ISCAS-SKLCS-19-02 Aug. , 2019

中国科学院软件研究所
计算机科学国家重点实验室
技术报告

Weak Well Founded Sets and Their Application to Formal Verification

by

Wenhui Zhang

State key Laboratory of Computer Science
Institute of Software
Chinese Academy of Sciences
Beijing 100190. China

Weak Well Founded Sets and Their Application to Formal Verification

Wenhui Zhang
SKLCS, Institute of Software, Chinese Academy of Sciences, and
University of Chinese Academy of Sciences
zwh@ios.ac.cn

August, 2019

1 Introduction

Verification condition is an important notion in developing techniques for program verification. For sequential programs, the main correctness concerns are partial correctness and termination. Foundations for verification condition generation have been formulated in Floyd-Hoare logic [16, 20]. The essential point is to turn a program verification problem into the problem of checking the validity of first order formulas. Due to that the verification problem is not decidable for reasonably expressive underlying first order logics for program construction, in order to be able to do so, human efforts are usually needed, i.e., we have to provide intermediate assertions and ranking functions in order to be able to use the rules for verification condition generation. The use of verification condition implies a clear separation of concerns in program verification: a first order logic part and a verification condition generation part. Both parts may be assisted by semi-automated techniques, such as theorem proving techniques [7, 14], invariant generation techniques [3, 4], ranking function synthesis techniques [27, 1, 18].

For concurrent programs, the correctness issues usually concern temporal properties, and the approach for reasoning of partial correctness and termination can be adapted to reasoning of temporal properties. In [25, 26], Owicki and Gries have developed rules for proving partial correctness, deadlock freedom and termination of a kind of parallel programs. For reasoning of LTL properties in a systematic way, proof rules have been proposed by Manna and Pnueli in [28]. For reasoning of CTL properties, proof rules have been proposed by Fix and Grumberg in [15]. For reasoning of CTL* properties, a kind of compositional deductive approach has been considered in [34, 21, 17] by Pnueli, Kesten and Gabbay. From a practical point of view, some of the recent works have focused on automated verification of temporal properties [10, 5, 11], and in particular in [11], Cook et. al. have put the emphasis on automated verification of CTL* properties. Among the aforementioned approaches, there might be two kinds of problems, i.e., the use of the approach might lead to transforming a verification problem to a problem that is equally hard to solve, and the approach might not be complete with respect to the targeted types of properties. The reader is referred to Appendix A for further discussions on these issues.

One of the obstacles seems to be that although there are many approaches for verification and reasoning of temporal properties, there are few underlying principles for such reasoning, for instance, for reasoning of partial correctness and safety properties, we may use the usual inductive argument (based on natural induction, or induction on time points), and for reasoning of termination, eventuality and response properties, we may use inductive argument on well-founded sets, however, for reasonably complicated temporal properties, it lacks well-established simple principles for doing this kind of reasoning and first order verification condition generation. In this work, similar to the Floyd-Hoare logic style proofs [16, 20] and the various works on deductive verification of temporal properties of concurrent systems, e.g., [28, 19, 29, 32, 31], we study proof rules such that verification of temporal properties can be reduced to first order reasoning, under the assumption that the necessary auxiliary constructs can be provided.

Structure of the Paper The contents of the rest of the paper are as follows. To begin with, we have a preliminary discussion on order sets and directed graphs, and develop the necessary background and induction principle for further reasoning of program models. Then we present the program model and the necessary background for further reasoning of temporal properties. After this, we study rules for proving LTL properties. Many rules are similar to those in [28, 29]. The set of rules is then identified to be relatively complete for a subset of LTL properties. For this subset of LTL properties, proof rules for negative satisfiability (essentially, this is the same as applying the existential interpretation to the negated LTL formula) are also developed, providing a way for proving the non-validity of such LTL properties. A combination of the proof rules for satisfiability and negative satisfiability of LTL properties naturally leads to a set of proof rules for CTL*, though, this combination is only sound and relatively complete for a subset of CTL*. Then a customized set of proof rules for a sublogic of CTL*, denoted CTL†, is provided. The sublogic is sufficiently expressive that it covers the properties considered in Appendix A and those of the interesting CTL* formulas in Section 8.2 of [11]. An example demonstrating the verification condition generation process with a supporting experimental tool is also presented.

2 Ordered Sets and Directed Graphs

Let $(S, \sqsubseteq)$ be a preorder, i.e., the relation $\sqsubseteq$ is reflexive and transitive. An infinite descending chain is an infinite sequence $\pi = \pi_0\pi_1\pi_2\cdots$ such that $\pi_i \sqsupset \pi_{i+1}$ for all $i \geq 0$. A finite descending chain of length $n+1$ is a finite sequence $\pi = \pi_0\pi_1\cdots\pi_n$ such that $\pi_i \sqsupset \pi_{i+1}$ for all $i \leq n-1$. Notice that since the chains are based on preorders, an element may appear many times or infinitely many times in a chain.

For convenience, we use π_0 to denote the first element of π (being a sequence of elements of any type), π_i to denote the $(i+1)$-element of π, and π^i to denote the sub-sequence starting from π_i. We use $\pi(a)$ to denote that π is starting from

a, i.e., $\pi_0 = a$. Then $\exists\pi(a)$ means that there exists a sequence π starting from a.

Let $Z \subseteq S$. An infinite descending Z-chain is an infinite descending chain such that every element in the chain is in Z. The set of infinite descending Z-chains is denoted $\Delta(Z)$.

Definition 1. *Let S be a set and $Z \subseteq S$. A preorder $(S, \sqsubseteq)$ is called a weak well-founded set upon Z (or Z-well-founded set, for short), if $a \sqsubseteq b \sqsubseteq a$ implies $a = b$ or $a, b \in Z$, and for every non-empty subset A of S, either A has a minimal element or $A \cap Z \neq \emptyset$.*

For simplicity, we use WWF(Z) to denote the set of Z-well-founded sets. It is easily seen that a preorder $(S, \sqsubseteq)$ is a well-founded set iff it is $\emptyset$-well-founded, and furthermore, the following holds: $(S, \sqsubseteq)$ is Z-well-founded iff for every infinite descending chain π, elements not in Z (referred to as non-Z elements in the sequel) only appear finitely many times on π.

Lemma 1 (Induction). *Let $(S, \sqsubseteq) \in$ WWF(Z). Let φ be a predicate on S. The following holds.*

$$\textit{If } \forall a \in S.(\forall b \sqsubset a.(\varphi(b) \vee \exists\pi(b) \in \Delta(Z)) \rightarrow \varphi(a)), \textit{ then } \forall a \in S.\varphi(a).$$

Proof. Suppose that $\forall a \in S.(\forall b \sqsubset a.(\varphi(b) \vee \exists\pi(b) \in \Delta(Z)) \rightarrow \varphi(a))$ holds and there is an $a \in S$ such that $\varphi(a)$ does not hold, we prove that there is a contradiction. Since $\varphi(a)$ does not hold, $\forall b \sqsubset a.(\varphi(b) \vee \exists\pi(b) \in \Delta(Z))$ does not hold. Then there is an $a' \sqsubset a$ such that a' does not satisfy φ and there are no infinite descending Z-chains starting from a'. Since $\varphi(a')$ does not hold, we can use the same argument and obtain an $a'' \sqsubset a'$ such that a'' does not satisfy φ and there are no infinite descending Z-chains starting from a''. By using the same argument repeatedly, we can construct an infinite descending chain π starting from a such that for every i, there are no infinite descending Z-chains starting from π_i. This implies that non-Z elements must appear infinitely many times on π, contradicting to that $(S, \sqsubseteq)$ is in WWF(Z). $\square$

Directed Graphs Let $G = (V, E)$ be a directed graph (possibly with infinitely many vertices). For convenience, we use $s \rightarrow s'$ to denote $(s, s') \in E$, and use $\xrightarrow{*}$ to denote the reflexive and transitive closure of $\rightarrow$. An infinite path is an infinite sequence $\pi = \pi_0\pi_1\pi_2\cdots$ such that $\pi_i \rightarrow \pi_{i+1}$ for all $i \geq 0$. A finite path is a finite prefix of an infinite path. An infinite path starting from s is called an s-path.

For $A \subseteq V$, we use $Gr(A)$ to denote the induced subgraph (A, E') where $E' = E \cap (A \times A)$. We use $succ(A)$ to denote $\{s' \mid s \rightarrow s', s \in A\}$, the set of successors of A. Suppose that $f : A \rightarrow B$ is a mapping from A to B. For $X \subseteq A$, we use $f(X)$ to denote $\{f(x) \mid x \in X\}$, the image of X under the mapping.

Definition 2. *Let (V, E) be a directed graph. $po(V, E)$ denotes the preorder $(S, \sqsubseteq)$ with $S = V$ and $\sqsubseteq$ defined by $s \sqsubseteq s'$ iff $s = s'$ or there is a finite path $s_0 \cdots s_k$ with $k \geq 1$ such that $s_0 = s$ and $s_k = s'$.*

It is easily seen that $po(V, E)$ is indeed a preorder.

Lemma 2. *Let (V, E) be a directed graph and $N_0, N_1, N_2 \in V$ such that $N_2 \subseteq N_0$, $N_1 \cap N_0 = \emptyset$, $succ(N_0) \subseteq N_0 \cup N_1$ and $Gr(N_0)$ is self-loop free. Let $(W, \sqsubseteq) = po(Gr(N_0))$. Suppose that $(W, \sqsubseteq)$ is N_2-well-founded. Let $\varphi(s)$ denote the following property.*

> *For every s-path π, there is a $k \geq 1$ such that $\pi_0, ..., \pi_{k-1} \in N_0$ and $\pi_k \in N_1$, or for all $i \geq 0$ we have $\pi_i \in N_0$ and there is an $l \geq 0$ such that $\pi_j \in N_2$ for all $j \geq l$.*

Then $\forall s \in N_0 . \varphi(s)$.

Proof. The property φ ensures that for all $a \in N_0$ we have the following.

$$\forall b \sqsubset a.(\varphi(b) \vee \exists \pi(b) \in \Delta(N_2)) \to \varphi(a).$$

This is argued as follows. If a is a minimal element of N_0, an a-path must start with aa' with a' in N_1, since $Gr(N_0)$ is self-loop free. Therefore we have $\varphi(a)$. Otherwise, a is not a minimal element. It is easily seen that if b satisfies φ, then every path that passes b (with all of the vertices up to b in N_0) satisfies the necessary path-requirement. If $\forall b \sqsubset a.(\varphi(b) \vee \exists \pi(b) \in \Delta(N_2))$ holds, then every path that passes some elements not in N_2 satisfies the necessary path-requirement (for this part, such a path has an initial sequence in N_0 and either this sequence is followed by an N_1 element, or an $N_0 \setminus N_2$ element b such that $\varphi(b)$ holds, since we have $b \sqsubset a$ and there are no infinite descending N_2-chains starting from b), and every path that has all vertices in N_2 trivially satisfies the necessary path-requirement. Therefore we have $\varphi(a)$. Then by induction over weak well-founded sets (Lemma 1), we have $\forall s \in N_0 . \varphi(s)$. $\square$

Remark For the intuitive understanding, a vertex s satisfies φ may be interpreted as that every s-path satisfies the following property:

$$N_0 \wedge X(((N_0)U(N_1)) \vee (G(N_0) \wedge FG(N_2)))$$

where X, U, F, G have the meaning of the usual temporal operators.

Z-Infinite Graphs

Definition 3 (Z-Infinite Graphs). *Let (V, E) be a directed graph and $Z \subseteq V$. (V, E) is Z-infinite, if it is self-loop free, and for every infinite path π in V, there is an $i \geq 0$ such that $\pi_j \in Z$ for all $j \geq i$.*

In other words, a Z-infinite directed graph is a self-loop free graph such that non-Z vertices may only appear finitely many times in any infinite path. A graph is $\emptyset$-infinite iff it is a graph with no infinite paths.

Lemma 3. *Let (V, E) be a Z-infinite directed graph. Then $(S, \sqsubseteq) = po(V, E)$ is Z-well-founded, and furthermore, if $(s, s') \in E$, then $s' \sqsubset s$.*

Proof. Suppose that, on the contrary, $po(V, E)$ is not Z-well-founded. Then there is an infinite descending chain in $po(V, E)$ such that elements not in Z appear infinitely many times. Then there is an infinite path in (V, E) such that elements not in Z appear infinitely many times, contradicting to that (V, E) is Z-infinite. For the second part, suppose that $(s, s') \in E$. By the definition of $po(V, E)$, we have $s' \sqsubseteq s$, and since (V, E) is Z-infinite, we have $s' \neq s$. □

Y-Bounded Subgraphs

Definition 4 (Y-Bounded Subgraphs). *Let (V, E) be a directed graph and $S, Y \subseteq V$. $Gr(S)$ is Y-bounded, if $S \cap Y = \emptyset$ and $succ(S) \subseteq S \cup Y$.*

In other words, a Y-bounded subgraph is subgraph such that every vertex in the subgraph is not in Y and every step that moves out of the subgraph moves to a vertex in Y.

