$\varphi = \mathbf{O}\,\Box c \wedge \mathbf{O}\,\Box t_3$$

and

$$\begin{aligned}
\varphi_R = {} & \mathbf{A}\,\Box(t_3 \Rightarrow \mathbf{A}\bigcirc t_2) \wedge \\
& \mathbf{A}\,\Box(t_2 \Rightarrow \mathbf{O}\,\Box\,(c \vee t_1)) \wedge \\
& \mathbf{A}\,\Box(t_1 \Rightarrow \mathbf{A}\,\Box\neg c).
\end{aligned}$$

Next (step 2) we replace the disjunction below $\mathbf{O}\,\Box$ in $\mathbf{A}\,\Box(t_2 \Rightarrow \mathbf{O}\,\Box\,(c \vee t_1))$ by t_4 to obtain

$$\begin{aligned}
& \mathbf{A}\,\Box(t_2 \Rightarrow \mathbf{O}\,\Box t_4) \\
& \mathbf{A}\,\Box(t_4 \Rightarrow (c \vee t_1)).
\end{aligned}$$

Next we apply τ as follows.

$$\begin{aligned}
& \tau(\mathbf{O}\,\Box c \wedge \mathbf{O}\,\Box t_3 \wedge \\
& \mathbf{A}\,\Box(t_3 \Rightarrow \mathbf{A}\bigcirc t_2) \wedge \\
& \mathbf{A}\,\Box(t_2 \Rightarrow \mathbf{O}\,\Box t_4) \wedge \\
& \mathbf{A}\,\Box(t_4 \Rightarrow (c \vee t_1)) \wedge \\
& \mathbf{A}\,\Box(t_1 \Rightarrow \mathbf{A}\,\Box\neg c) \wedge \\
& \mathbf{A}\,\Box\mathbf{E}\bigcirc\neg viol) \\
= {} & \tau(\mathbf{O}\,\Box c) \wedge \tau(\mathbf{O}\,\Box t_3) \wedge \\
& \mathbf{A}\,\Box(t_3 \Rightarrow \mathbf{A}\bigcirc t_2) \wedge \\
& \mathbf{A}\,\Box(t_2 \Rightarrow \tau(\mathbf{O}\,\Box t_4)) \wedge \\
& \mathbf{A}\,\Box(t_4 \Rightarrow (c \vee t_1)) \wedge \\
& \mathbf{A}\,\Box(t_1 \Rightarrow \mathbf{A}\,\Box\neg c) \wedge \\
& \mathbf{A}\,\Box\mathbf{E}\bigcirc\neg viol
\end{aligned}$$

The translation τ applied to these subformulae is as follows.

$$\begin{aligned}
\tau(\mathbf{O}\,\square c) &= c \wedge \mathbf{A}\bigcirc\mathbf{A}((viol \vee c)\,\mathcal{W}\,viol)\\
\tau(\mathbf{O}\,\square t_3) &= t_3 \wedge \mathbf{A}\bigcirc\mathbf{A}((viol \vee t_3)\,\mathcal{W}\,viol)\\
\tau(\mathbf{O}\,\square t_4) &= t_4 \wedge \mathbf{A}\bigcirc\mathbf{A}((viol \vee t_4)\,\mathcal{W}\,viol)
\end{aligned}$$

The final set of CTL formulae is as follows.

$$\begin{array}{l}
c \wedge \mathbf{A}\bigcirc\mathbf{A}((viol \vee c)\,\mathcal{W}\,viol)\wedge\\
t_3 \wedge \mathbf{A}\bigcirc\mathbf{A}((viol \vee t_3)\,\mathcal{W}\,viol)\wedge\\
\mathbf{A}\,\square(t_3 \Rightarrow \mathbf{A}\bigcirc t_2)\wedge\\
\mathbf{A}\,\square(t_2 \Rightarrow (t_4 \wedge \mathbf{A}\bigcirc\mathbf{A}((viol \vee t_4)\,\mathcal{W}\,viol)))\wedge\\
\mathbf{A}\,\square(t_4 \Rightarrow (c \vee t_1))\wedge\\
\mathbf{A}\,\square(t_1 \Rightarrow \mathbf{A}\,\square\neg c)\wedge\\
\mathbf{A}\,\square\mathbf{E}\bigcirc\neg viol
\end{array}$$

6.2 Permissible/Obligatory Formula

Consider the formula $\mathbf{P}\,\square\neg q \wedge \mathbf{O}p\,\mathcal{U}\,q$ which is unsatisfiable. As both steps 1 and 2 of the algorithm cannot be applied as there are no nested temporal formulae and formulae in the scope of the obligatory and permissible operators are literals we only have to apply τ.

$$\begin{array}{ll}
& \tau(\mathbf{P}\,\square\neg q \wedge \mathbf{O}p\,\mathcal{U}\,q\\
& \wedge\mathbf{A}\,\square\mathbf{E}\bigcirc\neg viol)\\
= & \tau(\mathbf{P}\,\square\neg q) \wedge \tau(\mathbf{O}p\,\mathcal{U}\,q)\\
& \wedge\mathbf{A}\,\square\mathbf{E}\bigcirc\neg viol\\
= & \neg q \wedge \mathbf{E}\bigcirc\mathbf{E}\,\square(\neg viol \wedge \neg q)\wedge\\
& q \vee (p \wedge \mathbf{A}\bigcirc\mathbf{A}((viol \vee p)\,\mathcal{U}\,(viol \vee q)))\wedge\\
& \mathbf{A}\,\square\mathbf{E}\bigcirc\neg viol
\end{array}$$

7 Resolution for CTL

The following resolution calculus for CTL was presented in [18] and has been shown to be sound, complete and terminating [18]. The resolution rules presented are split into three groups, initial resolution, step resolution and temporal resolution. The first two types of resolution are variants of classical resolution. Temporal resolution, however, is an extension allowing the resolution between formulae such as $\square p$ with $\diamondsuit\neg p$ on the same path.

Initial, global or step clauses may be resolved together as follows where in the following P and Q are conjunctions of literals and F and G are disjunction of literals.

$$\text{[IRES1]}\quad \frac{\begin{array}{l}\mathbf{start} \Rightarrow (F \vee l)\\ \mathbf{start} \Rightarrow (G \vee \neg l)\end{array}}{\mathbf{start} \Rightarrow (F \vee G)} \qquad \text{[IRES2]}\quad \frac{\begin{array}{r}\mathbf{start} \Rightarrow (F \vee l)\\ \mathbf{true} \Rightarrow (G \vee \neg l)\end{array}}{\mathbf{start} \Rightarrow (F \vee G)}$$

$$\text{[SRES1]}\quad \frac{\begin{array}{r}P \Rightarrow \mathbf{A}\bigcirc(F \vee l)\\ Q \Rightarrow \mathbf{A}\bigcirc(G \vee \neg l)\end{array}}{(P \wedge Q) \Rightarrow \mathbf{A}\bigcirc(F \vee G)} \qquad \text{[SRES2]}\quad \frac{\begin{array}{r}P \Rightarrow \mathbf{E}\bigcirc(F \vee l)_{\langle ind\rangle}\\ Q \Rightarrow \mathbf{A}\bigcirc(G \vee \neg l)\end{array}}{(P \wedge Q) \Rightarrow \mathbf{E}\bigcirc(F \vee G)_{\langle ind\rangle}}$$

$$\text{[SRES3]}\quad \frac{\begin{array}{r}P \Rightarrow \mathbf{E}\bigcirc(F \vee l)_{\langle ind\rangle}\\ Q \Rightarrow \mathbf{E}\bigcirc(G \vee \neg l)_{\langle ind\rangle}\end{array}}{(P \wedge Q) \Rightarrow \mathbf{E}\bigcirc(F \vee G)_{\langle ind\rangle}} \qquad \text{[SRES4]}\quad \frac{\begin{array}{r}\mathbf{true} \Rightarrow (F \vee l)\\ Q \Rightarrow \mathbf{A}\bigcirc(G \vee \neg l)\end{array}}{Q \Rightarrow \mathbf{A}\bigcirc(F \vee G)}$$

$$\text{[SRES5]}\quad \frac{\begin{array}{r}\mathbf{true} \Rightarrow (F \vee l)\\ Q \Rightarrow \mathbf{E}\bigcirc(G \vee \neg l)_{\langle ind\rangle}\end{array}}{Q \Rightarrow \mathbf{E}\bigcirc(F \vee G)_{\langle ind\rangle}} \qquad \text{[SRES6]}\quad \frac{\begin{array}{r}\mathbf{true} \Rightarrow (F \vee l)\\ \mathbf{true} \Rightarrow (G \vee \neg l)\end{array}}{\mathbf{true} \Rightarrow (F \vee G)}$$

Simplification and subsumption rules are also applied. Once a contradiction within a state is found, the following rules can be used to generate extra global constraints.

$$\text{[SRES7]} \quad \frac{Q \Rightarrow \mathbf{A}\bigcirc\mathbf{false}}{\mathbf{true} \Rightarrow \neg Q} \quad \text{[SRES8]} \quad \frac{Q \Rightarrow \mathbf{E}\bigcirc\mathbf{false}_{\langle ind \rangle}}{\mathbf{true} \Rightarrow \neg Q}$$

During temporal resolution the aim is to resolve one of the sometime clauses, $Q \Rightarrow \mathbf{H}\Diamond l$ (where $\mathbf{H}$ is $\mathbf{A}$ or $\mathbf{E}$), with a set of clauses that together imply $\Box\neg l$ *along the same path*, for example a set of clauses that together have the effect of $P \Rightarrow \mathbf{E}\bigcirc(\mathbf{E}\Box\neg l_{\langle ind \rangle})_{\langle ind' \rangle}$.

$$\begin{array}{ll}
\text{[ERES1]} & \text{[ERES2]} \\
P \Rightarrow \mathbf{E}\bigcirc(\mathbf{E}\Box\neg l_{\langle ind \rangle})_{\langle ind' \rangle} & P \Rightarrow \mathbf{E}\bigcirc(\mathbf{E}\Box\neg l_{\langle ind \rangle})_{\langle ind \rangle} \\
Q \Rightarrow \mathbf{A}\Diamond l & Q \Rightarrow \mathbf{E}\Diamond l_{\langle ind \rangle} \\
\hline
Q \Rightarrow \mathbf{A}(\neg P\,\mathcal{W}\,l) & Q \Rightarrow \mathbf{E}(\neg P\,\mathcal{W}\,l)_{\langle ind \rangle}
\end{array}$$

In each case the resolvent ensures that once Q has been satisfied, meaning that the eventuality $\Diamond l$ must be satisfied on some or all paths, the conditions for triggering a $\Box$-formula are not allowed to occur, i.e., either P must be false at every future moment or must be false until the eventuality (l) has been satisfied. It may be surprising that resolving a $\mathbf{A}$-formula with a $\mathbf{E}$-formula in ERES1 results in a $\mathbf{A}$-formula. This is because the eventuality l must appear on *all* paths so similarly the resolvent will also hold on all paths. Formulae of the form $\mathbf{E}\bigcirc(\mathbf{E}\Box\neg l_{\langle ind \rangle})_{\langle ind' \rangle}$ are constructed from the conjunction of one or more step or global clauses, for example $a \Rightarrow \mathbf{E}\bigcirc(a \wedge \neg l)_{\langle ind \rangle}$. Similarly the resolvent is rewritten into several step or global clauses labelled where appropriate by $\langle ind \rangle$. For more details see [18].

The calculus terminates when either no new resolvents are derived, or **false** is derived in the form of either **start** $\Rightarrow$ **false** or **true** $\Rightarrow$ **false**.

8 Resolution Examples

Next we translate the examples from Section 6 into normal form and show how to apply the resolution rules to the resulting SNF_{CTL} clauses. To save space we abbreviate the names of the resolution rules IRES1 to I1, SRES1 to S1 and ERES1 to E1 etc. New propositions introduced during the translation to normal form are denoted by r_i.

8.1 Example: Permissible/Obligatory Formula

Consider the formula $\mathbf{P}\Box\neg q \wedge \mathbf{O}p\,\mathcal{U}\,q$ which is unsatisfiable. Previously we saw that translating this into CTL gave

$$\begin{array}{l}
\neg q \wedge \mathbf{E}\bigcirc\mathbf{E}\Box(\neg viol \wedge \neg q) \wedge \\
q \vee (p \wedge \mathbf{A}\bigcirc\mathbf{A}((viol \vee p)\,\mathcal{U}\,(viol \vee q))) \wedge \\
\mathbf{A}\Box\mathbf{E}\bigcirc\neg viol
\end{array}$$

Translating into SNF we obtain the following where clauses 1–6 are from the first two conjuncts, 7–15 from the third conjunct and clause 16 from the final conjunct.

$$
\begin{array}{rl}
1. & \mathbf{start} \Rightarrow \neg q \\
2. & \mathbf{start} \Rightarrow r_0 \\
3. & r_0 \Rightarrow \mathbf{E}\bigcirc r_{2\langle ind_1 \rangle} \\
4. & r_2 \Rightarrow \mathbf{E}\bigcirc r_{2\langle ind_2 \rangle} \\
5. & \mathbf{true} \Rightarrow \neg r_2 \vee \neg viol \\
6. & \mathbf{true} \Rightarrow \neg r_2 \vee \neg q \\
7. & \mathbf{start} \Rightarrow q \vee r_3 \\
8. & \mathbf{true} \Rightarrow \neg r_3 \vee p \\
9. & r_3 \Rightarrow \mathbf{A}\bigcirc r_4 \\
10. & \mathbf{true} \Rightarrow \neg r_4 \vee viol \vee q \vee p \\
11. & \mathbf{true} \Rightarrow \neg r_4 \vee viol \vee q \vee r_5 \\
12. & r_4 \Rightarrow \mathbf{A}\Diamond r_6 \\
13. & \mathbf{true} \Rightarrow \neg r_6 \vee viol \vee q \\
14. & r_5 \Rightarrow \mathbf{A}\bigcirc(viol \vee q \vee p) \\
15. & r_5 \Rightarrow \mathbf{A}\bigcirc(viol \vee q \vee r_5) \\
16. & \mathbf{true} \Rightarrow \mathbf{E}\bigcirc \neg viol_{\langle ind_3 \rangle}
\end{array}
$$

The proof continues as follows.

$$
\begin{array}{rll}
17. & \mathbf{true} \Rightarrow \neg r_6 \vee \neg r_2 \vee q & [5, 13, S6] \\
18. & \mathbf{true} \Rightarrow \neg r_6 \vee \neg r_2 & [6, 17, S6] \\
19. & r_2 \Rightarrow \mathbf{E}\bigcirc \neg r_{6\langle ind_2 \rangle} & [4, 18, S5]
\end{array}
$$

The clauses 4 and 19 together give $r_2 \Rightarrow \mathbf{E}\bigcirc(\mathbf{E}\,\square \neg r_{6\langle ind_2 \rangle})_{\langle ind_2 \rangle}$ to which we can apply temporal resolution with clause 12 obtaining $r_4 \Rightarrow \mathbf{A} \neg r_2 \,\mathcal{W}\, r_6$. Rewriting this into SNF$_{CTL}$ we obtain the clauses 20 and others.

$$
\begin{array}{rll}
20. & \mathbf{true} \Rightarrow (\neg r_4 \vee r_6 \vee \neg r_2) & [4, 12, 19, E1] \\
21. & r_3 \Rightarrow \mathbf{A}\bigcirc(r_6 \vee \neg r_2) & [9, 20, S4] \\
22. & r_3 \Rightarrow \mathbf{A}\bigcirc(viol \vee q \vee \neg r_2) & [13, 21, S4] \\
23. & r_3 \Rightarrow \mathbf{A}\bigcirc(q \vee \neg r_2) & [5, 22, S4] \\
24. & r_3 \Rightarrow \mathbf{A}\bigcirc(\neg r_2) & [6, 23, S4] \\
25. & r_0 \wedge r_3 \Rightarrow \mathbf{E}\bigcirc(\mathbf{false})_{\langle ind_1 \rangle} & [3, 24, S2] \\
26. & \mathbf{true} \Rightarrow \neg r_0 \vee \neg r_3 & [25, S8] \\
27. & \mathbf{start} \Rightarrow \neg r_0 \vee q & [7, 26, I2] \\
28. & \mathbf{start} \Rightarrow \neg r_0 & [1, 27, I1] \\
29. & \mathbf{start} \Rightarrow \mathbf{false} & [2, 28, I1]
\end{array}
$$

As we have derived **start** $\Rightarrow$ **false** the set of clauses and therefore the original formula is unsatisfiable.