Lemma 4. *Let (V, E) be a directed graph and $N_0, N_1 \in V$ such that $Gr(N_0)$ is an N_1-bounded subgraph. Let $\varphi(s)$ denote the following property.*

> *For every s-path π, there is a $k \geq 1$ such that $\pi_0, ..., \pi_{k-1} \in N_0$ and $\pi_k \in N_1$, or for all $i \geq 0$ we have that $\pi_i \in N_0$.*
>
> *Then $\forall s \in N_0.\varphi(s)$.*

Proof. This lemma follows from the definition of N_1-bounded subgraphs. □

Lemma 5. *Let (V, E) be a directed graph and $N_0, N_1, N_2 \subseteq V$ such that $N_0 \cap N_1 = \emptyset$ and $N_2 \subseteq N_0$. Let $Z \subseteq W$ and $(W, \sqsubseteq)$ be Z-well-founded. Let $f : N_0 \to W$ such that $f(N_0 \setminus N_2) \cap Z = \emptyset$. Suppose that $\forall a \in N_0$, if $a \to b$, then (i) $b \in N_1$ or (ii) $b \in N_0$ and $f(b) \sqsubset f(a)$. Then $Gr(N_0)$ is an N_1-bounded N_2-infinite subgraph.*

Proof. We have to prove (i) $N_0 \cap N_1 = \emptyset$ and $succ(N_0) \subseteq N_0 \cup N_1$, and (ii) $Gr(N_0)$ is N_2-infinite. The former follows easily from the premises. The latter is argued as follows.

Suppose that $Gr(N_0)$ is not N_2-infinite.

Since it is easily verified that $Gr(N_0)$ is self-loop free, there must be an infinite path π in N_0 such that $N_0 \setminus N_2$ elements appear infinitely many times in π.

For $\pi_i \in N_0$, we have $f(\pi_i) \in W$ and for $\pi_j \in (N_0 \setminus N_2)$, we have $f(\pi_j) \notin Z$. Therefore we have an infinite chain $f(\pi) = f(\pi_0)f(\pi_1)\cdots$ such that non-Z elements appear infinitely many times on $f(\pi)$, contradicting to that $(W, \sqsubseteq)$ is Z-well-founded. □

Lemma 6. *Let (V, E) be a directed graph and $N_0, N_1, N_2 \in V$ such that $N_2 \subseteq N_0$ and $Gr(N_0)$ is an N_1-bounded N_2-infinite subgraph. Let $\varphi(s)$ denote the following property.*

For every s-path π, there is a $k \geq 1$ such that $\pi_0, ..., \pi_{k-1} \in N_0$ and $\pi_k \in N_1$, or for all $i \geq 0$ we have that $\pi_i \in N_0$ and there is an $l \geq 0$ such that $\pi_j \in N_2$ for all $j \geq l$.

Then $\forall s \in N_0.\varphi(s)$.

Proof. Let $(W, \sqsubseteq) = po(Gr(N_0))$. By Lemma 3, $(W, \sqsubseteq)$ is N_2-well-founded. Then by Lemma 2, the conclusion holds.

Lemma 7. *Let (V, E) be a directed graph and $S, Z, Y \subseteq V$ such that $Z \subseteq S$. Suppose that $Gr(S)$ is a Y-bounded Z-infinite subgraph. Let $(W, \sqsubseteq) = po(Gr(S))$. Then $W = S$ and $(W, \sqsubseteq)$ is Z-well-founded, and furthermore, if $s \in S$ and $s \to s'$, then (i) $s' \in Y$ or (ii) $s' \in S$ and $s' \sqsubset s$.*

Proof. The first part of this lemma follows from Lemma 3. The second part follows from the definition of Y-bounded subgraphs and the last part of Lemma 3. □

Some Special Cases of the Lemmas

Lemma 8. *Let (V, E) be a directed graph with no infinite paths. Then $(S, \sqsubseteq) = po(V, E)$ is a well-founded set, and furthermore, if $(s, s') \in E$, then $s' \sqsubset s$.*

Proof. This is a special case of Lemma 3, by considering a directed graph with no infinite paths as an $\emptyset$-infinite directed graph.

Lemma 9. *Let (V, E) be a directed graph and $N_0, N_1 \subseteq V$ such that $N_0 \cap N_1 = \emptyset$. Let $(W, \sqsubseteq)$ be a well-founded set. Let $f : N_0 \to W$. Suppose that $\forall a \in N_0$, if $a \to b$, then (i) $b \in N_1$ or (ii) $b \in N_0$ and $f(b) \sqsubset f(a)$. Then $Gr(N_0)$ is an N_1-bounded subgraph with no infinite paths.*

Proof. This is a special case of Lemma 5 by considering a subgraph with no infinite paths as an $\emptyset$-infinite directed graph, and replacing N_2 with the empty set.

Y-Terminating Subgraphs

Definition 5 (Y-Terminating Subgraphs). *Let (V, E) be a directed graph and $S, Y \subseteq V$. $Gr(S)$ is a Y-terminating subgraph of (V, E), if $S \cap Y = \emptyset$ and for every $a \in S$, there is a finite path $s_0 \cdots s_k$ with $s_0 = a$ and $k \geq 1$ such that $s_0, ..., s_{k-1} \in S$ and $s_k \in Y$.*

Lemma 10. *Let (V, E) be a directed graph and $N_0, N_1 \subseteq V$ such that $N_0 \cap N_1 = \emptyset$. Let $(W, \sqsubseteq)$ be a well-founded set. Let $f : N_0 \to W$. Suppose that $\forall a \in N_0$, there exists b such that $a \to b$ and (i) $b \in N_1$ or (ii) $b \in N_0$ and $f(b) \sqsubset f(a)$. Then $Gr(N_0)$ is an N_1-terminating subgraph.*

Proof. It is easily seen by applying an inductive argument over the well-founded set that for every vertex in N_0, there is a finite path of length > 1 such that the last vertex in the path is in N_1 and the rest of the elements of the path are in N_0, and since $N_0 \cap N_1 = \emptyset$, we have that $Gr(N_0)$ is an N_1-terminating subgraph. □

Lemma 11. *Let* (V, E) *be a directed graph and* $S, Y \subseteq V$. *If* $Gr(S)$ *is a* Y*-terminating subgraph, then for every* $s \in S$ *the following hold.*

> *There exists an* s*-path* π *such that* $\pi_0, ..., \pi_{k-1} \in S$ *and* $\pi_k \in Y$ *for some* $k \geq 1$.

Proof. This follows from the definition of Y-terminating subgraphs. $\square$

Definition 6. *Let* (V, E) *be a directed graph and* $Y \subseteq V$. $wo(V, E, Y)$ *denotes the preorder* $(S, \sqsubseteq)$ *with* S *and* $\sqsubseteq$ *defined as follows.*

- *Let* S_{-1} *denote* Y.
- *Let* S_i *for* $i \geq 0$ *be defined as follows.*
  $s \in S_i$ *iff* $s \notin \cup_{j=-1}^{i-1} S_j$ *and there is an* $s' \in S_{i-1}$ *such that* $(s, s') \in E$.
- $S = \cup_{j \geq 0} S_j$.
- $\sqsubseteq = \{(s, s') \mid s \in S_i, s' \in S_j, j > i \geq 0\} \cup \{(s, s) \mid s \in S\}$.

By the definition, it is easily seen that $(V', \sqsubseteq) = wo(V, E, Y)$ is a well-founded set, $V' \subseteq V$ and $V' \cap Y = \emptyset$.

Lemma 12. *Let* (V, E) *be a directed graph and* $S, Y \subseteq V$ *such that* $Gr(S)$ *is a* Y*-terminating subgraph. Let* $(S', \sqsubseteq) = wo(S \cup Y, E, Y)$. *Then* $(S', \sqsubseteq)$ *is a well-founded set and* $S' = S$, *and furthermore, the following hold.*

> *If* $s \in S'$ *is not a minimal element, then there exists* $s' \in S'$ *such that* $(s, s') \in E$ *and* $s' \sqsubset s$, *and if* $s \in S'$ *is a minimal element, then there exists* $s' \in Y$ *such that* $(s, s') \in E$.

Proof. This follows from the definition of Y-terminating subgraphs and that of the definition of $wo(S \cup Y, E, Y)$. $\square$

Y-Weak-Bounded Subgraphs

Definition 7 (Y-Weak-Bounded Subgraphs). *Let* (V, E) *be a directed graph and* $S, Y \subseteq V$. $Gr(S)$ *is a* Y*-weak-bounded subgraph of* (V, E), *if* $S \cap Y = \emptyset$ *and for every* $a \in S$, $succ(\{a\}) \cap (S \cup Y) \neq \emptyset$.

Lemma 13. *Let* (V, E) *be a directed graph and* $S, Y \subseteq V$. *If* $Gr(S)$ *is a* Y*-weak-bounded subgraph, then for every* $s \in S$ *the following hold.*

> *There exists an* s*-path* π *such that* $\pi_0, ..., \pi_{k-1} \in S$ *and* $\pi_k \in Y$ *for some* $k \geq 1$, *or all vertices on* π *are in* S.

Proof. This follows from the definition of Y-weak-bounded subgraphs. $\square$

3 First Order Kripke Structures

Let $B = (F, P)$ where F is a set of function symbols and P is a set of predicate symbols be the base for a first order logic. Let $\mathcal{T}_B$ denote the set of terms induced by F, and $\mathcal{L}_B$ denote the set of the first order formulas induced by B.

For $\phi \in \mathcal{L}_B$, we use $\phi^{e_1,...,e_k}_{x_1,...,x_k}$ to denote the result of simultaneously replacing all occurrences of the free variables $x_1, ..., x_k$ with respectively $e_1, ..., e_k$.

Similarly, for $e \in \mathcal{T}_B$, we use $e^{e_1,...,e_k}_{x_1,...,x_k}$ to denote the result of simultaneously replacing all occurrences of the variables $x_1, ..., x_k$ with respectively $e_1, ..., e_k$.

We use $var(\phi)$ to denote the set of free variables appearing in ϕ. We say that $\phi \in \mathcal{L}_B$ is a formula over V, if $var(\phi) \subseteq V$. The set of formulas over V is denoted $\mathcal{L}_{B,V}$.

For a formula $\phi \in \mathcal{L}_{B,V}$ with $V = \{v_1, ..., v_n\}$, we use ϕ' to denote $\phi^{v'_1,...,v'_n}_{v_1,...,v_n}$.

Let $I = (D, I_0)$ be an interpretation of B.

Let Σ denote the set of assignments of variables.

For $\sigma \in \Sigma$, we use $\sigma \models_I \phi$, or simply $\sigma \models \phi$ when I is understood in the context, to denote $I(\phi)\sigma = true$. In this case, we say that σ satisfies ϕ.

Sometimes, $I(\phi)\sigma = true$ is also written as $I(\phi)\sigma$ or $\phi(\sigma)$ when the meaning is clear from the context.

For $d \in D$, we use $\sigma[v/d]$ to denote an assignment σ' such that $\sigma'(x) = \sigma(x)$ for $x \neq v$ and $\sigma'(x) = d$ for $x = v$.

An assignment of variables restricted to those of V is a function in $(V \to D)$. Such a function is called V-specific assignment.

For $\alpha \in (V \to D)$, we use $(\sigma\alpha)$ to denote an assignment σ' such that $\sigma'(x) = \sigma(x)$ for $x \notin V$ and $\sigma'(x) = \alpha(x)$ for $x \in V$.

Then for $\phi \in \mathcal{L}_{B,V}$, we have $I(\phi)(\sigma\alpha)$ iff $I(\phi)(\sigma'\alpha)$ for any $\sigma, \sigma' \in \Sigma$.

In such a case, we may write $I(\phi)\alpha$ instead of $I(\phi)(\sigma\alpha)$, and $\alpha \models \phi$ instead of $\sigma\alpha \models \phi$.

If $\alpha \models \phi$, we say that α satisfies ϕ.

Similarly, for e being a term with all of the variables in V, we have $I(e)(\sigma\alpha) = I(e)(\sigma'\alpha)$ for any $\sigma, \sigma' \in \Sigma$, and in such a case, we may write $I(e)\alpha$ instead of $I(e)(\sigma\alpha)$.

We use $\sigma|_V$ to denote $\alpha \in (V \to D)$ such that $\alpha(v) = \sigma(v)$ for $v \in V$. Then for $\phi \in \mathcal{L}_{B,V}$, we have that σ satisfies ϕ iff $\sigma|_V$ satisfies ϕ. For brevity, we may not always distinguish σ and the V-specific assignment $\sigma|_V$ when they have the same function in the context.

For a formula $\phi \in \mathcal{L}_{B,V}$, we use $\theta(\phi)$ to denote $\{\sigma|_V \mid I(\phi)(\sigma)\}$, the set of V-specific assignments satisfying ϕ.

First Order Kripke Structures Let V be a set of variables. We use V' to denote the set $\{v' \mid v \in V\}$.

Definition 8. *A first order Kripke structure over (B, V) is a triple (I, ρ, Θ) where $I = (D, I_0)$ is an interpretation of B, $\rho \in \mathcal{L}_{B,V \cup V'}$ is a formula over $V \cup V'$, and $\Theta \in \mathcal{L}_{B,V}$ is a formula over V.*

Let (B, V) with $V = \{v_1, ..., v_n\}$ and $M = (I, \rho, \Theta)$ over (B, V) be given.

States Let $\mathcal{A}$ denote the set of V-specific assignments $V \to D$. For convenience, an assignment $s \in \mathcal{A}$ is called a state. For a set $S \subseteq \mathcal{A}$, if $s \in S$, we say that s is an S-state. For a formula $\phi \in \mathcal{L}_{B,V}$, if $s \models \phi$, we say that s is a ϕ-state, or in other words, a state of ϕ. Sometimes, for convenience, we may consider ϕ as a set of states, i.e., we may not distinguish the formula ϕ and the set $\{s \mid s \models \phi\}$.

Transitions Let s, s' be states. We use $s \to s'$ to denote that there is a transition from s to s'. $s \to s'$ iff there is a $\sigma \in \Sigma$ such that $\sigma|_V = s$ and one of the following holds.

- $\sigma[v_1'/s'(v_1)]...[v_n'/s'(v_n)] \models \rho$
- $\forall \sigma'.\sigma[v_1'/\sigma'(v_1)]...[v_n'/\sigma'(v_n)] \not\models \rho$ and $s' = s$.

The first line represents that there is a transition from s to s' specified by ρ. The second line represents a stuttering step (i.e., a transition step where the state does not change) when no transitions are specified by ρ. Notice that the symbol $\to$ is also used for logical implication. The meaning of the symbol is determined by the context.

Successors If $s \to s'$, we say that s' is an s-successor, or in other words, a successor state of s. For a set $S \subseteq \mathcal{A}$, if s is a successor state of some S-state, we say that s is an S-successor, or in other words, a successor state of S. For a formula $\phi \in \mathcal{L}_{B,V}$, if s is a successor state of some ϕ-state, we say that s is a ϕ-successor, or in other words, a successor state of ϕ.

Paths and Computations A path of M is a path of the graph $(\mathcal{A}, \to)$. A computation is an infinite path π such that $\pi_0 \models \Theta$. The set of computations of M is denoted $[[M]]$.

Reachability We say that s' is reachable from s, if $s \xrightarrow{*} s'$. Let S be a set of states. We say that S is reachable from s, if there is a state $s' \in S$ such that $s \xrightarrow{*} s'$.

Nonstuttering Models A nonstuttering model is a model that stuttering steps are not allowed unless the current state is a state at which there are no other choices for making a transition step. Suppose that we have variables over natural numbers or over any domain with at least two values. Then a first order Kripke structure over (B, V) not satisfying the nonstuttering condition can be transformed into a model satisfying the condition by adding a new variable to V and modifying ρ to ρ' such that the value of the variable changes at every ρ' step. Without loss of generality, in the following, we only consider nonstuttering first order Kripke structures, and assume that $M = (I, \rho, \Theta)$ over (B, V) and $I = (D, I_0)$ are given.

3.1 On Weakest Preconditions

Definition 9. *Let $\phi \in \mathcal{L}_{B,V}$ be a formula. The one step weakest precondition of ϕ with respect to M, denoted $[M, \phi]$, or simply written as $[\phi]$, when M is understood in the context, is defined as follows.*

$$[\phi] \triangleq (\forall v_1' \cdots v_n'.(\rho \to \phi') \wedge (\exists v_1' \cdots v_n'.\rho \vee \phi)).$$

Intuitively, $[\phi]$ represents the set of states in which every state has all its successors in ϕ. This is clarified by the following lemmas.

Lemma 14. $\phi_0 \to [\phi_1]$ *iff every ϕ_0-successor is a ϕ_1-state.*

Proof.

- The if-part.
  Suppose that s is a ϕ_0 state implies that if $s \to s'$ then s' is a ϕ_1 state.
  Suppose s is a ϕ_0 state and $s \not\models \forall v_1' \cdots v_n'.(\rho \to \phi_1') \wedge (\exists v_1' \cdots v_n'.\rho \vee \phi_1)$.
  We show that there is a contradiction.
  We have two cases:
  (1) $s \not\models \forall v_1' \cdots v_n'.(\rho \to \phi_1')$;
  (2) $s \not\models \exists v_1' \cdots v_n'.\rho \vee \phi_1$.
  In the first case, we have $s \models \exists v_1' \cdots v_n'.(\rho \wedge \neg\phi_1')$;
  Let σ be an assignment such that $\sigma|_V = s$.
  There is an s' such that $\sigma[v_1'/s'(v_1)]...[v_n'/s'(v_n)] \models \rho \wedge \neg\phi_1'$.
  Then we have $s \to s'$ and $s' \models \neg\phi_1$, contradicting to the first supposition.
  In the second case, we have $s \models \forall v_1' \cdots v_n'.(\neg\rho) \wedge \neg\phi_1$;
  Let σ be an assignment such that $\sigma|_V = s$.
  Then we have $s \to s$ and $s \models \neg\phi_1$, which yields also a contradiction.
- The only-if part.
  By definition, we have the following.
  $\phi_0 \to [\phi_1]$ iff $\phi_0 \to \forall v_1' \cdots v_n'.(\rho \to \phi_1') \wedge (\exists v_1' \cdots v_n'.\rho \vee \phi_1)$.
  Suppose that $\phi_0 \to [\phi_1]$ holds, s is a ϕ_0 state and $s \to s'$.
  We have to prove that s' is a ϕ_1 state.
  Since $s \models \phi_0$, we have $s \models \forall v_1' \cdots v_n'.(\rho \to \phi_1') \wedge (\exists v_1' \cdots v_n'.\rho \vee \phi_1)$.
  Let σ be an assignment such that $\sigma|_V = s$.
  Then we have $\sigma \models \forall v_1' \cdots v_n'.(\rho \to \phi_1') \wedge (\exists v_1' \cdots v_n'.\rho \vee \phi_1)$.
  Since $s \to s'$, we have two cases:
  (1) $\sigma[v_1'/s'(v_1)]...[v_n'/s'(v_n)] \models \rho$;
  (2) $\forall\sigma'.\sigma[v_1'/\sigma'(v_1)]...[v_n'/\sigma'(v_n)] \not\models \rho$ and $s' = s$.
  In the first case, since we already have $\sigma \models \forall v_1' \cdots v_n'.(\rho \to \phi_1')$, we have $\sigma[v_1'/s'(v_1)]...[v_n'/s'(v_n)] \models \phi_1'$, and therefore s' is a ϕ_1 state.
  In the second case, since we already have $\sigma \models \exists v_1' \cdots v_n'.\rho \vee \phi_1$, we have $\sigma \models \phi_1$, and therefore $s \models \phi_1$.
  Then since $s' = s$, we have $s' \models \phi_1$.

$\square$

Lemma 15. *If every s-successor is a ϕ-state, then s is a $[\phi]$-state.*

Proof. Let ϕ_s be the representation of s, i.e., $\phi_s(\sigma)$ holds iff $\sigma|_V = s$. Suppose that every s-successor is a ϕ-state. Then by Lemma 14, we have $\phi_s \to [\phi]$. Then every ϕ_s-state is a $[\phi]$-state. Therefore s is a $[\phi]$-state. $\square$

Lemma 16. *Let η_0 and η_1 be first order formulas. Suppose that $\eta_0 \wedge [\eta_1] \to \eta_1$ holds. Let $N_i = \theta(\neg\eta_i)$ for $i = 0, 1$. Then $Gr(N_1 \setminus N_0)$ is an $(N_1 \cap N_0)$-weak-bounded subgraph.*

Proof. Let $s \in (N_1 \setminus N_0)$, i.e., s satisfies $\neg\eta_1$ and η_0.

By the premise and Lemma 15, not every successor of s is an η_1 state, i.e., there is an s-successor s' such that s' is a $\neg\eta_1$ state, i.e., $s' \in N_1$.

This means that for every $s \in (N_1 \setminus N_0)$, $succ(\{s\}) \cap N_1 \neq \emptyset$, and therefore $Gr(N_1 \setminus N_0)$ is an $(N_1 \cap N_0)$-weak-bounded subgraph, since $N_1 = (N_1 \setminus N_0) \cup (N_1 \cap N_0)$. $\square$

Lemma 17. *Let η_0 and η_1 be first order formulas. Suppose that $\neg\eta_0 \wedge \eta_1 \to [\eta_1]$ holds. Let $N_i = \theta(\eta_i)$ for $i = 0, 1$. Then $Gr(N_1 \setminus N_0)$ is an $(N_1 \cap N_0)$-bounded subgraph.*

Proof. Let $s \in N_1 \setminus N_0$, i.e., s satisfies η_1 and $\neg\eta_0$.

By the premise and Lemma 14, every successor of s is an η_1 state, i.e., $succ(\{s\}) \in N_1$.

This means that $succ(N_1 \setminus N_0) \subseteq N_1$, and therefore $Gr(N_1 \setminus N_0)$ is an $(N_1 \cap N_0)$-bounded subgraph, since $N_1 = (N_1 \setminus N_0) \cup (N_1 \cap N_0)$. $\square$

Lemma 18. *Let $\eta_0, \eta_1, \eta_2, w, u \in \mathcal{L}_B$ such that w, u are formulas with x as the only free variable. Let $e \in \mathcal{T}_B$, $\sqsubseteq$ be a binary predicate symbol of P, and v be a variable not appearing in $\eta_0, \eta_1, \eta_2, e, w, u$. Let $W = \{\sigma(x) \mid I(w)(\sigma)\}$ and $Z = \{\sigma(x) \mid I(w \wedge u)(\sigma)\}$. Suppose that $(W, I_0(\sqsubseteq))$ with $W \subseteq D$ is Z-well-founded, $\eta_0 \wedge \neg\eta_2 \to \neg u^e_x$ and $\forall v.(\eta_0 \to (w^e_x \wedge (e = v \to [\eta_1 \vee (\eta_0 \wedge e \sqsubset v)])))$. Let $N_0 = \theta(\eta_i)$ for $i = 0, 1, 2$. Then $Gr(N_0 \setminus N_1)$ is an N_1-bounded $((N_0 \setminus N_1) \cap N_2)$-infinite subgraph.*

Proof. Let $N'_0 = N_0 \setminus N_1$ and $N'_2 = N'_0 \cap N_2$. It is easily seen that $N'_0 \cap N_1 = \emptyset$, $N'_2 \subseteq N'_0$.

By weakening the premise, we have $\forall v.(\eta_0 \wedge \neg\eta_1 \to (w^e_x \wedge (e = v \to [\eta_1 \vee ((\eta_0 \wedge \neg\eta_1) \wedge e \sqsubset v)])))$.

Let f be defined by $f(\sigma) = I(e)(\sigma)$.

Since we have $\eta_0 \wedge \neg\eta_1 \to w^e_x$, $\eta_0 \wedge \neg\eta_2 \to \neg u^e_x$ and $\forall v.(\eta_0 \wedge \neg\eta_1 \to ((e = v \to ([\eta_1 \vee ((\eta_0 \wedge \neg\eta_1) \wedge e \sqsubset v)]))))$, it is easily seen f is a mapping from N'_0 to W such that $f(N'_0 \setminus N_2) \cap Z = \emptyset$ holds, and the supposition in Lemma 5 holds. Therefore by Lemma 5, $Gr(N'_0)$ is an N_1-bounded N'_2-infinite subgraph. $\square$

Lemma 19. *Let $\eta_0, \eta_1, w \in \mathcal{L}_B$ such that w is a formula with x as the only free variable. Let $e \in \mathcal{T}_B$, $\sqsubseteq$ be a binary predicate symbol of P, and v be a variable not appearing in η_0, η_1, e, w. Let $W = \{\sigma(x) \mid I(w)(\sigma)\}$. Suppose that $(W, I_0(\sqsubseteq))$ with $W \subseteq D$ is a well-founded set, and $\forall v.(\eta_0 \to (w^e_x \wedge (e = v \to [\eta_1 \vee (\eta_0 \wedge e \sqsubset v)])))$. Let $N_0 = \theta(\eta_i)$ for $i = 0, 1$. Then $Gr(N_0 \setminus N_1)$ is an N_1-bounded subgraph with no infinite paths.*

Proof. This lemma is a special case of Lemma 18, with u and η_2 replaced by $false$.

Lemma 20. *Let $\eta_0, \eta_1, w \in \mathcal{L}_B$ such that w is a formula with x as the only free variable. Let $e \in \mathcal{T}_B$, $\sqsubseteq$ be a binary predicate symbol of P, and v be a variable not appearing in η_0, η_1, e, w. Let $W = \{\sigma(x) \mid I(w)(\sigma)\}$. Suppose that $(W, I_0(\sqsubseteq))$ with $W \subseteq D$ is a well-founded set, and $\forall v.(\neg\eta_0 \to (w^e_x \wedge ([(\eta_1 \wedge (e \sqsubset v \to \eta_0)] \to e \neq v))))$. Let $N_i = \theta(\neg\eta_i)$ for $i = 0, 1$. Then $Gr(N_0 \setminus N_1)$ is an N_1-terminating subgraph.*

Proof. Let $N'_0 = N_0 \setminus N_1 = \theta(\neg(\eta_0 \vee \neg\eta_1))$. It is easily seen that $N'_0 \cap N_1 = \emptyset$.

By weakening the premise, we have $\forall v.(\neg(\eta_0 \vee \neg\eta_1) \to (w^e_x \wedge ([(\eta_1 \wedge (e \sqsubset v \to (\eta_0 \vee \neg\eta_1))] \to e \neq v))))$.