8.2 Heartbeat Example

After the translation into CTL we obtained the following formulae.

$$
\begin{array}{l}
c \wedge \mathbf{A}\bigcirc\mathbf{A}((viol \vee c)\,\mathcal{W}\, viol) \wedge \\
t_3 \wedge \mathbf{A}\bigcirc\mathbf{A}((viol \vee t_3)\,\mathcal{W}\, viol) \wedge \\
\mathbf{A}\,\square(t_3 \Rightarrow \mathbf{A}\bigcirc t_2) \wedge \\
\mathbf{A}\,\square(t_2 \Rightarrow (t_4 \wedge \mathbf{A}\bigcirc\mathbf{A}((viol \vee t_4)\,\mathcal{W}\, viol))) \wedge \\
\mathbf{A}\,\square(t_4 \Rightarrow (c \vee t_1)) \wedge \\
\mathbf{A}\,\square(t_1 \Rightarrow \mathbf{A}\,\square \neg c) \wedge \\
\mathbf{A}\,\square\mathbf{E}\bigcirc \neg viol
\end{array}
$$

We can translate into SNF$_{CTL}$ as follows where clauses 1–7 represent the first two conjuncts, clauses 8–13 represent the third and fourth conjuncts, clause 14 represents the fifth conjunct, clauses 15–20 represent the sixth conjunct, clause 21 represents the seventh conjunct and clauses 22–24 represent the eighth conjunct and clause 25 represents the last conjunct.

1. $\mathbf{start} \Rightarrow c$
2. $\mathbf{start} \Rightarrow r_0$
3. $r_0 \Rightarrow \mathbf{A}\bigcirc r_1$
4. $\mathbf{true} \Rightarrow \neg r_1 \vee viol \vee c$
5. $\mathbf{true} \Rightarrow \neg r_1 \vee viol \vee r_2$
6. $r_2 \Rightarrow \mathbf{A}\bigcirc(viol \vee c)$
7. $r_2 \Rightarrow \mathbf{A}\bigcirc(viol \vee r_2)$
8. $\mathbf{start} \Rightarrow t_3$
9. $r_0 \Rightarrow \mathbf{A}\bigcirc r_3$
10. $\mathbf{true} \Rightarrow \neg r_3 \vee viol \vee t_3$
11. $\mathbf{true} \Rightarrow \neg r_3 \vee viol \vee r_4$
12. $r_4 \Rightarrow \mathbf{A}\bigcirc(viol \vee t_3)$
13. $r_4 \Rightarrow \mathbf{A}\bigcirc(viol \vee r_4)$
14. $t_3 \Rightarrow \mathbf{A}\bigcirc t_2$
15. $\mathbf{true} \Rightarrow \neg t_2 \vee t_4$
16. $t_2 \Rightarrow \mathbf{A}\bigcirc r_5$
17. $\mathbf{true} \Rightarrow \neg r_5 \vee viol \vee t_4$
18. $\mathbf{true} \Rightarrow \neg r_5 \vee viol \vee r_6$
19. $r_6 \Rightarrow \mathbf{A}\bigcirc(viol \vee t_4)$
20. $r_6 \Rightarrow \mathbf{A}\bigcirc(viol \vee r_6)$
21. $\mathbf{true} \Rightarrow \neg t_4 \vee c \vee t_1$
22. $\mathbf{true} \Rightarrow \neg t_1 \vee r_7$
23. $r_7 \Rightarrow \mathbf{A}\bigcirc r_7$
24. $\mathbf{true} \Rightarrow \neg r_7 \vee \neg c$
25. $\mathbf{true} \Rightarrow \mathbf{E}\bigcirc \neg viol_{\langle ind_1 \rangle}$

Whilst we may apply initial and step resolution between several clauses we will not be able to derive a contradiction (deriving **false**) showing that this set of clauses is satisfiable. Note we cannot apply temporal resolution as there are no sometime clauses in the set of clauses.

9 Properties of the Translation and RoCTL

Next we show that the transformation from RoCTL$^-$ to CTL is satisfiability preserving. We begin with some definitions.

Definition 4. *Let* flat normal form *be a Boolean combination of formulae of the form φ or $\mathbf{A}\,\square(l \Rightarrow \varphi)$ where either φ is a CTL formula such that $depth(\varphi) \leqslant 1$ or φ is of the form $\mathbf{HT}l_1$ or $\mathbf{H}l_1\mathbf{T}l_2$ where $\mathbf{H}$ is either obligatory or permissible, $\mathbf{T}$ is a temporal operator of suitable arity and l_1, l_2 are literals.*

Lemma 1. *Let φ be a RoCTL$^-$ formula and $NNF(\varphi)$ be the translation of φ into negation normal form. φ is satisfiable if and only if $NNF(\varphi)$ is satisfiable.*

Proof. It can be easily shown that φ can be translated into $NNF(\varphi)$ by applying standard equivalences which push negations through to propositions see for example [8, 11]. Thus φ is satisfiable if and only if $NNF(\varphi)$ is satisfiable.

Lemma 2. *Let φ be a RoCTL formula in negation normal form and $FLAT(\varphi)$ be the translation of φ into flat normal form from applying steps 1 and 2. φ is satisfiable if and only if $FLAT(\varphi)$ is satisfiable.*

Proof. Note first that all well-formed RoCTL$^-$ subformulae of φ are state formulae. It is well known that given a formula φ containing a subformula ψ which is a state formula (not in the scope of a negation) φ is satisfiable if and only if $\varphi' \wedge \mathbf{A}\,\square(t \Rightarrow \psi)$ is satisfiable where t is a new proposition and φ' is φ where the subformula ψ is replaced by t. See for example [5, 15].

Next we show that the translation τ is satisfiability preserving.

Lemma 3. *Let φ be a RoCTL formula in flat normal form and $\tau(\varphi \wedge \mathbf{A}\,\square\mathbf{A}\bigcirc\neg viol)$ be the translation of $\varphi \wedge \mathbf{A}\,\square\mathbf{A}\bigcirc\neg viol$ into CTL. φ is satisfiable in an RoCTL model if and only if $\tau(\varphi \wedge \mathbf{A}\,\square\mathbf{A}\bigcirc\neg viol)$ is satisfiable in a CTL model.*

Proof. First we show if $\tau(\varphi \wedge \mathbf{A}\,\Box\mathbf{A}\bigcirc\neg viol)$ is satisfiable then so is φ. Assume that $\tau(\varphi \wedge \mathbf{A}\,\Box\mathbf{A}\bigcirc\neg viol)$ is satisfiable on some path σ in a CTL structure $\mathcal{M}$ where $\mathcal{M} = \langle S,\ R,\ L\rangle$. We construct a RoCTL model M and show it satisfies φ. We define M in terms of a new function $CONS$ such that $CONS(\mathcal{M}) = M = \langle A, \xrightarrow{s}, \xrightarrow{f}, \alpha\rangle$ where

- $A = S$
- $\xrightarrow{s} = \{(w_i, w_{i+1}) \mid (w_i, w_{i+1}) \in R \text{ and } viol \notin L(w_{i+1})\}$
- $\xrightarrow{f} = \{(w_i, w_{i+1}) \mid (w_i, w_{i+1}) \in R \text{ and } viol \in L(w_{i+1})\}$
- $\alpha(w_i) = L(w_i)$

As $\mathcal{M}, \sigma \models \tau(\varphi \wedge \mathbf{A}\,\Box\mathbf{A}\bigcirc\neg viol)$ from the definition of τ, $\mathcal{M}, \sigma \models \tau(\varphi) \wedge \mathbf{A}\,\Box\mathbf{A}\bigcirc\neg viol$. By the semantics of conjunction $\mathcal{M}, \sigma \models \tau(\varphi)$ and $\mathcal{M}, \sigma \models \mathbf{A}\,\Box\mathbf{A}\bigcirc\neg viol$. From the semantics of $\mathbf{A}\,\Box$ for any reachable state $w_i \in S$ there must be some $w_{i+1} \in S$ such that $(w_i, w_{i+1}) \in R$ and $viol \notin L(w_{i+1})$. That is for any reachable state we can construct a path π such that $\mathcal{M}, \pi_{\geqslant i} \models \neg viol$ for all $i \geqslant 1$. From the construction of M this means that the success relation must be serial required by RoCTL models.

Next we consider the different cases of φ.