Let f be defined by $f(\sigma) = I(e)(\sigma)$.

Since we have $\neg(\eta_0 \vee \neg\eta_1) \to w^e_x$ and $\forall v.(\neg\eta_0 \to ([(\eta_1 \wedge (e \sqsubset v \to \neg(\eta_0 \vee \neg\eta_1))] \to e \neq v)))$, it is easily seen f is a mapping from N'_0 to W, and the supposition in Lemma 10 holds. Therefore by Lemma 10, $Gr(N'_0)$ is an N_1-terminating subgraph. $\square$

3.2 On Sufficiently Expressive Underlying First Order Logics

In order to be able to formulate necessary assertions on states for specification and verification purposes, we assume that the underlying first order logic is sufficiently expressive. The expressiveness condition assumes the following.

- If a representation of a set of states is needed, then the set is representable by a first order formula.
- If a relation is need for comparing elements of a weak well-founded set, then the relation is representable by a predicate symbol.
- If a function is needed for mapping a set of states to values, then the function is representable by a term.

Suppose that w, u are formulas with x as the only free variable, and $\sqsubseteq$ is a binary relation symbol.

Let $W = \{\sigma(x) \mid I(w)(\sigma)\} \subseteq D$ and $Z = \{\sigma(x) \mid I(w \wedge u)(\sigma)\} \subseteq W$.

We say that w, u and $\sqsubseteq$ define a weak-well-founded set, if $(W, I_0(\sqsubseteq))$ is Z-well-founded. As a special case, if $(W, I_0(\sqsubseteq))$ is well-founded, we say that w and $\sqsubseteq$ define a well-founded set.

Then we have the following notations and remarks that concretizing the expressiveness condition.

- For S being a set of states, we use $\mathcal{F}(S)$ to denote the first order formula representing S, i.e., $I(\mathcal{F}(S))(s)$ holds iff $s \in S$.
- For $(W, \preceq)$ being a Z-well-founded set where W is a set of states and $Z \subseteq W$, there are formulas w, u with x as the only free variable, and a binary relation symbol $\sqsubseteq$, such that w, u and $\sqsubseteq$ define a weak-well-founded set.

– Furthermore, suppose that $W' = \{\sigma(x) \mid I(w)(\sigma)\}$ and $Z' = \{\sigma(x) \mid I(w \wedge u)(\sigma)\}$. Then there is a term e such that $I(e)$ represents a function f from W to W' satisfying $b \preceq a$ iff $(f(b), f(a)) \in I_0(\sqsubseteq)$.

Lemma 21. *Let $(V, \rightarrow)$ be a directed graph and $S, Z, Y \subseteq V$. Suppose that $Gr(S)$ is a Y-bounded Z-infinite subgraph. Then there are e, w, u and $\sqsubseteq$ such that they define a weak-well-founded set and the following hold.*

- $\digamma(S) \wedge \neg\digamma(Z) \models \neg u_x^e$;
- $\digamma(S) \models w_x^e \wedge (e = v \rightarrow [\digamma(Y) \vee (\digamma(S) \wedge e \sqsubset v)])$;

Proof. Let $(W, \sqsubseteq_S) = po(Gr(S))$. By Lemma 7, $W = S$ and $(S, \sqsubseteq_S)$ is a Z-well-founded set. By the expressiveness condition, there are an expression e, first order formulas w, u, a symbol $\sqsubseteq$, a set $W' = \{\sigma(x) \mid I(w)(\sigma)\} \subseteq D$ and a set $Z' = \{\sigma(x) \mid I(w \wedge u)(\sigma)\}$ such that the following hold.

- $(W', I_0(\sqsubseteq))$ is Z'-well-founded,
- $s \in S$ iff $I(e)(s) \in W'$,
- $s \in Z$ iff $I(e)(s) \in Z'$,
- $(s, s') \in \sqsubseteq_S$ iff $(I(e)(s), I(e)(s')) \in I_0(\sqsubseteq)$.

By the construction, we have $\digamma(S) \wedge \neg\digamma(Z) \models \neg u_x^e$ and $\digamma(S) \models w_x^e$, explained as follows.

- Suppose that $I(\digamma(S))(s)$ holds.
  Then we have $s \in S$, $I(e)(s) \in W$, $I(w)(\sigma[x/I(e)(s)])$, and therefore $I(w_x^e)(s)$.
- Suppose that $I(\neg\digamma(Z))(s)$ holds.
  Then we have $s \notin Z$, $I(e)(s) \notin Z'$, $I(w \wedge u)(\sigma[x/I(e)(s)]) = false$.
  Suppose that $I(\digamma(S) \wedge \neg\digamma(Z))(s)$ holds.
  Then we have $I(u)(\sigma[x/I(e)(s)]) = false$, $I(\neg u)(\sigma[x/I(e)(s)]) = true$, and therefore $I(\neg u_x^e)(s)$.

Let s be a $\digamma(Y)$ state.

By Lemma 7, if $s \rightarrow s'$, then s' is either in Y or in S. Then we have $\digamma(S) \rightarrow [\digamma(Y) \vee \digamma(S)]$. In addition, if $s' \in S$, then $(s', s) \in \sqsubset_S$, i.e., $(I(e)(s'), I(e)(s)) \in I_0(\sqsubset)$. Therefore $\digamma(S) \models w_x^e \wedge (e = v \rightarrow [\digamma(Y) \vee (\digamma(S) \wedge e \sqsubset v)])$. ☐

Lemma 22. *Let $(V, \rightarrow)$ be a directed graph. Let $S, Y \subseteq V$. Suppose that $Gr(S)$ is a Y-bounded subgraph with no infinite paths. Then there are e, w and $\sqsubseteq$ such that they define a well-founded set and*

$$\digamma(S) \models w_x^e \wedge (e = v \rightarrow [\digamma(Y) \vee (\digamma(S) \wedge e \sqsubset v)]).$$

Proof. This is a special case of Lemma 21 by considering a subgraph with no infinite paths as an $\emptyset$-infinite directed graph, and replacing Z with the empty set and u with $false$. ☐

Lemma 23. *Let $(V, \rightarrow)$ be a directed graph and $S, Y \subseteq V$ such that $Gr(S)$ is a Y-terminating subgraph. Then there are e, w and $\sqsubseteq$ such that they define a well-founded set and*

$$\digamma(S) \models w_x^e \wedge ([\neg\digamma(Y) \wedge (e \sqsubset v \rightarrow \neg\digamma(S))] \rightarrow e \neq v).$$

Proof.

Let $(W, \sqsubseteq_S) = wo(S \cup Y, \rightarrow, Y)$. By Lemma 12, $W = S$ and $(S, \sqsubseteq_S)$ is a well-founded set. By the expressiveness condition, there are an expression e, a first order formula w, a symbol $\sqsubseteq$, a set $W' = \{\sigma(x) \mid I(w)(\sigma)\} \subseteq D$ such that the following hold.

- $(W', I_0(\sqsubseteq))$ is a well-founded set.
- $s \in S$ iff $I(e)(s) \in W'$,
- $(s, s') \in \sqsubseteq_S$ iff $(I(e)(s), I(e)(s')) \in I_0(\sqsubseteq)$.

By the construction, we have $\mathcal{F}(S) \models w^e_x$.

Let s be a $\mathcal{F}(S)$ state.

By Lemma 12, if s is a minimal element of S, there exists an s-successor s' such that s' is a Y-state, i.e., s is not in $[\neg \mathcal{F}(Y) \wedge (e \sqsubset v \rightarrow \neg \mathcal{F}(S))]$ for every v such that $v = I(e)(s)$. On the other hand, if s is not a minimal element of S, then there exists an s-successor s' such that s' is an S-state and $(s', s) \in \sqsubset_S$. This means that we have $(I(e)(s'), I(e)(s)) \in I_0(\sqsubset)$, and for every v such that $v = I(e)(s)$, s' is an $\mathcal{F}(S)$ state and $(I(e)(s'), v) \in I_0(\sqsubset)$. Therefore $\mathcal{F}(S) \models w^e_x \wedge ([\neg \mathcal{F}(Y) \wedge (e \sqsubset v \rightarrow \neg \mathcal{F}(Z))] \rightarrow e \neq v)$. □

4 LTL Formulas

Let (B, V) be given. In the following, we present a first order linear time temporal logic (LTL). The logic was introduced in [33] and the following presentation can be seen as a subset of the one in [28].

Syntax Let ϕ range over $\mathcal{L}_{B,V}$. The set of LTL formulas over (B, V) is defined as follows.

$$\Phi ::= \phi \mid \neg\Phi \mid \Phi \wedge \Phi \mid \Phi \vee \Phi \mid \Phi \rightarrow \Phi \mid X\,\Phi \mid F\,\Phi \mid G\,\Phi \mid \Phi\,U\,\Phi \mid \Phi\,R\,\Phi$$

Semantics Let the first order Kripke structure $M = \langle I, \rho, \Theta \rangle$ over (B, V) be given.

Definition 10. *Let π denote an infinite path of M. Let φ (possibly with subscripts) denote an LTL formula. That the path π satisfies φ, denoted $\pi \models_M \varphi$, or simply $\pi \models \varphi$ when M is understood in the context, is defined as follows.*

$\pi \models \varphi$	*if* $\varphi \in \mathcal{L}_{B,V}$ *and* $I(\varphi)(\pi_0) = true$
$\pi \models \neg\varphi$	*if* $\pi \not\models \varphi$
$\pi \models \varphi_0 \vee \varphi_1$	*if* $\pi \models \varphi_0$ *or* $\pi \models \varphi_1$
$\pi \models \varphi_0 \wedge \varphi_1$	*if* $\pi \models \varphi_0$ *and* $\pi \models \varphi_1$
$\pi \models \varphi_0 \rightarrow \varphi_1$	*if* $\pi \models \varphi_0$ *implies* $\pi \models \varphi_1$
$\pi \models X\varphi$	*if* $\pi^1 \models \varphi$
$\pi \models G\varphi$	*if* $\forall i \geq 0.(\pi^i \models \varphi)$
$\pi \models F\varphi$	*if* $\exists i \geq 0.(\pi^i \models \varphi)$
$\pi \models \varphi_0 U \varphi_1$	*if* $\exists i \geq 0.((\pi^i \models \varphi_1) \wedge \forall j < i.(\pi^j \models \varphi_0))$
$\pi \models \varphi_0 R \varphi_1$	*if* $\forall i \geq 0.(\forall j < i.(\pi^j \not\models \varphi_0) \rightarrow (\pi^i \models \varphi_1))$

Definition 11. *$M \models \varphi$, if $\pi \models \varphi$ for every computation $\pi \in [[M]]$.*

Definition 12 (Equivalence). *Let φ_0 and φ_1 be two LTL formulas. φ_0 and φ_1 are equivalent, denoted $\varphi_0 \equiv \varphi_1$, if for every first order Kripke structure M over (B, V), we have $M \models \varphi_0$ iff $M \models \varphi_1$.*

For convenience, we use $\perp$ to denote the logical constant *false* (or the formula $t \neq t$ for some ground term t of the first order language, assuming that the set of ground terms is not empty), and $\top$ to denote the logical constant *true*.

In addition to the traditional binary operators U and R, we introduce two quinary operators U and R. The quinary operators are a kind of generalization of their respective binary ones, with the following interpretation.

$$\begin{array}{c}
\hline
\varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4) \equiv \varphi_0 U(\varphi_1 \vee (\varphi_2 R \varphi_3) \vee F\varphi_4) \\
\varphi_0 R(\varphi_1, \varphi_2, \varphi_3, \varphi_4) \equiv \varphi_0 R(\varphi_1 \wedge (\varphi_2 U \varphi_3) \wedge G\varphi_4) \\
\hline
\end{array}$$

The motivation of adding the quinary operators is to have a single operator (with its dual one) to cover the set of CTL* properties considered as the interesting ones in [11]. We have the following equivalences.

$$\begin{aligned}
F\varphi &\equiv \top U \varphi \\
G\varphi &\equiv \perp R \varphi \\
\varphi_0 U \varphi_1 &\equiv \varphi_0 U(\varphi_1, \perp, \perp, \perp) \\
\varphi_0 R \varphi_1 &\equiv \varphi_0 R(\varphi_1, \top, \top, \top) \\
\neg(\varphi_0 R(\varphi_1, \varphi_2, \varphi_3, \varphi_4)) &\equiv (\neg\varphi_0 U(\neg\varphi_1, \neg\varphi_2, \neg\varphi_3, \neg\varphi_4)) \\
\neg(\varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4)) &\equiv (\neg\varphi_0 R(\neg\varphi_1, \neg\varphi_2, \neg\varphi_3, \neg\varphi_4)) \\
\varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4) &\equiv (\varphi_0 U \varphi_1) \vee (\varphi_0 U(\varphi_2 R \varphi_3)) \vee F\varphi_4
\end{aligned}$$

Normal Form An LTL formula is in the negation normal form (NNF), if the negation $\neg$ is applied only to first order formulas and the formula does not contain the symbol $\rightarrow$. Let NNF(X,U,R) denote the set of NNF formulas with temporal operators only in $\{X, U, R\}$ where U, R are the two quinary operators. Let ϕ range over $\mathcal{L}_{B,V}$. The set of NNF(X,U,R) formulas is defined as follows.

$$\Phi ::= \phi \mid \Phi \wedge \Phi \mid \Phi \vee \Phi \mid X\,\Phi \mid \Phi\; U\; (\Phi, \Phi, \Phi, \Phi) \mid \Phi\; R\; (\Phi, \Phi, \Phi, \Phi)$$

Every LTL formula can be transformed into an equivalent one in NNF(X,U,R). Then without loss of generality, we only consider NNF(X,U,R) formulas. Formulas not in such a form are considered as an abbreviation of the equivalent ones in NNF(X,U,R).

4.1 A Proof System

In the following, we use ϕ to denote a first order formula, Γ to denote a set of first order formulas, and φ to denote an LTL formula (in NNF). For brevity, we sometimes write ϕ for $\{\phi\}$, and Γ, ϕ for $\Gamma \cup \{\phi\}$.

- A state s is called a φ-state, if $\forall \pi(s).(\pi \models \varphi)$.

– A state s is called a Γ-state, if it is a ϕ-state for every $\phi \in \Gamma$.

Since a first order formula ϕ is also an LTL formula, whether a state is a ϕ-state may be determined by this definition. This usage coincides with the meaning of ϕ-states defined in the previous section.

For convenience, the set of φ states is denoted $\theta(\varphi)$, and we use $\bar{\theta}(\varphi)$ to denote the set of states such that each of the states is a starting point for some path satisfying $\neg\varphi$.

Definition 13. *$\Gamma \models \varphi$, if every Γ-state is a φ-state.*

Proposition 1. *$M \models \varphi$ iff $\Theta \models \varphi$.*

This proposition is a consequence of the definitions of $M \models \varphi$ and $\Theta \models \varphi$. In the following, we present a proof system for $\Gamma \models \varphi$.

Lemma 24. *Let η_0 and η_1 be first order formulas. Suppose that $\neg\eta_0 \wedge \eta_1 \to [\eta_1]$ holds. Then $\eta_1 \models \eta_0 R \eta_1$.*

Proof. Let $N_i = \theta(\eta_i)$ for $i = 0, 1$.

By Lemma 17, $Gr(N_1 \setminus N_0)$ is an $N_1 \cap N_0$-bounded subgraph. Following from Lemma 4, we have $\eta_1 \wedge \neg\eta_0 \models \eta_0 R \eta_1$.

Since it is trivially that $\eta_1 \wedge \eta_0 \models \eta_0 R \eta_1$ holds, we have $\eta_1 \models \eta_0 R \eta_1$. □

Lemma 25. *Let $\eta_0, \eta_1, \eta_2, w, u \in \mathcal{L}_B$ such that w, u are formulas with x as the only free variable. Let $e \in \mathcal{T}_B$, $\sqsubseteq$ be a binary relation symbol of P, and v be a variable not appearing in $\eta_0, \eta_1, \eta_2, e, w, u$. Let $W = \{\sigma(x) \mid I(w)(\sigma)\}$ and $Z = \{\sigma(x) \mid I(w \wedge u)(\sigma)\}$. Suppose that $(W, I_0(\sqsubseteq))$ with $W \subseteq D$ is Z-well-founded, $\eta_0 \wedge \neg\eta_2 \to \neg u^e_x$ and $\forall v.(\eta_0 \to (w^e_x \wedge (e = v \to [\eta_1 \vee (\eta_0 \wedge e \sqsubset v)])))$. Then $\eta_0 \vee \eta_1 \models (\eta_0 U \eta_1) \vee (G(\eta_0) \wedge FG(\eta_2))$ holds.*

Proof.

Let $X_i = \theta(\eta_i)$ for $i = 0, 1, 2$.

Let $N_0 = X_0 \setminus X_1$, $N_1 = X_1$ and $N_2 = N_0 \cap X_2$.

By Lemma 18, $Gr(N_0)$ is an N_1-bounded N_2-infinite subgraph. Following from Lemma 6, we have $\eta_0 \wedge \neg\eta_1 \models X(((\eta_0 \wedge \neg\eta_1) U \eta_1) \vee (G(\eta_0 \wedge \neg\eta_1) \wedge FG(\eta_0 \wedge \neg\eta_1 \wedge \eta_2)))$.

Since it implies $\eta_0 \wedge \neg\eta_1 \models (\eta_0 U \eta_1) \vee (G(\eta_0) \wedge FG(\eta_2))$ and it is trivially that $\eta_1 \models (\eta_0 U \eta_1) \vee (G(\eta_0) \wedge FG(\eta_2))$ holds, we have $\eta_0 \vee \eta_1 \models (\eta_0 U \eta_1) \vee (G(\eta_0) \wedge FG(\eta_2))$. □

Lemma 26. *Let $\eta_0, \eta_1, w \in \mathcal{L}_B$ such that w is a formula with x as the only free variable. Let $e \in \mathcal{T}_B$, $\sqsubseteq$ be a binary relation symbol of P, and v be a variable not appearing in η_0, η_1, e, w. Let $W = \{\sigma(x) \mid I(w)(\sigma)\}$. Suppose that $(W, I_0(\sqsubseteq))$ with $W \subseteq D$ is a well-founded set, and $\forall v.(\eta_0 \to (w^e_x \wedge (e = v \to [\eta_1 \vee (\eta_0 \wedge e \sqsubset v)])))$. Then $\eta_0 \vee \eta_1 \models \eta_0 U \eta_1$ holds.*

Proof. This lemma is a special case of Lemma 25, with u and η_2 replaced by $false$.

Proving First Order Formulas When φ is a first order formula, $\Gamma \models \varphi$ holds iff the conjunction of the formulas of Γ implies φ. We assume that we have an underlying proof system for proving $\Gamma \models \varphi$ in this case. We assume that this proof system is powerful enough such that we can freely use the usual first order reasoning techniques.

Proving Temporal Formulas Let $B = (F, P)$ be given. Let e (possibly with subscripts) denote a term of the first order logic, w, u denote first order formulas with x as the only free variable, v denote a variable, η denote a first order formula, and $\sqsubseteq$ denote a binary relation symbol of P. A set of reduction rules (referred to as RED-rules) is provided in Table 1. The reduction rules are used to reduce a proof of a formula to proofs of simpler ones (by using the rules backwards).

For the application of the rule involving both of w and u, it is required that w, u and $\sqsubseteq$ define a weak-well-founded set. For the application of the rule involving w without the accompanying u, it is required that $w, \sqsubseteq$ define a well-founded set. Similar restriction applies to $w_1, \sqsubseteq_1$ as well. In addition, v, v_1 are required to be variables not appearing in any places other than those explicitly specified in the rule.

Remark Notice that the use of terms to represent values imposes a restriction on the applicability of the rule, since what a term can express is constrained by the available symbols specified in B. As discussed in [24], one may as well use formulas for representing values in a rule. For simplicity, we still use terms for representing values. Besides using formulas for increasing the expressivity, for practicality, one may extend the set of symbols in B, which is discussed in Section 6.3.

Derived Rules For convenience, we formulate a set of derived rules for the unary operators F, G and the binary operators U, R. The rules are presented in Table 2. The name R_G indicates that the rule is derived from the rule R for the operator G, and R_R indicates that the rule is derived from the rule R for the binary operator R. The other two names have similar meaning. The explanation of the derivation is in the following table, where the meaning of the rows is as follows: The rule indicated in the column *Rule* is obtained from the rule in the column *Origin* by replacing the formulas listed in the column *True* with $\top$ and replacing those in the column *False* with $\bot$.

$Rule$	$Origin$	$True$	$False$
R_R	R	$\varphi_2, \varphi_3, \varphi_4, \eta_3, \eta_4$	η_2
U_U	U		$\varphi_2, \varphi_3, \varphi_4, \eta_2, \eta_3, \eta_4, \eta_5, \eta_6, u$
R_G	R_R		φ_0, η_0
U_F	U_U	φ_0	
U_{UR}	U		$\varphi_1, \varphi_4, \eta_1, \eta_4, \eta_5$

Table 1. RED Rules

$\wedge$	$\dfrac{\Gamma \vdash \varphi_0 \qquad \Gamma \vdash \varphi_1}{\Gamma \vdash \varphi_0 \wedge \varphi_1}$
$\vee$	$\dfrac{\eta_0 \vdash \varphi_0 \qquad \eta_1 \vdash \varphi_1 \qquad \Gamma \vdash \eta_0 \vee \eta_1}{\Gamma \vdash \varphi_0 \vee \varphi_1}$
X	$\dfrac{\eta_1 \vdash \varphi_1 \qquad \Gamma \vdash [\eta_1]}{\Gamma \vdash X\varphi_1}$
R	$\dfrac{\begin{array}{r l} \eta_0 & \vdash \varphi_0 \\ \eta_1 & \vdash \varphi_1 \\ \eta_3 & \vdash \varphi_3 \\ \eta_4 & \vdash \varphi_4 \\ \eta_1 & \vdash (\eta_2 \vee \eta_3) \wedge \eta_4 \\ \eta_1, \neg\eta_0 & \vdash [\eta_1] \\ \eta_4 & \vdash [\eta_4] \\ \eta_2 & \vdash \varphi_2 \wedge w^e_x \wedge (e = v \rightarrow [\eta_3 \vee (\eta_2 \wedge e \sqsubset v)]) \\ \Gamma & \vdash \eta_1 \end{array}}{\Gamma \vdash \varphi_0 R(\varphi_1, \varphi_2, \varphi_3, \varphi_4)}$
U	$\dfrac{\begin{array}{r l} \eta_1 & \vdash \varphi_1 \\ \eta_2 & \vdash \varphi_2 \\ \eta_3 & \vdash \varphi_3 \\ \eta_4 & \vdash \varphi_4 \\ \eta_6, \neg\eta_2, \neg\eta_4 & \vdash [\eta_6] \\ \eta_6, \neg\eta_3 & \vdash \eta_5 \vee \eta_4 \\ \eta_0, \neg\eta_3 & \vdash \neg u^e_x \\ \eta_0 & \vdash \varphi_0 \wedge w^e_x \wedge (e = v \rightarrow [\eta_1 \vee \eta_6 \vee (\eta_0 \wedge e \sqsubset v)]) \\ \eta_5 & \vdash (w_1)^{e_1}_x \wedge (e_1 = v_1 \rightarrow [\eta_4 \vee (\eta_5 \wedge e_1 \sqsubset_1 v_1)]) \\ \Gamma & \vdash \eta_0 \vee \eta_1 \vee \eta_6 \end{array}}{\Gamma \vdash \varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4)}$

Table 2. RED Derived Rules

R_G	$\dfrac{\eta_1 \vdash \varphi_1 \qquad \eta_1 \vdash [\eta_1] \qquad \Gamma \vdash \eta_1}{\Gamma \vdash G\varphi_1}$
R_R	$\dfrac{\eta_0 \vdash \varphi_0 \qquad \eta_1 \vdash \varphi_1 \qquad \eta_1, \neg\eta_0 \vdash [\eta_1] \qquad \Gamma \vdash \eta_1}{\Gamma \vdash \varphi_0 R \varphi_1}$
U_F	$\dfrac{\eta_0 \vdash w^e_x \wedge (e = v \rightarrow [\eta_1 \vee (\eta_0 \wedge e \sqsubset v)]) \qquad \eta_1 \vdash \varphi_1 \qquad \Gamma \vdash \eta_0 \vee \eta_1}{\Gamma \vdash F\varphi_1}$
U_U	$\dfrac{\eta_0 \vdash \varphi_0 \wedge w^e_x \wedge (e = v \rightarrow [\eta_1 \vee (\eta_0 \wedge e \sqsubset v)]) \qquad \eta_1 \vdash \varphi_1 \qquad \Gamma \vdash \eta_0 \vee \eta_1}{\Gamma \vdash \varphi_0 U \varphi_1}$
U_{UR}	$\dfrac{\begin{array}{r l} \eta_2 & \vdash \varphi_2 \\ \eta_3 & \vdash \varphi_3 \\ \eta_6 & \vdash \eta_3 \\ \eta_6, \neg\eta_2 & \vdash [\eta_6] \\ \eta_0, \neg\eta_3 & \vdash \neg u^e_x \\ \eta_0 & \vdash \varphi_0 \wedge w^e_x \wedge (e = v \rightarrow [\eta_6 \vee (\eta_0 \wedge e \sqsubset v)]) \\ \Gamma & \vdash \eta_0 \vee \eta_6 \end{array}}{\Gamma \vdash \varphi_0 U(\varphi_2 R \varphi_3)}$

4.2 Soundness

In the following, we prove that the proof system is sound.

Theorem 1. *If $\Gamma \vdash \varphi$, then $\Gamma \models \varphi$.*

Proof by induction. If φ is a first order formula, then that $\Gamma \vdash \varphi$ implies $\Gamma \models \varphi$ is implied by the assumption on the soundness of the underlying proof system for the first order logic. For the RED-rules, we consider the rules case by case as follows.

Case 1. $\wedge$.

Suppose that we have $\Gamma \models \varphi_0$ and $\Gamma \models \varphi_1$. We prove $\Gamma \models \varphi_0 \wedge \varphi_1$ as follows.
Let s be a Γ-state. Then s is a state of φ_0 and s is a state of φ_1. Therefore s is a state of $\varphi_0 \wedge \varphi_1$.