- $\varphi = \mathbf{P}\bigcirc l$. Assume that $\tau(\mathbf{P}\bigcirc l)$ is satisfiable on path σ in a CTL model structure $\mathcal{M} = \langle S, R, L\rangle$, i.e. $\mathcal{M}, \sigma \models \mathbf{E}\bigcirc(\neg viol \wedge l)$. We show $M, \sigma \models \mathbf{P}\bigcirc l$ where $M = CONS(\mathcal{M})$. In $\mathcal{M}$ from the semantics of $\mathbf{E}$ and $\bigcirc$ there is a path $\pi \in SF(\sigma_0)$ such that $\sigma_0 = \pi_0$ and $(\pi_0, \pi_1) \in R$ and $\mathcal{M}, \pi_{\geqslant 1} \models (\neg viol \wedge l)$. Additionally from the structure of the CTL models (see above) we can choose π such that $\mathcal{M}, \pi_{\geqslant i} \models \neg viol$ for all $i \geqslant 1$. From the semantics of conjunction $\mathcal{M}, \pi_{\geqslant 1} \models \neg viol$ and $\mathcal{M}, \pi_{\geqslant 1} \models l$. From the definition of the RoCTL structure M as $M, \pi_{\geqslant 1} \models \neg viol$ then $(\pi_0, \pi_1) \in \xrightarrow{s}$ and $M, \pi_{\geqslant 1} \models l$. Further, from how we have chosen π, $M, \pi_{\geqslant i} \models \neg viol$ for all $i \geqslant 1$ then $(\pi_{i-1}, \pi_i) \in \xrightarrow{s}$ and from the semantics of $\mathbf{P}$ and $\bigcirc$, $M, \sigma \models \mathbf{P}\bigcirc l$ as required.
- $\varphi = \mathbf{P}\,\Box l$. Assume that $\tau(\mathbf{P}\,\Box l)$ is satisfiable at some path σ in a CTL model structure $\mathcal{M} = \langle S, R, L\rangle$, i.e. $\mathcal{M}, \sigma \models l \wedge \mathbf{E}\bigcirc\mathbf{E}\,\Box(\neg viol \wedge l)$. We show $M, \sigma \models \mathbf{P}\,\Box l$ where $M = CONS(\mathcal{M})$. In $\mathcal{M}$ from the semantics of conjunction $\mathcal{M}, \sigma \models l$ and $\mathcal{M}, \sigma \models \mathbf{E}\bigcirc\mathbf{E}\,\Box(\neg viol \wedge l)$. In $\mathcal{M}$ from the semantics of $\mathbf{E}$ and $\bigcirc$ there is a path $\pi \in SF(\sigma_0)$ such that $\sigma_0 = \pi_0$ and $(\pi_0, \pi_1) \in R$ and $\mathcal{M}, \pi_{\geqslant 1} \models \mathbf{E}\,\Box(\neg viol \wedge l)$. From the semantics of $\mathbf{E}$ and $\Box$ there is a path $\pi' \in SF(\pi_1)$ such that $\pi_1 = \pi'_0$ and $(\pi'_i, \pi'_{i+1}) \in R$ for $i \geqslant 0$ and $\mathcal{M}, \pi'_{\geqslant i} \models (\neg viol \wedge l)$ for all $i \geqslant 0$. From the semantics of conjunction for all $i \geqslant 0$, $\mathcal{M}, \pi'_{\geqslant i} \models \neg viol$ and $\mathcal{M}, \pi'_{\geqslant i} \models l$. From the definition of the RoCTL structure M, $M, \pi'_{\geqslant i} \models l$ for all $i \geqslant 0$ and as $M, \pi'_{\geqslant i} \models \neg viol$ for all $i \geqslant 0$ then $(\pi'_i, \pi'_{i+1}) \in \xrightarrow{s}$. Further as $\mathcal{M}, \pi'_{\geqslant 0} \models \neg viol$, $\pi_1 = \pi'_0$ and $(\pi_0, \pi_1) \in R$ in the CTL model we have $(\pi_0, \pi_1) \in \xrightarrow{s}$ and the path $\langle \pi_0 : \pi'\rangle$ is failure free. Recall $\mathcal{M}, \sigma \models l$ so $M, \sigma \models l$ and as $\sigma_0 = \pi_0$ then $M, \langle \pi_0 : \pi'\rangle \models l$, $M, \pi'_{\geqslant i} \models l$ for all $i \geqslant 0$ and $\langle \pi_0 : \pi'\rangle \in S(\sigma_0)$ so from the semantics of $\mathbf{P}$ and $\Box$ $M, \sigma \models \mathbf{P}\,\Box l$ as required.
- $\varphi = \mathbf{P}\Diamond l$. Assume that $\tau(\mathbf{P}\Diamond l)$ is satisfiable on some path σ in a CTL model structure $\mathcal{M} = \langle S, R, L\rangle$, i.e. $\mathcal{M}, \sigma \models l \vee \mathbf{E}\bigcirc\mathbf{E}(\neg viol\,\mathcal{U}\,(\neg viol \wedge l))$. We show $M, \sigma \models \mathbf{P}\Diamond l$ where $M = CONS(\mathcal{M})$. In $\mathcal{M}$ from the semantics of disjunction either $\mathcal{M}, \sigma \models l$ or $\mathcal{M}, \sigma \models \mathbf{E}\bigcirc\mathbf{E}(\neg viol\,\mathcal{U}\,(\neg viol \wedge l))$. For the former $\mathcal{M}, \sigma \models l$ and additionally from the structure of the CTL models (see above) we can choose some π such that $\sigma_0 = \pi_0$ so $\mathcal{M}, \pi \models l$ and and $\mathcal{M}, \pi_{\geqslant i} \models \neg viol$ for all $i \geqslant 1$. From the definition of the RoCTL structure M, $M, \pi \models l$ and as $M, \pi_{\geqslant i} \models \neg viol$ for all $i \geqslant 1$ then $(\pi_i, \pi_{i+1}) \in \xrightarrow{s}$ for $i \geqslant 0$ and $\pi \in S(\sigma_0)$ so from the semantics of $\mathbf{P}$ and $\Diamond$, $M, \sigma \models \mathbf{P}\Diamond l$ as required. Next consider the latter, i.e. $\mathcal{M}, \sigma \models \mathbf{E}\bigcirc\mathbf{E}(\neg viol\,\mathcal{U}\,(\neg viol \wedge l))$. In $\mathcal{M}$ from the semantics of $\mathbf{E}$ and $\bigcirc$ there is a path $\pi \in SF(\sigma_0)$ such that $\sigma_0 = \pi_0$ and $(\pi_0, \pi_1) \in R$ and $\mathcal{M}, \pi_{\geqslant 1} \models \mathbf{E}(\neg viol\,\mathcal{U}\,(\neg viol \wedge l))$. From the semantics of $\mathbf{E}$ and $\mathcal{U}$ there is a path $\pi' \in SF(\pi_1)$ such that $\pi_1 = \pi'_0$ and for some j, $\mathcal{M}, \pi'_{\geqslant j} \models (\neg viol \wedge l)$ and for all $0 \leqslant i < j$, $\mathcal{M}, \pi'_{\geqslant i} \models \neg viol$. Additionally from the structure of the CTL models (see above) we can choose π' such that $\mathcal{M}, \pi_{\geqslant j+k} \models \neg viol$ for all $k \geqslant 1$. Hence from the semantics of conjunction and our choice of path $\mathcal{M}, \pi'_{\geqslant i} \models \neg viol$ for all $i \geqslant 0$. From the definition of the RoCTL structure M, $M, \pi'_{\geqslant i} \models \neg viol$ for all $i \geqslant 0$ and $(\pi'_i, \pi'_{i+1}) \in \xrightarrow{s}$. Further as $\mathcal{M}, \pi'_{\geqslant 0} \models \neg viol$, $\pi_1 = \pi'_0$ and $(\pi_0, \pi_1) \in R$ in the CTL model we have $(\pi_0, \pi_1) \in \xrightarrow{s}$ in the RoCTL model and the path $\langle \pi_0 : \pi'\rangle$ is failure free. Recall for some j we have $\mathcal{M}, \pi'_{\geqslant j} \models l$ so $M, \pi'_{\geqslant j} \models l$ and as $\sigma_0 = \pi_0$ and $\langle \pi_0 : \pi'\rangle \in S(\sigma_0)$ from the semantics of $\mathbf{P}$ and $\Diamond$ $M, \sigma \models \mathbf{P}\Diamond l$ as required.
- $\varphi = \mathbf{P}l_1\,\mathcal{U}\,l_2$. Assume that $\tau(\mathbf{P}l_1\,\mathcal{U}\,l_2)$ is satisfiable on some path σ in a CTL model structure $\mathcal{M} = \langle S, R, L\rangle$, i.e. $\mathcal{M}, \sigma \models l_2 \vee (l_1 \wedge \mathbf{E}\bigcirc\mathbf{E}((\neg viol \wedge l_1)\,\mathcal{U}\,(\neg viol \wedge l_2)))$. We show $M, \sigma \models \mathbf{P}1_1\,\mathcal{U}\,l_2$ where $M = CONS(\mathcal{M})$. In $\mathcal{M}$ from the semantics of disjunction either $\mathcal{M}, \sigma \models l_2$ or $\mathcal{M}, \sigma \models (l_1 \wedge$