Case 2. $\vee$.

Suppose that we have $\eta_0 \models \varphi_0$, $\eta_1 \models \varphi_1$, and $\Gamma \models \eta_0 \vee \eta_1$. We prove $\Gamma \models \varphi_0 \vee \varphi_1$ as follows.
Let s be a Γ-state. Then s is a state of $\eta_0 \vee \eta_1$.
Since η_0 and η_1 are first order formulas, either s is a state of η_0 or s is a state of η_1. Then either s is a state of φ_0 or s is a state of φ_1. Therefore s is a state of $\varphi_0 \vee \varphi_1$.

Case 3. X.

Suppose that we have $\eta_1 \models \varphi_1$ and $\Gamma \models [\eta_1]$. We prove $\Gamma \models X\varphi_1$ as follows.
Let s be a Γ-state. Since we have $\Gamma \models [\eta_1]$, by Lemma 14, every s-successor is an η_1 state. Therefore every s-successor is a φ_1 state. Therefore s is a state of $X\varphi_1$.

Case 4. R.

Suppose that the premises hold.
By the 6th premise and Lemma 24, we have the following.

(i) $\eta_1 \models \eta_0 R \eta_1$

By the 1st and 2nd premises, we have (i') $\eta_1 \models \varphi_0 R \varphi_1$.
By the second part of the 8th premise and Lemma 26, we have $\eta_2 \vee \eta_3 \models \eta_2 U \eta_3$, and then by the first part of the 8th premise and the 3rd premise, we have the following.

(ii) $\eta_2 \vee \eta_3 \models \varphi_2 U \varphi_3$

Suppose that $\Gamma \models \varphi_0 R(\varphi_1, \varphi_2, \varphi_3, \varphi_4)$ does not hold.
Let $s \in \Gamma$ and π be an s-path such that $\pi \models \neg\varphi_0 U(\neg\varphi_1 \vee (\neg\varphi_2 R \neg\varphi_3) \vee F\neg\varphi_4)$.
By the 9th premise, we have that s is an η_1 state.
We prove that there is a contradiction. We have three cases.

- Case 1: $\pi \models \neg\varphi_0 U \neg\varphi_1$.
  By (i'), π_0 is not an η_1 state, contradicting to that s (we have $\pi_0 = s$) is an η_1 state.
- Case 2: $\pi \models \neg\varphi_0 U(\neg\varphi_2 R \neg\varphi_3)$.
  Then there is a $k \geq 0$ such that $\pi^0, ..., \pi^{k-1}$ satisfy $\neg\varphi_0$ and π^k satisfies $\neg\varphi_2 R \neg\varphi_3$.
  By the 1st premise, $\pi_0, ..., \pi_{k-1}$ are not η_0 states.
  On the other hand, by (i), s is an $\eta_0 R \eta_1$ state, and then since $\pi_0, ..., \pi_{k-1}$ are not η_0 states and $\pi_0 = s$, we have that π_k is an η_1 state.
  By (ii), we have $\eta_2 \vee \eta_3 \models \varphi_2 U \varphi_3$.
  Then by the 5th premise, we have $\eta_1 \models \varphi_2 U \varphi_3$, and therefore π_k is a $\varphi_2 U \varphi_3$ state, contradicting to that π^k satisfies $\neg\varphi_2 R \neg\varphi_3$.
- Case 3: $\pi \models F \neg\varphi_4$.
  Then there is a $k \geq 0$ such that π^k satisfies $\neg\varphi_4$.
  This means that π_k is not a φ_4 state.
  Since s is an η_1 state, s is a φ_4 state, by the 5th and 4th premises.
  Then we have $k \geq 1$.
  Without loss of generality, we may assume that k is the least i such that π_i is not a φ_4 state.
  According to the 7th premise, π_{k-1} cannot be a φ_4 state, contradicting to the above assumption.

Case 5. U.

Suppose that the premises hold.

By the 5th premises and Lemma 24, we have $\eta_6 \models (\eta_2 \vee \eta_4) R(\eta_6)$, and then by the 6th premise, we have the following.

(i) $\eta_6 \models (\eta_2 \vee \eta_4) R(\eta_5 \vee \eta_4 \vee \eta_3)$.

By the 7th premise, the second part of the 8th premise and Lemma 25, we have the following.

(ii) $\eta_0 \vee \eta_1 \vee \eta_6 \models (\eta_0 U(\eta_1 \vee \eta_6)) \vee (G(\eta_0) \wedge FG(\eta_3))$

By the 9th premise and Lemma 26, we have the following.

(iii) $\eta_5 \vee \eta_4 \models \eta_5 U \eta_4$

Suppose that $\Gamma \models \varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4)$ does not hold.

Let $s \in \Gamma$ and π be an s-path such that $\pi \models \neg\varphi_0 R(\neg\varphi_1 \wedge (\neg\varphi_2 U \neg\varphi_3) \wedge G\neg\varphi_4)$.

By the 10th premise, s is also an $\eta_0 \vee \eta_1 \vee \eta_6$ state.

Let ψ denote $(\varphi_1 \vee (\varphi_2 R \varphi_3) \vee F\varphi_4)$.

Then $\pi \models \neg\varphi_0 R \neg\psi$, i.e., $\pi \models ((\neg\psi) U(\neg\psi \wedge \neg\varphi_0)) \vee G\neg\psi$. We prove that there is a contradiction. We have two cases.

- Case 1: $\pi \models (\neg\psi) U(\neg\psi \wedge \neg\varphi_0)$.
  Then π^j satisfies $\neg\varphi_4$ for all $j \geq 0$, and there is a $k \geq 0$ such that π^k satisfies $\neg\varphi_0$, and π^i satisfies $\neg\varphi_1$ and $\neg\varphi_2 U \neg\varphi_3$ for $i = 0, 1, ..., k$.

By the first part of the 8th premise, π_k is a $\neg\eta_0$ state.
By the 1st premise, $\pi_0, ..., \pi_k$ are $\neg\eta_1$ states.
By the 4th premise, π^j satisfies $\neg\eta_4$ for all $j \geq 0$, and then by (iii) π_j is not an $\eta_5 \vee \eta_4$ state for all $j \geq 0$.
Then by (i), $\pi_0, ..., \pi_k$ are $\neg\eta_6$ states.
Otherwise, we have a contradiction explained as follows.
Suppose that π_j is an η_6 state for some $0 \leq j \leq k$.
Then $\pi^j \models (\eta_2 \vee \eta_4)R(\eta_5 \vee \eta_4 \vee \eta_3)$.
Since η_5 and η_4 are not satisfied on any position on π^j, we have $\pi^j \models (\eta_2)R(\eta_3)$, and therefore $\pi^j \models (\varphi_2)R(\varphi_3)$ by the 2nd and 3rd premises, which yields a contradiction to that π^i satisfies $\neg\varphi_2 U \neg\varphi_3$ for $i = 0, 1, ..., k$.
This explains that $\pi_0, ..., \pi_k$ are $\neg\eta_6$ states, and then we have that π does not satisfy $(\eta_0 U(\eta_1 \vee \eta_6)) \vee (G(\eta_0) \wedge FG(\eta_3))$.
This contradicts to (ii), since $\pi_0 = s$ is an $\eta_0 \vee \eta_1 \vee \eta_6$ state.

- Case 2: $\pi \models G\neg\psi$.
Then π^j satisfies $\neg\varphi_4$ for $j \geq 0$, and for all $i \geq 0$, we have π^i satisfies $\neg\varphi_1$ and $\neg\varphi_2 U \neg\varphi_3$.
Similar to the argument in Case 1, π_j is a $\neg\eta_1$ state and a $\neg\eta_6$ state for all $j \geq 0$.
In addition, since π^i satisfies $\neg\varphi_2 U \neg\varphi_3$ for all $i \geq 0$, there are infinitely many positions on π satisfying $\neg\varphi_3$.
By the 3rd premise, the states on these positions are $\neg\eta_3$ states, and then we have that π does not satisfy $(\eta_0 U(\eta_1 \vee \eta_6)) \vee (G(\eta_0) \wedge FG(\eta_3))$.
This contradicts to (ii), since $\pi_0 = s$ is an $\eta_0 \vee \eta_1 \vee \eta_6$ state.

$\square$

4.3 Relative Completeness

Relativeness The relative completeness[1] assumes the expressiveness condition stated in Section 3.2 and the following condition on the underlying first order proof system.

> If φ is a first order formulas and $\Gamma \vdash \varphi$ is needed as a premise in the proof, then $\Gamma \vdash \varphi$ is provable by the underlying first order proof system when $\Gamma \models \varphi$ holds.

In the following, we prove that the proof system (with the set of RED-rules) is relatively complete for a subset of LTL defined as follows.

[1] Relative completeness is a notion for separation of concerns on techniques for manipulating programs and techniques for manipulating formulas of the underlying logic, and there has been a lot of research work discussing completeness and relative completeness, e.g., [9, 2, 22, 36].

Simple LTL Formulas Let ϕ range over $\mathcal{L}_{B,V}$. The subset of LTL, denoted SL, and called simple LTL formulas, is defined as follows (parts of the definition resemble that of LIN and ULIN in [6]), with UL being an auxiliary subset of SL.

$$\begin{array}{ll} \mathrm{SL} & ::= \mathrm{SL} \vee \phi \mid \phi \vee \mathrm{SL} \mid \mathrm{SL} \wedge \mathrm{SL} \mid X(\mathrm{SL}) \mid \phi\, R\, (\mathrm{SL}, \phi, \phi, \phi) \mid \phi\, U(\phi, \phi, \phi, \phi) \mid \mathrm{UL} \\ \mathrm{UL} & ::= \phi \mid \mathrm{SL}\, U\, \phi \mid \phi\, U\, (\mathrm{UL}) \mid \mathrm{UL} \vee \phi \mid \phi \vee \mathrm{UL} \end{array}$$

Lemma 27. *Let $\varphi U \psi$ be an LTL formula. If π satisfies $G(\neg\psi)$, then π satisfies $G(\neg(\varphi U \psi))$.*

Proof. This follows directly from the semantics. □

Lemma 28. *Let ψ be a* UL *formula. Suppose that π is an infinite path such that starting from every position of π there is a path satisfying $\neg\psi$. Then π satisfies $G(\neg\psi)$.*

Proof. In case ψ is a first order formula, from every position of π there is a path satisfying $\neg\psi$ implies that every position of π satisfies $\neg\psi$, and therefore π satisfies $G(\neg\psi)$. The rest of the cases is proved inductively as follows.

Case 1. $\psi = (\varphi U r)$ where φ is an SL formula and r is a first order formula.

Since from every position of π there is a path satisfying $\neg r$, we have that π satisfies $G(\neg r)$. By Lemma 27, π satisfies $G(\neg\psi)$.

Case 2. $\psi = (r U \psi_1)$ where r is a first order formula and ψ_1 is a UL formula.

Since from every position of π there is a path satisfying $\neg\psi$, we have that from every position of π there is a path satisfying $\neg\psi_1$, and then by the inductive hypothesis, we have π satisfies $G(\neg\psi_1)$. By Lemma 27, π satisfies $G(\neg\psi)$.

Case 3. $\psi = (\psi_1 \vee r)$ where r is a first order formula and ψ_1 is a UL formula.

Since from every position of π there is a path satisfying $\neg\psi$, we have that every position of π satisfies $\neg r$ and from every position of π there is a path satisfying $\neg\psi_1$. The former implies that π satisfies $G(\neg r)$, and by the induction hypothesis, the latter implies that π satisfies $G(\neg\psi_1)$. Therefore π satisfies $G(\neg\psi)$.

Case 4. $\psi = (r \vee \psi_1)$ where r is a first order formula and ψ_1 is a UL formula.

This case is similar to the previous one. □

Definition 14. *Let r denote a first order formula, φ denote an* SL *formula and ψ denote a* UL *formula. $f_0(\psi)$ is defined as follows.*

$$\boxed{\begin{array}{ll} f_0(r) & = r \\ f_0(\psi_0 \vee \psi_1) & = f_0(\psi_0) \vee f_0(\psi_1) \\ f_0(\varphi U \psi) & = f_0(\psi) \end{array}}$$

$f_0(\psi)$ maps a formula to a first order formula.

Lemma 29. *Let π be a path and ψ be a* UL *formula. If $\pi_0 \models f_0(\psi)$, then $\pi \models \psi$.*

Proof. It is easily seen this lemma holds by an application of structural induction.

Separation of a Path

Lemma 30. *Let π be a path and ψ be a* UL *formula. If $\pi \models \psi$, then $\pi_0 \models f_0(\psi)$ or $\pi^1 \models \psi$.*

Proof. In case ψ is a first order formula, we have $\pi \models \psi$ iff $\pi_0 \models \psi$ iff $\pi_0 \models f_0(\psi)$. The rest of the cases is proved inductively as follows.

Case 1. $\psi = (\varphi U r)$ where φ is an SL formula and r is a first order formula.

If $\pi \not\models r$, we have $\pi^1 \models \varphi U r$. Otherwise, we have $\pi_0 \models r$ and therefore $\pi_0 \models f_0(\psi)$.

Case 2. $\psi = (r U \psi_1)$ where r is a first order formula and ψ_1 is a UL formula.

If $\pi \not\models \psi_1$, we have $\pi^1 \models r U \psi_1$. Otherwise, by the induction hypothesis, either $\pi_0 \models f_0(\psi_1)$ or $\pi^1 \models \psi_1$. In the former case, we have $\pi_0 \models f_0(\psi)$, since $f_0(\psi) = f_0(\psi_1)$. In the latter case, we have $\pi^1 \models r U \psi_1$.

Case 3. $\psi = (\psi_1 \vee r)$ where r is a first order formula and ψ_1 is a UL formula.

If $\pi_0 \models r$, we are done. Otherwise, $\pi \models \psi_1$. By the induction hypothesis, either $\pi_0 \models f_0(\psi_1)$ or $\pi^1 \models \psi_1$. In the former case, we are done, since $f_0(\psi) = f_0(\psi_1) \vee r$ and therefore we have $\pi_0 \models f_0(\psi)$. Otherwise, we are also done, since we have $\pi^1 \models \psi_1 \vee r$.

Case 4. $\psi = (r \vee \psi_1)$ where r is a first order formula and ψ_1 is a UL formula.

This case is similar to the previous one. □

Lemma 31. *Let $\varphi = \varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4) \in$ SL be an SL formula with $\varphi_0, ..., \varphi_4$ being first order formulas. Let π be a path. If $\pi \models \varphi$, then $\pi_0 \models \varphi_1$ or $\pi_0 \models \varphi_2 \wedge \varphi_3$ or $\pi_0 \models \varphi_4$ or $\pi^1 \models \varphi$.*

Proof. We have three cases: $\pi \models \varphi_0 U \varphi_1$, $\pi \models \varphi_0 U(\varphi_2 R \varphi_3)$ and $\pi \models F\varphi_4$

- Case 1: $\pi \models \varphi_0 U \varphi_1$.
  By Lemma 30, we have $\pi_0 \models f_0(\varphi_0 U \varphi_1)$ or $\pi^1 \models \varphi$. Since $f_0(\varphi_0 U \varphi_1) = f_0(\varphi_1) = \varphi_1$, we are done.
- Case 2: $\pi \models \varphi_0 U(\varphi_2 R \varphi_3)$.
  Then we have $\pi \models (\varphi_2 \wedge \varphi_3) \vee (\varphi_3 \wedge X(\varphi_2 R \varphi_3)) \vee (\varphi_0 \wedge X(\varphi_0 U(\varphi_2 R \varphi_3)))$.
  Then we have $\pi_0 \models \varphi_2 \wedge \varphi_3$ or $\pi \models (\varphi_3 \wedge X(\varphi_2 R \varphi_3)) \vee (\varphi_0 \wedge X(\varphi_0 U(\varphi_2 R \varphi_3)))$.
  In the former case, we have $\pi_0 \models \varphi_2 \wedge \varphi_3$, and in the latter case, we have $\pi^1 \models \varphi$.
- Case 3: $\pi \models F\varphi_4$.
  Then we have $\pi_0 \models \varphi_4$ or $\pi^1 \models F\varphi_4$, and therefore $\pi_0 \models \varphi_4$ or $\pi^1 \models \varphi$.

□

We provide some definitions and lemmas for dealing with formulas of the forms $\varphi U \psi$ and $\varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4)$.

Definition 15. *Let $\varphi = \varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4)$. The set S^*_φ and S_φ are defined as follows.*

- *$s \in S^*_\varphi$, if s is a $(\varphi_2 R \varphi_3) \vee F\varphi_4$ state.*
- *$s \in S_\varphi$, if s is a φ state and not a φ_1 state and not an S^*_φ state.*

The set $S_{\varphi_0 U \varphi_1}$, where $\varphi_0 U \varphi_1$ is a special case of $\varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4)$, is defined according to S_φ, that is, $s \in S_{\varphi_0 U \varphi_1}$ iff s is a $\varphi_0 U \varphi_1$ state and there is an s-path satisfying $\neg\varphi_1$. It is easily seen that the following hold.

- If $\varphi_0, ..., \varphi_4$ are first order formulas, then every S_φ state is a φ_0 state.
- If $\varphi_0 U \varphi_1$ is a UL formula, then every $S_{\varphi_0 U \varphi_1}$ state is a φ_0 state.
  This can be seen from that for a UL formula $\varphi_0 U \varphi_1$ and a state s, it is not the case that there exist s-paths π and ζ such that $\pi \models \varphi_0 \wedge \neg\varphi_1$ and $\zeta \models \neg\varphi_0 \wedge \varphi_1$, since at least one of φ_0 and φ_1 is a first order formula.

Lemma 32. *Let $\varphi U \psi$ be a* UL *formula. Then $Gr(S_{\varphi U \psi})$ is a directed graph without infinite paths.*

Proof. Suppose that there is an infinite path. We prove that there is a contradiction. Let π be an infinite path. Since all the states on the path are in $S_{\varphi U \psi}$, we have that there is a path satisfying $\neg\psi$ from every such state, and then by Lemma 28, π satisfies $G(\neg\psi)$, contradicting to that π_0 is a $\varphi U \psi$ state. $\square$

Corollary 1. *Let $\varphi U \psi$ be a* UL *formula. Let $(S, \sqsubseteq_{\varphi U \psi}) = po(Gr(S_{\varphi U \psi}))$. Then $(S, \sqsubseteq_{\varphi U \psi})$ is a well-founded set, and furthermore, if $s, s' \in S_{\varphi U \psi}$ and $s \to s'$, then $s' \sqsubset_{\varphi U \psi} s$.*

Proof. This follows from Lemma 32 and Lemma 8. $\square$

Lemma 33. *Let $\varphi U \psi$ be a* UL *formula. Then $Gr(S_{\varphi U \psi})$ is $\theta(\psi)$-bounded.*

Proof.

Firstly, it is easily seen that $S_{\varphi U \psi} \cap \theta(\psi) = \emptyset$ from the definition.

Secondly, suppose that s is a state of $S_{\varphi U \psi}$. Since there is a path π starting from s such that $\pi \models \neg\psi$, by Lemma 29, s (i.e., π_0) does not satisfy $f_0(\psi)$. We have $f_0(\varphi U \psi) = f_0(\psi)$. Since every path starting from s satisfies $\varphi U \psi$ and s does not satisfy $f_0(\varphi U \psi)$, by Lemma 30, for every such path π, we have $\pi^1 \models \varphi U \psi$. Therefore such a π_1 is a state of $\varphi U \psi$. If π_1 is a state of ψ, we are done. Otherwise, π_1 is a state of $S_{\varphi U \psi}$.

Therefore $Gr(S_{\varphi U \psi})$ is $\theta(\psi)$-bounded. $\square$

Lemma 34. *Let $\varphi_0 U \varphi_1$ be a* UL *formula. Let $\eta_0 = \ulcorner(S_{\varphi_0 U \varphi_1})$ be the representation of $S_{\varphi_0 U \varphi_1}$, and $\eta_1 = \ulcorner(\theta(\varphi_1))$ be the representation of the set of φ_1 states. Then there are e, w and $\sqsubseteq$ such that they define a well-founded set and $\eta_0 \models w^e_x \wedge (e = v \to [\eta_1 \vee (\eta_0 \wedge e \sqsubset v)])$.*

Proof. This lemma follows from Lemma 22, with the following instantiation of S, Y.

- $S = S_{\varphi_0 U \varphi_1}$.
- $Y = \theta(\varphi_1)$.

The conditions in Lemma 22 are ensured by Lemma 32 and Lemma 33. $\square$

Lemma 35. *Let $F\varphi_1$ be a* UL *formula. Let $\eta_0 = \digamma(\theta(\neg\varphi_1 \wedge F\varphi_1))$, and $\eta_1 = \digamma(\theta(\varphi_1))$. Then there are e, w and $\sqsubseteq$ such that they define a well-founded set and $\eta_0 \models w^e_x \wedge (e = v \rightarrow [\eta_1 \vee (\eta_0 \wedge e \sqsubset v)])$.*

This is a special case of Lemma 34 with $\varphi_0 U \varphi_1$ replaced by $F\varphi_1$ and $S_{\varphi_0 U \varphi_1}$ replaced by $\theta(\neg\varphi_1 \wedge F\varphi_1)$. $\square$

Lemma 36. *Let $\varphi = \varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4) \in$* SL *be an* SL *formula with $\varphi_0, ..., \varphi_4$ being first order formulas. Then $Gr(S_\varphi)$ is a $\theta(\varphi_3)$-infinite directed graph.*

Proof.

(1) Suppose that there is an infinite path in $Gr(S_\varphi)$ such that $\neg\varphi_3$ states appears infinitely many times. We prove that there is a contradiction.

Let π be such an infinite path.

By the construction of S_φ, φ_2 and φ_3 cannot be satisfied at the same time on any position, otherwise, the state violates the condition that from the state there is a path satisfying $(\neg\varphi_2 U \neg\varphi_3) \wedge G(\neg\varphi_4)$.

Since on π, $\neg\varphi_3$ is satisfied infinitely many times, and φ_2 and φ_3 are not satisfied at the same time on any position, $\varphi_2 R \varphi_3$ is not satisfied on any position.

In addition, since φ_4 is a first order formulas, φ_4 is not satisfied on π^i for any $i \geq 0$, and $F\varphi_4$ is not satisfied on π.

Since every state on π is in S_φ, there is a path satisfying $\neg\varphi_1$ from every such state. Since φ_1 is a first order formula, φ_1 is not satisfied on π^i for any $i \geq 0$.

Therefore π does not satisfy φ, contradicting to that π_0 is a φ-state.

(2) Suppose that there is a self-loop in $Gr(S_\varphi)$. We prove that there is a contradiction.

Let s be a state with a self-loop. Since $s \in S_\varphi$, s satisfies φ. Since we are considering models with the nonstuttering condition, starting from s there is only one infinite path repeating s infinitely many times, and therefore s must be a φ_1 state or an S^*_φ state, contradicting to that s is in S_φ.

Therefore $Gr(S_\varphi)$ is a $\theta(\varphi_3)$-infinite directed graph. $\square$

Corollary 2. *Let $\varphi = \varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4) \in$* SL *be an* SL *formula with $\varphi_0, ..., \varphi_4$ being first order formulas. Let $(S, \sqsubseteq_\varphi) = po(Gr(S_\varphi))$. Then $(S, \sqsubseteq_\varphi)$ is $\theta(\varphi_3)$-well-founded, and furthermore, if $s, s' \in S_\varphi$ and $s \rightarrow s'$, then $s' \sqsubset_\varphi s$.*

Proof. This follows from Lemma 36 and Lemma 3. $\square$

Lemma 37. *Let $\varphi = \varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4) \in$* SL *be an* SL *formula with $\varphi_0, ..., \varphi_4$ being first order formulas. Then $Gr(S_\varphi)$ is $(\theta(\varphi_1) \cup S^*_\varphi)$-bounded.*

Proof.

Firstly, it is easily seen that $S_\varphi \cap (\theta(\varphi_1) \cup S^*_\varphi) = \emptyset$ from the definition.

Secondly, suppose that s is a state of S_φ. Since there are an s-path satisfying $\neg\varphi_1$ and an s-path satisfying $(\neg\varphi_2 U \neg\varphi_3) \wedge G\neg\varphi_4$, we have that s satisfies none of $\varphi_2 \wedge \varphi_3$, φ_1 and φ_4.

By Lemma 31, for every path π starting from s, we have $\pi^1 \models \varphi$. If π_1 is a state of φ_1, we are done. If π_1 is a state of $(\varphi_2 R \varphi_3) \vee F\varphi_4$, then it is a state of S^*_φ. Otherwise, there are an π_1-path satisfying $\neg\varphi_1$ and an π_1-path satisfying $(\neg\varphi_2 U \neg\varphi_3) \wedge G\neg\varphi_4$, and then π_1 is a state of S_φ.

Therefore $Gr(S_\varphi)$ is $(\theta(\varphi_1) \cup S^*_\varphi)$-bounded. □

Lemma 38. *Let $\varphi = \varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4) \in$ SL be an SL formula with $\varphi_0, ..., \varphi_4$ being first order formulas. Let $\eta_0 = \digamma(S_\varphi)$ and $\eta_6 = \digamma(S^*_\varphi)$. Then there are e, w, u and $\sqsubseteq$ such that the following hold.*

- $\eta_0, \neg\varphi_3 \models u^e_x$;
- $\eta_0 \models w^e_x \wedge (e = v \to [\varphi_1 \vee \eta_6 \vee (\eta_0 \wedge e \sqsubset v)])$;
- $(\{\sigma(x) \mid I(w)(\sigma)\}, \sqsubseteq)$ *is* $\{\sigma(x) \mid I(w \wedge u)(\sigma)\}$*-well-founded.*

Proof. This lemma follows from Lemma 21, with the following instantiation of S, Z, Y.

- $S = S_\varphi$.
- $Z = \theta(\varphi_3)$.
- $Y = \theta(\varphi_1) \cup S^*_\varphi$.

The conditions in Lemma 21 are ensured by Lemma 36 and Lemma 37. □

Remark It might be tempting to consider Lemma 34 as a special case of Lemma 38. However this is not the case, since φ_1 in the first lemma could be a UL formula and that in the second one is a first order formula.

Completeness The proof system is relatively complete for the set of simple LTL formulas. This is stated and proved as follows.