$\mathbf{E}\bigcirc\mathbf{E}((\neg viol \wedge l_1)\,\mathcal{U}\,(\neg viol \wedge l_2)))$. For the former $\mathcal{M}, \sigma \models l_2$ and additionally from the structure of the CTL models (see above) we can choose some π such that $\sigma_0 = \pi_0$ so $\mathcal{M}, \pi \models l_2$ and $\mathcal{M}, \pi_{\geqslant i} \models \neg viol$ for all $i \geqslant 1$. From the definition of the RoCTL structure M, $M, \pi \models l_2$ and $(\pi_i, \pi_{i+1}) \in \xrightarrow{s}$ for all $i \geqslant 0$ so $\pi \in S(\sigma_0)$ and from the semantics of $\mathbf{P}$ and $\mathcal{U}$, $M, \sigma \models \mathbf{P} l_1 \,\mathcal{U}\, l_2$ as required. Next consider the latter, i.e. $\mathcal{M}, \sigma \models (l_1 \wedge \mathbf{E}\bigcirc\mathbf{E}((\neg viol \wedge l_1)\,\mathcal{U}\,(\neg viol \wedge l_2)))$. In $\mathcal{M}$ from the semantics of conjunction $\mathcal{M}, \sigma \models l_1$ and $\mathcal{M}, \sigma \models \mathbf{E}\bigcirc\mathbf{E}((\neg viol \wedge l_1)\,\mathcal{U}\,(\neg viol \wedge l_2))$. In $\mathcal{M}$ from the semantics of $\mathbf{E}$ and $\bigcirc$ there is a path $\pi \in SF(\sigma_0)$ such that $\sigma_0 = \pi_0$ and $(\pi_0, \pi_1) \in R$ and $\mathcal{M}, \pi_{\geqslant 1} \models \mathbf{E}((\neg viol \wedge l_1)\,\mathcal{U}\,(\neg viol \wedge l_2))$. From the semantics of $\mathbf{E}$ and $\mathcal{U}$ there is a path $\pi' \in SF(\pi_1)$ such that $\pi_1 = \pi'_0$ and for some j, $\mathcal{M}, \pi'_{\geqslant j} \models (\neg viol \wedge l_2)$ and for all $0 \leqslant i < j$, $\mathcal{M}, \pi'_{\geqslant i} \models \neg viol \wedge l_1$. Additionally from the structure of the CTL models (see above) we can choose π' such that $\mathcal{M}, \pi_{\geqslant j+k} \models \neg viol$ for all $k \geqslant 1$. Hence from the semantics of conjunction and our choice of path $\mathcal{M}, \pi'_{\geqslant i} \models \neg viol$ for all $i \geqslant 0$. From the definition of the RoCTL structure M, for all $i \geqslant 0$, $(\pi'_i, \pi'_{i+1}) \in \xrightarrow{s}$. Further as $\mathcal{M}, \pi'_{\geqslant 0} \models \neg viol$, $\pi_1 = \pi'_0$ and $(\pi_0, \pi_1) \in R$ in the CTL model we have $(\pi_0, \pi_1) \in \xrightarrow{s}$ in the RoCTL model and the path $\langle \pi_0 : \pi' \rangle$ is failure free. Recall for some j we have $\mathcal{M}, \pi'_{\geqslant j} \models l_2$ so $M, \pi'_{\geqslant j} \models l_2$ and for all $0 \leqslant i < j$, $\mathcal{M}, \pi'_{\geqslant i} \models l_1$ so $M, \pi'_{\geqslant i} \models l_1$. Also $M, \sigma \models l_1$ and as $\sigma_0 = \pi_0$ then $M, \pi \models l_1$. As $\sigma_0 = \pi_0$, the path $\langle \pi_0 : \pi' \rangle \in S(\sigma_0)$ so from the semantics of $\mathbf{P}$ and $\mathcal{U}$, $M, \sigma \models \mathbf{P} l_1 \,\mathcal{U}\, l_2$ as required.
- $\varphi = \mathbf{P} l_1 \,\mathcal{W}\, l_2$. This is similar to the case for $\mathbf{P} l_1 \,\mathcal{U}\, l_2$.
- $\varphi = \mathbf{O}\bigcirc l$. Assume that $\tau(\mathbf{O}\bigcirc l)$ is satisfiable on path σ in a CTL model structure $\mathcal{M} = \langle S, R, L \rangle$, i.e. $\mathcal{M}, \sigma \models \mathbf{A}\bigcirc(viol \vee l)$. We show $M, \sigma \models \mathbf{O}\bigcirc l$ where $M = CONS(\mathcal{M})$. In $\mathcal{M}$ from the semantics of $\mathbf{A}$ and $\bigcirc$ for all paths $\pi \in SF(\sigma_0)$ such that $\sigma_0 = \pi_0$ and $(\pi_0, \pi_1) \in R$, $\mathcal{M}, \pi_{\geqslant 1} \models (viol \vee l)$. Additionally from the structure of the CTL models (see above) we can choose a π' such that $\pi_1 = \pi'_0$ and $\mathcal{M}, \pi_{\geqslant i} \models \neg viol$ for all $i \geqslant 1$. From the semantics of disjunction either $\mathcal{M}, \pi_{\geqslant 1} \models viol$ or $\mathcal{M}, \pi_{\geqslant 1} \models l$. Thus for any path π if $\mathcal{M}, \pi_{\geqslant 1} \models \neg viol$ then $\mathcal{M}, \pi_{\geqslant 1} \models l$. From the definition of the RoCTL structure M if $\mathcal{M}, \pi_{\geqslant 1} \models \neg viol$ then $(\pi_0, \pi_1) \in \xrightarrow{s}$ and $M, \pi_{\geqslant 1} \models l$. Also we can find some π' such that $\pi_1 = \pi'_0$ and $\mathcal{M}, \pi'_{\geqslant i} \models \neg viol$ for $i \geqslant 1$. Hence in M then $(\pi_i, \pi_{i+1}) \in \xrightarrow{s}$ for $i \geqslant 0$ and for path $\langle \pi_0 : \pi' \rangle$ such that if $\mathcal{M}, \pi \models \neg viol$ and π' is as previously defined $\langle \pi_0 : \pi' \rangle \in S(\sigma_0)$ and from the semantics of $\mathbf{O}$ and $\bigcirc$ $M, \sigma \models \mathbf{O}\bigcirc l$ as required.

The other cases for obligatory paired with different temporal operators are similar to the above cases.

Next we show if φ is satisfiable on path σ in an RoCTL model $M = \langle A, \xrightarrow{s}, \xrightarrow{f}, \alpha \rangle$ then $\tau(\varphi \wedge \mathbf{A}\,\Box\mathbf{A}\bigcirc\neg viol)$ is satisfiable in a CTL model. We construct CTL model $\mathcal{M}$ from M show it satisfies $\tau(\varphi \wedge \mathbf{A}\,\Box\mathbf{A}\bigcirc\neg viol)$. We define $\mathcal{M}$ in terms of a function $CONS2$ such that $CONS2(M) = \mathcal{M} = \langle S, R, L \rangle$ where

- $S = A$
- $R = \xrightarrow{s} \cup \xrightarrow{f}$
- $L(w_i) = \alpha(w_i) \cup viol$ iff $(w_i, w_{i+1}) \in \xrightarrow{f}$
- $L(w_i) = \alpha(w_i)$ iff $(w_i, w_{i+1}) \in \xrightarrow{s}$
- $L(w_0) = \alpha(w_i)$ iff there is no w_i such that $(w_i, w_0) \in \xrightarrow{s} \cup \xrightarrow{f}$

As $M, \sigma \models \varphi$, let $CONS2(M) = \mathcal{M}$ and we show $M, \sigma \models \tau(\varphi \wedge \mathbf{A}\,\Box\mathbf{A}\bigcirc\neg viol)$. By the definition of τ we must show $M, \sigma \models \tau(\varphi)$ and $M, \sigma \models \mathbf{A}\,\Box\mathbf{A}\bigcirc\neg viol$. Regarding the latter as $\xrightarrow{s}$ is serial in any RoCTL model M we must have that for any state w_i there is some w_{i+1} such that $(w_i, w_{i+1}) \in \xrightarrow{s}$. Thus by the definition of CONS2 for any fullpath π, $\mathcal{M}, \pi_{\geqslant 1} \models \neg viol$ and $\mathcal{M}, \pi \models \mathbf{E}\bigcirc\neg viol$. As π could be any path then $\mathcal{M}, \sigma \models \mathbf{A}\,\Box\mathbf{E}\bigcirc\neg viol$ as required. Next we show $M, \sigma \models \tau(\varphi)$ by considering the different cases of φ.

- $\varphi = \mathbf{P}\bigcirc l$. Assume that $\mathbf{P}\bigcirc l$ is satisfiable on path σ in an RoCTL model structure $M = \langle A, \xrightarrow{s}, \xrightarrow{f}, \alpha \rangle$, i.e. $M, \sigma \models \mathbf{P}\bigcirc l$. We show $\mathcal{M}, \sigma \models \tau(\mathbf{P}\bigcirc l)$, i.e. $\mathcal{M}, \sigma \models \mathbf{E}\bigcirc(\neg viol \wedge l)$ where $\mathcal{M} = CONS2(M)$. From the semantics of $\mathbf{P}$ and $\bigcirc$ there must be a path π such that $\pi \in S(\sigma_0)$ and $M, \pi_{\geqslant 1} \models l$. As $\pi \in S(\sigma_0)$ then we have then $(\pi_i, \pi_{i+1}) \in \xrightarrow{s}$ for all $i \geqslant 0$ and from the definition of the CTL structure $\mathcal{M}$, $\mathcal{M}, \pi_{\geqslant i} \models \neg viol$ for $i \geqslant 1$. Also $\mathcal{M}, \pi_{\geqslant 1} \models l$ and from the semantics of conjunction $\mathcal{M}, \pi_{\geqslant 1} \models \neg viol \wedge l$. From the definition of $\mathcal{M}$ and as path $\pi \in S(\sigma_0)$ we have $\pi \in SF(\sigma_0)$ so $\mathcal{M}, \sigma \models \mathbf{E}\bigcirc(\neg viol \wedge l)$.
- $\varphi = \mathbf{P}\,\Box l$. Assume that $\mathbf{P}\,\Box l$ is satisfiable on path σ in an RoCTL model structure $M = \langle A, \xrightarrow{s}, \xrightarrow{f}, \alpha \rangle$, i.e. $M, \sigma \models \mathbf{P}\,\Box l$. We show $\mathcal{M}, \sigma \models \tau(\mathbf{P}\,\Box l)$, i.e. $\mathcal{M}, \sigma \models l \wedge \mathbf{E}\bigcirc\mathbf{E}\,\Box(\neg viol \wedge l)$ where

$\mathcal{M} = CONS2(M)$. From the semantics of $\mathbf{P}$ and $\Box$ there must be a path π such that $\pi \in S(\sigma_0)$ and $M, \pi_{\geqslant i} \models l$ for $i \geqslant 0$. As $\pi \in S(\sigma_0)$ then we have then $(\pi_i, \pi_{i+1}) \in \xrightarrow{s}$ for all $i \geqslant 0$ and from the definition of the CTL structure $\mathcal{M}$, $\mathcal{M}, \pi_{\geqslant i} \models \neg viol$ for $i \geqslant 1$. Also as $M, \pi_{\geqslant i} \models l$ for $i \geqslant 0$ and from the definition of the CTL structure $\mathcal{M}$, $\mathcal{M}, \pi_{\geqslant i} \models l$ for $i \geqslant 0$. In particular, $\mathcal{M}, \pi_{\geqslant 0} \models l$ and $\mathcal{M}, \pi_{\geqslant i} \models l$ for $i \geqslant 1$. From the semantics of conjunction $\mathcal{M}, \pi_{\geqslant i} \models \neg viol \wedge l$ for $i \geqslant 1$. Thus from the semantics of $\mathbf{E}$ and $\Box$, $\mathcal{M}, \pi_{\geqslant 1} \models \mathbf{E}\Box \neg viol \wedge l$. From the semantics of $\mathbf{E}$ and $\bigcirc$ $\mathcal{M}, \pi \models \mathbf{E}\bigcirc\mathbf{E}\Box\neg viol \wedge l$ and as $\pi \in S(\sigma_0)$ then $\pi \in SF(\sigma_0)$ and $\mathcal{M}, \sigma \models \mathbf{E}\bigcirc\mathbf{E}\Box\neg viol \wedge l$. Further as $\mathcal{M}, \pi \models l$ and $\pi_0 = \sigma_0$ then $\mathcal{M}, \sigma \models l$. From the semantics of conjunction $\mathcal{M}, \sigma \models l \wedge \mathbf{E}\bigcirc\mathbf{E}\Box\neg viol$ as required.

- $\varphi = \mathbf{P}\Diamond l$. Assume that $\mathbf{P}\Diamond l$ is satisfiable on path σ in an RoCTL model structure $M = \langle A, \xrightarrow{s}, \xrightarrow{f}, \alpha\rangle$, i.e. $M, \sigma \models \mathbf{P}\Diamond l$. We show $\mathcal{M}, \sigma \models \tau(\mathbf{P}\Diamond l)$, i.e. $\mathcal{M}, \sigma \models l \vee \mathbf{E}\bigcirc\mathbf{E}(\neg viol\,\mathcal{U}\,(\neg viol \wedge l))$ where $\mathcal{M} = CONS2(M)$. From the semantics of $\mathbf{P}$ and $\Diamond$ there must be a path π such that $\pi \in S(\sigma_0)$ and there exists some $j \geqslant 0$ such that $M, \pi_{\geqslant j} \models l$. As $\pi \in S(\sigma_0)$ then $(\pi_i, \pi_{i+1}) \in \xrightarrow{s}$ for all $i \geqslant 0$ and from the definition of the CTL structure $\mathcal{M}$, $\mathcal{M}, \pi_{\geqslant i} \models \neg viol$ for $i \geqslant 1$. First assume that $j = 0$, i.e. $M, \pi \models l$ and as $\pi_0 = \sigma_0$ and l is a literal then $M, \sigma \models l$. From the definition of the CTL structure $\mathcal{M}$, $\mathcal{M}, \sigma \models l$. Next assume that $j \geqslant 1$, i.e. there exists some $j \geqslant 1$ such that $M, \pi_{\geqslant j} \models l$. From the definition of the CTL structure $\mathcal{M}$, there exists some $j \geqslant 1$ such that $\mathcal{M}, \pi_{\geqslant j} \models l$. As we have shown that $\mathcal{M}, \pi_{\geqslant i} \models \neg viol$ for $i \geqslant 1$ from the semantics of conjunction there exists some $j \geqslant 1$ such that $\mathcal{M}, \pi_{\geqslant j} \models \neg viol \wedge l$ and $\mathcal{M}, \pi_{\geqslant i} \models \neg viol$ for $1 \leqslant i < j$. From the semantics of $\mathbf{E}$ and $\mathcal{U}$, $\mathcal{M}, \pi_{\geqslant 1} \models \mathbf{E}\neg viol\,\mathcal{U}\,(\neg viol \wedge l)$. From the semantics of $\mathbf{E}$ and $\bigcirc$ $\mathcal{M}, \pi \models \mathbf{E}\bigcirc\mathbf{E}(\neg viol\,\mathcal{U}\,(\neg viol \wedge l))$. As $\pi \in S(\sigma_0)$ then $\pi \in SF(\sigma_0)$ and $\mathcal{M}, \sigma \models \mathbf{E}\bigcirc\mathbf{E}(\neg viol\,\mathcal{U}\,(\neg viol \wedge l))$. We have examined the two possible cases either $\mathcal{M}, \sigma \models l$ or $\mathcal{M}, \sigma \models \mathbf{E}\bigcirc\mathbf{E}\neg viol\,\mathcal{U}\,(\neg viol \wedge l)$ and by the semantics of disjunction $\mathcal{M}, \sigma \models l \vee \mathbf{E}\bigcirc\mathbf{E}(\neg viol\,\mathcal{U}\,(\neg viol \wedge l))$ as required.
- $\varphi = \mathbf{P}l_1\,\mathcal{U}\,l_2$. Assume that $\mathbf{P}l_1\,\mathcal{U}\,l_2$ is satisfiable on path σ in an RoCTL model structure $M = \langle A, \xrightarrow{s}, \xrightarrow{f}, \alpha\rangle$, i.e. $M, \sigma \models \mathbf{P}l_1\,\mathcal{U}\,l_2$. We show $\mathcal{M}, \sigma \models \tau(\mathbf{P}l_1\,\mathcal{U}\,l_2)$, i.e. $\mathcal{M}, \sigma \models l_2 \vee (l_1 \wedge \mathbf{E}\bigcirc\mathbf{E}((\neg viol \wedge l_1)\,\mathcal{U}\,(\neg viol \wedge l_2)))$ where $\mathcal{M} = CONS2(M)$. From the semantics of $\mathbf{P}$ and $\mathcal{U}$ there must be a path π such that $\pi \in S(\sigma_0)$ and there exists some $j \geqslant 0$ such that $M, \pi_{\geqslant j} \models l_2$ and $M, \pi_{\geqslant i} \models l_1$ for $0 \leqslant i < j$. As $\pi \in S(\sigma_0)$ then $(\pi_i, \pi_{i+1}) \in \xrightarrow{s}$ for all $i \geqslant 0$ and from the definition of the CTL structure $\mathcal{M}$, $\mathcal{M}, \pi_{\geqslant i} \models \neg viol$ for $i \geqslant 1$. First assume that $j = 0$, i.e. $M, \pi \models l_2$ and as $\pi_0 = \sigma_0$ and l_2 is a literal then $M, \sigma \models l_2$. From the definition of the CTL structure $\mathcal{M}$, $\mathcal{M}, \sigma \models l_2$. Next assume that $j \geqslant 1$, i.e. there exists some $j \geqslant 1$ such that $M, \pi_{\geqslant j} \models l_2$ and $M, \pi_{\geqslant i} \models l_1$ for $0 \leqslant i < j$. From the definition of the CTL structure $\mathcal{M}$, there exists some $j \geqslant 1$ such that $\mathcal{M}, \pi_{\geqslant j} \models l_2$ and $\mathcal{M}, \pi_{\geqslant i} \models l_1$ for $0 \leqslant i < j$. As we have shown that $\mathcal{M}, \pi_{\geqslant i} \models \neg viol$ for $i \geqslant 1$ from the semantics of conjunction there exists some $j \geqslant 1$, $\mathcal{M}, \pi_{\geqslant j} \models \neg viol \wedge l_2$ and $\mathcal{M}, \pi_{\geqslant i} \models \neg viol \wedge l_1$ for $1 \leqslant i < j$. From the semantics of $\mathbf{E}$ and $\mathcal{U}$, $\mathcal{M}, \pi_{\geqslant 1} \models \mathbf{E}(\neg viol \wedge l_1)\,\mathcal{U}\,(\neg viol \wedge l_2)$. From the semantics of $\mathbf{E}$ and $\bigcirc$, $\mathcal{M}, \pi \models \mathbf{E}\bigcirc\mathbf{E}((\neg viol \wedge l_1)\,\mathcal{U}\,(\neg viol \wedge l_2))$. As $\pi \in S(\sigma_0)$ then $\pi \in SF(\sigma_0)$ and $\mathcal{M}, \sigma \models \mathbf{E}\bigcirc\mathbf{E}((\neg viol \wedge l_1)\,\mathcal{U}\,(\neg viol \wedge l_2))$. We have examined the two possible cases either $\mathcal{M}, \sigma \models l_2$ or $\mathcal{M}, \sigma \models \mathbf{E}\bigcirc\mathbf{E}(\neg viol \wedge l_1)\,\mathcal{U}\,(\neg viol \wedge l_2)$ and by the semantics of disjunction $\mathcal{M}, \sigma \models l_2 \vee \mathbf{E}\bigcirc\mathbf{E}((\neg viol \wedge l_1)\,\mathcal{U}\,(\neg viol \wedge l_2))$ as required.
- $\varphi = \mathbf{P}l_1\,\mathcal{W}\,l_2$. This is similar to the case for $\mathbf{P}l_1\,\mathcal{U}\,l_2$.
- $\varphi = \mathbf{O}\bigcirc l$.

  Assume that $\mathbf{O}\bigcirc l$ is satisfiable on path σ in an RoCTL model structure $M = \langle A, \xrightarrow{s}, \xrightarrow{f}, \alpha\rangle$, i.e. $M, \sigma \models \mathbf{O}\bigcirc l$. We show $\mathcal{M}, \sigma \models \tau(\mathbf{O}\bigcirc l)$, i.e. $\mathcal{M}, \sigma \models \mathbf{A}\bigcirc(viol \vee l)$ where $\mathcal{M} = CONS2(M)$. From the semantics of $\mathbf{O}$ and $\bigcirc$ for all paths π such that $\pi \in S(\sigma_0)$ then $M, \pi_{\geqslant 1} \models l$. As $\pi \in S(\sigma_0)$ then we have then $(\pi_i, \pi_{i+1}) \in \xrightarrow{s}$ for all $i \geqslant 0$ and from the definition of the CTL structure $\mathcal{M}$, $\mathcal{M}, \pi_{\geqslant i} \models \neg viol$ for $i \geqslant 1$. For any $\pi' \in SF(\sigma_0)$ such that $(\pi'_0, \pi'_1) \in \xrightarrow{f}$ from the definition of the CTL structure $\mathcal{M}$, $\mathcal{M}, \pi'_{\geqslant 1} \models viol$. Thus for all paths $\pi \in SF(\sigma_0)$ either $(\pi_0, \pi_1) \in \xrightarrow{s}$ and $M, \pi_{\geqslant 1} \models l$ or $(\pi_0, \pi_1) \in \xrightarrow{f}$ and $M, \pi_{\geqslant 1} \models viol$. From the definition of the CTL structure $\mathcal{M}$, for all paths $\pi \in SF(\sigma_0)$ either $\mathcal{M}, \pi_{\geqslant 1} \models \neg viol$ and $\mathcal{M}, \pi_{\geqslant 1} \models l$ or $\mathcal{M}, \pi_{\geqslant 1} \models viol$. From the semantics of disjunction for all paths $\pi \in SF(\sigma_0)$ $\mathcal{M}, \pi_{\geqslant 1} \models viol \vee l$ and from the semantics of $\mathbf{A}$ and $\bigcirc$, $\mathcal{M}, \sigma \models \mathbf{A}\bigcirc(viol \vee l)$.

The other cases for obligatory paired with different temporal operators are similar to the above cases.

Theorem 1. *Let φ be a RoCTL$^-$ formula and $TRAN(\varphi)$ be the translation of φ into CTL. φ is satisfiable if and only if $TRAN(\varphi)$ is satisfiable.*

Proof. Let $TRAN(\varphi) = \tau(\varphi' \wedge \mathbf{A}\,\square\mathbf{A}\bigcirc\neg viol)$ where φ' is the translation of φ into negation normal form and then into flat normal form. From Lemma 1 and 2 we can translate any RoCTL$^-$ formula φ into φ' into negation normal form and then flat normal form such that φ is satisfiable if and only if φ' is satisfiable. Finally in Lemma 3 we show that for some φ' in flat normal φ' is satisfiable if and only if $\tau(\varphi' \wedge \mathbf{A}\,\square\mathbf{A}\bigcirc\neg viol)$ is satisfiable.

10 Complexity

We consider the increase in size of a formula in the translation from RoCTL$^-$ formulae to CTL.

First we define the length "len" of a formula φ as follows.

$$\begin{array}{llll}
\mathsf{len}(\mathbf{H}\bigcirc\varphi) & = \mathsf{len}(\mathbf{H}\,\square\varphi) & = \mathsf{len}(\mathbf{H}\Diamond\varphi) & = 1 + \mathsf{len}(\varphi) \\
\mathsf{len}(\mathbf{H}\varphi\,\mathcal{U}\,\psi) & = \mathsf{len}(\mathbf{H}\varphi\,\mathcal{W}\,\psi) & = 1 + \mathsf{len}(\varphi) + \mathsf{len}(\psi) & \\
\mathsf{len}(\varphi \wedge \psi) & = 1 + \mathsf{len}(\varphi) + \mathsf{len}(\psi) & & \\
\mathsf{len}(\varphi \vee \psi) & = 1 + \mathsf{len}(\varphi') + \mathsf{len}(\psi') & & \\
\mathsf{len}(\varphi \Rightarrow \psi) & = 1 + \mathsf{len}(\varphi') + \mathsf{len}(\psi') & & \\
\mathsf{len}(\neg\varphi) & = 1 + \mathsf{len}(\varphi) & & \\
\mathsf{len}(p) & = \mathsf{len}(\mathbf{true}) & = \mathsf{len}(\mathbf{false}) & = 1
\end{array}$$

where $\mathbf{H} \in \{\mathbf{A}, \mathbf{E}, \mathbf{O}, \mathbf{P}\}$, and p is a proposition.

We assume that φ is is negated normal form.

Lemma 4. *Let φ be an RoCTL$^-$ formula in negated normal form and φ' be its translation into flat normal form via steps 1 and 2 of the algorithm. The length of φ' is at most $7 \times \mathsf{len}(\varphi) + 1$, i.e. $len(\varphi') \leqslant 7 \times \mathsf{len}(\varphi) + 1$*

Proof. Consider the replacement of any subformula ψ in φ by the new proposition t, i.e. φ is rewritten as φ' which is φ with ψ replaced by t and $\varphi'_R = \varphi_R \wedge \mathbf{A}\,\square(t \Rightarrow \psi)$. We have $\mathsf{len}(\varphi') = \mathsf{len}(\varphi) - \mathsf{len}(\psi) + \mathsf{len}(t)$ and $\mathsf{len}(\varphi'_R) = \mathsf{len}(\varphi_R) + 1 + \mathsf{len}(\mathbf{A}\,\square(t \Rightarrow \psi)) = \mathsf{len}(\varphi_R) + 1 + 3 + \mathsf{len}(\psi)$ and so $\mathsf{len}(\varphi' \wedge \varphi'_R) = \mathsf{len}(\varphi) - \mathsf{len}(\psi) + 1 + \mathsf{len}(\varphi_R) + 1 + 3 + \mathsf{len}(\psi) + 1 = len(\varphi) + \mathsf{len}(\varphi_R) + 6$. There are at most $\mathsf{len}(\varphi)$ subformulae we could replace hence we obtain a maximum length of $7 \times \mathsf{len}(\varphi) + 1$.

Lemma 5. *Let φ be an RoCTL$^-$ formula in flat normal form. The length of its translation into CTL, $\tau(\varphi)$, is at most $14 \times \mathsf{len}(\varphi)$, i.e. $len(\tau(\varphi)) \leqslant 14 \times \mathsf{len}(\varphi)$*

Proof. Only subformulae of the form $\mathbf{HT}l_1$ or $\mathbf{H}l_1\mathbf{T}l_2$ where $\mathbf{H}$ is $\mathbf{P}$ or $\mathbf{O}$ and $\mathbf{T}$ is a temporal operator will increase the length of $\tau(\varphi)$. By inspection the translations that increase the length the most are for $\tau(\mathbf{P}l_1\,\mathcal{U}\,l_2)$ and $\tau(\mathbf{P}l_1\,\mathcal{W}\,l_2)$ where $\mathsf{len}(\tau(\mathbf{P}l_1\,\mathcal{U}\,l_2) = \mathsf{len}(\tau(\mathbf{P}l_1\,\mathcal{U}\,l_2)) = 14$. As there are at most $\mathsf{len}(\varphi)$ formulae of this form the $len(\tau(\varphi)) \leqslant 14 \times \mathsf{len}(\varphi)$.

Lemma 4 and 5 together show that the complexity of the translation results in a linear increase in length of the formula.

Theorem 2. *The complexity of satisfiability of RoCTL$^-$ formulae is EXPTIME.*

Proof. Lemma 4, Lemma 5 and Theorem 1 show a satisfiability preserving translation into CTL which increases the length of the formula linearly. As the complexity of satisfiability of CTL is known to be EXPTIME [8] then the complexity of satisfiability of RoCTL$^-$ formulae is EXPTIME.

11 Conclusions and Related Work

This paper has presented RoCTL$^-$, a CTL like restriction of RoCTL*, and its translation into CTL. Thus a resolution decision procedure based on this normal form can be applied to obtain a decision procedure for RoCTL$^-$. The translation has been shown to be satisfiability preserving. RoCTL$^-$ includes not only the usual path and temporal operators of CTL but also allows deontic operators quantifying over successful paths. Examples demonstrating the expressiveness of this logic have been presented.

Whilst we haven't considered full RoCTL* but a CTL-like restriction we have shown that useful systems and properties can still be expressed in the restricted logic. Similarly we note that CTL is still expressive enough for many real world uses (see e.g. [4]). A related branching time logic, PCTL [13], which uses probabilities to represent reliability, also does not extend to the full CTL* logic. PCTL has demonstrated its usefulness as part of the PRISM tool [14].

Although we can decide RoCTL* via QCTL*, it is important to find a more efficient decision procedure as QCTL* does not have an elementary decision procedure [17, 10]. Here we show that the translation from RoCTL$^-$ into CTL produces a linear increase in the length of the formula. Hence, the results in this paper provide a way to apply practical resolution based methods for CTL to RoCTL$^-$. Given the translation into CTL is linear and that the complexity of satisfiability of CTL is EXPTIME we can conclude that RoCTL$^-$ can be decided in EXPTIME. As with CTL*, RoCTL includes non-state formulae. This makes us believe that it is unlikely that we will be able to translate all of RoCTL into CTL.

As well as other approaches to deontic logics and robustness using temporal logics, for example [13, 3], related work includes resolution proof methods for CTL be found in [2, 18]. Tableaux based methods have also been developed for CTL see for example [8, 1] and for bundled CTL* [16].

Further work includes applying RoCTL to other examples and extending the translation to deal with a larger subset of RoCTL* if possible. Another avenue to explore is to apply the techniques developed in this paper to extend Reynolds tableau decision procedure for bundled CTL* (BCTL*) in [16] to handle obligation operators. We are also interested in developing resolution calculi for CTL*. We will also seek axiomatizations of RoCTL and RoCTL*.

References

1. P. Abate, R. Goré, and F. Widmann. One-Pass Tableaux for Computation Tree Logic. In *Logic for Programming, Artificial Intelligence, and Reasoning*, volume 4790 of *LNCS*, pages 32–46. Springer, 2007.
2. A. Bolotov. *Clausal Resolution for Branching-Time Temporal Logic*. PhD thesis, Dept. of Computing and Mathematics, Manchester Metropolitan University, 2000.
3. J. Broersen, F. Dignum, V. Dignum, and J.-J.Ch.Meyer. Designing a deontic logic of deadlines. In A. Lomuscio and D. Nute, editors, *DEON*, volume 3065 of *Lecture Notes in Computer Science*, pages 43–56. Springer, 2004.
4. S.D. Das. Formal verification of queue flow-control through model-checking, 1998. `http://www.freepatentsonline.com/EP0915426.html`.
5. E. Emerson and A. Sistla. Deciding Full Branching Time Logic. *Information and Control*, 61:175 – 201, 1984.
6. E. A. Emerson and E. M. Clarke. Using Branching Time Temporal Logic to Synthesize Synchronization Skeletons. *Science of Computer Programming*, 2(3):241–266, 1982.
7. E. A. Emerson and J. Y. Halpern. “Sometimes” and “Not Never” Revisited: On Branching Versus Linear Time. In *Proceedings of the 10th ACM Symposium on Principles of Programming Languages*, pages 127–140, 1983.
8. E. A. Emerson and J. Y. Halpern. Decision Procedures and Expressiveness in the Temporal Logic of Branching Time. *Journal of Computer and System Sciences*, 30(1):1–24, February 1985.
9. J.W. Forrester. Gentle murder, or the adverbial samaritan. *The Journal of Philosophy*, 81(4):193–7, April 1984.
10. T. French. *Bisimulation quantifiers for modal logics*. PhD thesis, School of Computer Science and Software Engineering, University of Western Australia, 2006.
11. T. French, J.C. M^{c}Cabe-Dansted, and M. Reynolds. Temporal Logic of Robustness. In B. Konev and F. Wolter, editors, *Proceedings of the 6th International Symposium of the Frontiers of Combining Systems*, volume 4720 of *Lecture Notes in Artificial Intelligence*, pages 193–205. Springer, 2007.
12. D. Gabbay, A. Pnueli, S. Shelah, and J. Stavi. The Temporal Analysis of Fairness. In *Proceedings of the Seventh ACM Symposium on the Principles of Programming Languages*, pages 163–173, Las Vegas, Nevada, January 1980.
13. H. Hansson and B. Jonsson. A logic for reasoning about time and reliability. *Formal Aspects of Computing*, 6(5):512–535, 1994.
14. M.Z. Kwiatkowska. Model checking for probability and time: from theory to practice. In *LICS*, pages 351–. IEEE Computer Society, 2003.
15. D. A. Plaisted and S. A. Greenbaum. A Structure-Preserving Clause Form Translation. *Journal of Symbolic Computation*, 2(3):293–304, September 1986.
16. M. Reynolds. A Tableau for Bundled CTL*. *J Logic Computation*, 17(1):117–132, 2007.
17. A. P. Sistla, M. Vardi, and P. Wolper. The Complementation Problem for Büchi Automata with Applications to Temporal Logic. *Theoretical Computer Science*, 49:217–237, 1987.
18. L. Zhang, U. Hustadt, and C. Dixon. A Refined Resolution Calculus for CTL. In *Automated Deduction—CADE-22*, LNAI, pages 245–260. Springer, 2009.