Theorem 2. *Let φ be an SL formula. If $\Gamma \models \varphi$, then $\Gamma \vdash \varphi$.*

Proof. Suppose that $\Gamma \models \varphi$ holds. If φ is a first order formula, we have $\Gamma \vdash \varphi$ by the relativeness condition. The rest of cases is proved by induction on the structure of φ as follows.

Case 1. $\varphi = X\varphi_1$.

The X-rule is applicable.

We prove that there is an η_1 such that the premises of the rule hold.

Let $\eta_1 = \digamma(\theta(\varphi_1))$.

We have $\eta_1 \vdash \varphi_1$. Since $\Gamma \models X\varphi_1$, by Lemma 14, we also have $\Gamma \models [\eta_1]$.

Case 2. $\varphi = \varphi_0 \wedge \varphi_1$.

The $\wedge$-rule is applicable.

We prove that $\Gamma \models \varphi_0$ and $\Gamma \models \varphi_1$ hold.

Let s be a Γ-state. Since s is a state of $\varphi_0 \wedge \varphi_1$, we have that s is a state of φ_0 and s is a state of φ_1.

Case 3. $\varphi = \varphi_0 \vee \varphi_1$.

Since φ is a simple LTL formula, we have the following cases: (1) φ_0 is a first order formula; (2) φ_1 is a first order formula.

We prove the first case, the other is similar.

In the first case, the $\vee$-rule is applicable.

We prove that there are η_0 and η_1 such that $\eta_0 \vdash \varphi_0$, $\eta_1 \vdash \varphi_1$ and $\Gamma \vdash \eta_0 \vee \eta_1$ hold.

Let $\eta_0 = \varphi_0$ and Let $\eta_1 = \digamma(\theta(\varphi_1))$.

It is easily seen that $\eta_0 \vdash \varphi_0$, $\eta_1 \vdash \varphi_1$ and $\Gamma \vdash \eta_0 \vee \eta_1$ hold.

Case 4. $\varphi = \varphi_0 R(\varphi_1, \varphi_2, \varphi_3, \varphi_4)$.

The R-rule is applicable.

We prove that there are $\eta_0, \eta_1, \eta_2, \eta_3, \eta_4, e, w$ and $\sqsubseteq$ such that the premises of the rule hold.

Let $\eta_0 = \digamma(\theta(\varphi_0))$.

Let $\eta_1 = \digamma(\theta(\varphi))$.

Let $\eta_2 = \digamma(S_{\varphi_2 U \varphi_3})$.

Let $\eta_3 = \varphi_3$.

Let $\eta_4 = \digamma(\theta(G\varphi_4))$.

Then the 1st, 2nd, 3rd, 4th and 9th premises hold trivially.

Since an η_1 state satisfies $\varphi_2 U \varphi_3$ and $G\varphi_4$, it satisfies η_4 and it either satisfies η_3 or satisfies η_2, and therefore the 5th premise holds.

Since an η_1 state is a φ state, if it is not an φ_0 state, every successor state of the state must be a φ state, and therefore the 6th premise holds.

Since an η_4 state is a $G\varphi_4$ state, every successor state of the state must be a $G\varphi_4$ state, and therefore the 7th premise holds.

By the construction of η_2, we have $\eta_2 \models \varphi_2$, and since η_3 is φ_3, by Lemma 34, there are e, w and $\sqsubseteq$ such that the 8th premise of the rule hold.

Case 5. $\varphi = \varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4)$.

We have two cases.

- φ is a UL formula, i.e., $\varphi_2 = \varphi_3 = \varphi_4 = \bot$, and $\varphi = \varphi_0 U \varphi_1$.
  The derived rule U_U is applicable.
  We prove that there are η_0, η_1, e, w and $\sqsubseteq$ such that the premises of the rule hold.
  Let $\eta_0 = \digamma(S_{\varphi_0 U \varphi_1})$.
  Let $\eta_1 = \digamma(\theta(\varphi_1))$.
  Then the 2nd premise holds trivially.

By the construction of η_0, we have $\eta_0 \models \varphi_0$, and by Lemma 34, there are e, w and $\sqsubseteq$ such that the 1st premise of the rule holds.
Let s be a state of Γ. Since s is a state of $\varphi_0 U \varphi_1$, s is either a state of φ_1 (i.e., a state of η_1) or a state of η_0. Therefore the 3rd premise holds.

- $\varphi_0, \varphi_1, \varphi_2, \varphi_3, \varphi_4$ are all first order formulas.
  The U-rule is applicable.
  We prove that there are $\eta_0, \eta_1, \eta_2, \eta_3, \eta_4, \eta_5, \eta_6, e, w, u, \sqsubseteq, e_1, w_1$ and $\sqsubseteq_1$ such that the premises of the rule hold.
  Let $\eta_0 = \digamma(S_\varphi)$.
  Let $\eta_i = \varphi_i$ for $i = 1, 2, 3, 4$.
  Let $\eta_5 = \digamma(\theta(\neg\varphi_4 \wedge F\varphi_4))$.
  Let $\eta_6 = \digamma(S_\varphi^*) = \digamma(\theta((\varphi_2 R \varphi_3) \vee F\varphi_4))$.
  Then the 1st, 2nd, 3rd, and 4th premises hold trivially.
  By the construction of η_6, if an η_6 state is not an φ_4 state and not an φ_2 state, then the successors of such a state must still be an η_6 state. Therefore the 5th premise holds.
  By the construction of η_6, if an η_6 state is not an φ_3 state, then it must be a $F\varphi_4$ state. Therefore the 6th premise holds.
  By the construction of η_0, η_1, η_3 and η_6, we have $\eta_0 \models \varphi_0$, and by Lemma 38, there are e, w, u and $\sqsubseteq$ such that the 7th and 8th premises of the rule holds.
  By the construction of η_5 and η_4, and Lemma 35, there are e_1, w_1 and $\sqsubseteq_1$ such that the 9th premise of the rule holds.
  Let s be a state of Γ. Since s is a state of $\varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4)$, s is either a state of η_1, a state of η_6, or a state of η_0. Therefore the 10th premise holds.

4.4 Examples

In this subsection, we provide an example showing the use of proof rules for satisfiability. The reader is referred to Appendix B for additional details.

Example 1. Let the program[2] be the one presented in Fig. 1. The transition relation are specified on the edges. For brevity, if a variable is not changed, the specification is omitted. The initial location is l_0 and the transition relation specified on the ingoing edge to l_0 may be interpreted as the condition (when the primed variables are replaced by the ordinary ones) for the initial states.

The program written as a first order Kripke structure is $M = (I, \rho, \Theta)$ over (B, V) where $B = (\{0, 1, 2, 3, 4, +, -\}, \{=, \geq\})$, $V = \{z, y\}$, and

- $I = (Int, I_0)$ is the usual interpretation where Int is the set of integers and I_0 maps the symbols of B into integers, functions over integers and relations over integers.

[2] A program is presented as a control-flow graph, with a set of locations, a set of edges and a set variables. The reader is referred to [30, 11] for details.

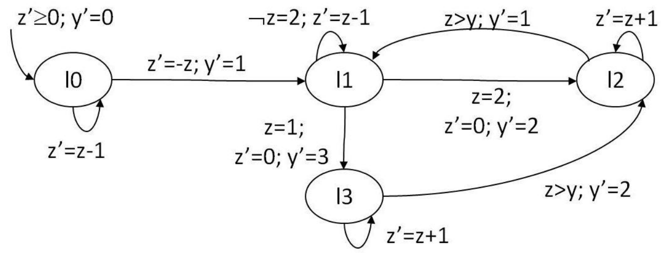

Fig. 1. The Program $P_1 = (\mathcal{L}_1, E_1, Vars_1)$

– ρ is the disjunction of the following formulas.

$$
\begin{array}{l}
(y = 0 \wedge y' = 1 \wedge z' = -z) \\
(y = 0 \wedge y' = 0 \wedge z' = z - 1) \\
(y = 1 \wedge (\neg z = 2) \wedge y' = 1 \wedge z' = z - 1) \\
(y = 1 \wedge z = 2 \wedge y' = 2 \wedge z' = 0) \\
(y = 1 \wedge z = 1 \wedge y' = 3 \wedge z' = 0) \\
(y = 2 \wedge z > y \wedge y' = 1 \wedge z' = z) \\
(y = 2 \wedge y' = 2 \wedge z' = z + 1) \\
(y = 3 \wedge z > y \wedge y' = 2 \wedge z' = z) \\
(y = 3 \wedge y' = 3 \wedge z' = z + 1)
\end{array}
$$

– $\Theta = (y = 0 \wedge z \geq 0)$.

Verification Goals Suppose that the verification goals are as follows.

$$
\begin{array}{l}
(1)\ M \models ((y = 0 \vee y = 1)\ U\ (y = 2, z = 2, y = 3 \vee z < 0, \bot)) \\
(2)\ M \models ((y = 1)\ R\ (y = 0 \vee y = 1, z > 0, z \leq 0, \top))
\end{array}
$$

The verification goals are reformulated as follows.

$$
\begin{array}{l}
(1')\ y = 0 \wedge z \geq 0 \models ((y = 0 \vee y = 1)\ U\ (y = 2, z = 2, y = 3 \vee z < 0, \bot)) \\
(2')\ y = 0 \wedge z \geq 0 \models ((y = 1)\ R\ (y = 0 \vee y = 1, z > 0, z \leq 0, \top))
\end{array}
$$

Accordingly, we may try to establish the following.

$$
\begin{array}{l}
(1'')\ y = 0 \wedge z \geq 0 \vdash ((y = 0 \vee y = 1)\ U\ (y = 2, z = 2, y = 3 \vee z < 0, \bot)) \\
(2'')\ y = 0 \wedge z \geq 0 \vdash ((y = 1)\ R\ (y = 0 \vee y = 1, z > 0, z \leq 0, \top))
\end{array}
$$

Proof of (1) For proving (1), we use the rule U with $\Gamma, \varphi_0, ..., \varphi_4$ instantiated to respectively $y = 0 \wedge z \geq 0$, $y = 0 \vee y = 1$, $y = 2$, $z = 2$, $y = 3 \vee z < 0$, $\bot$. Let

$\eta_0, ..., \eta_6, w, u, e, w_1, e_1$ be defined as follows.

$$
\begin{array}{|ll|}
\hline
\eta_0 : & (y = 0) \vee (y = 1 \wedge z \geq 0) \\
\eta_1 : & (y = 2) \\
\eta_2 : & (z = 2) \\
\eta_3 : & (y = 3 \vee z < 0) \\
\eta_4 : & \bot \\
\eta_5 : & \bot \\
\eta_6 : & (y = 3 \wedge z \leq 2) \vee (y = 1 \wedge z < 0) \\
w : & (even(x) \vee x \geq 0) \\
u : & (even(x) \wedge x < 0) \\
e : & (2 \cdot z + y) \\
w_1 : & (x \geq 0) \\
e_1 : & 0 \\
\hline
\end{array}
$$

Let $\sqsubseteq$ be defined as the following set of pairs.

$$\{(a, b) \mid even(b - a), a \leq b\} \cup \{(a, b) \mid odd(a), even(b)\}$$

It is easily seen that $w, u, \sqsubseteq$ define a weak-well-founded set.

let $\sqsubseteq_1$ be $\leq$. It is easily seen that $w_1, \sqsubseteq_1$ define a well founded set.

Let $\varphi(y, z)$ denote $(y = 3 \wedge z \leq 2) \vee (y = 1 \wedge z < 0))$, which is η_6 with y, z explicitly specified as the parameters. The computation of weakest precondition $[\eta_6]$ is shown as follows.

$$
\begin{array}{|l|}
\hline
[\eta_6] = \\
[(y = 3 \wedge z \leq 2) \vee (y = 1 \wedge z < 0)] = \\
\forall y'z'.(\rho \to (\varphi(y, z))') \wedge (\exists y'z'.\rho \vee \varphi(y, z)) = \\
\forall y'z'.(\rho \to (\varphi(y, z))') \wedge (0 \leq y \leq 3 \vee \varphi(y, z))) = \\
(y = 0 \to \varphi(1, -z)) \wedge (y = 0 \to \varphi(0, z - 1)) \wedge \\
(y = 1 \wedge z \neq 2 \to \varphi(1, z - 1)) \wedge \\
(y = 1 \wedge z = 2 \to (\varphi(2, 0)) \wedge (y = 1 \wedge z = 1 \to \varphi(3, 0)) \wedge \\
(y = 2 \wedge z > y \to \varphi(1, z)) \wedge (y = 2 \to \varphi(2, z + 1)) \wedge \\
(y = 3 \wedge z > y \to \varphi(2, z)) \wedge (y = 3 \to \varphi(3, z + 1)) \wedge \\
(0 \leq y \leq 3 \vee \varphi(y, z)) \\
\hline
\end{array}
$$

Let $\psi(y, z, v)$ denote $(2 \cdot z + y) \sqsubset v$, which is $e \sqsubset v$ with y, z, v explicitly specified as the parameters. The result of the computation of weakest precondition $[\eta_1 \vee \eta_6 \vee (\eta_0 \wedge e \sqsubset v)]$ is shown as follows.

$$
\begin{array}{|l|}
\hline
[\eta_1 \vee \eta_6 \vee (\eta_0 \wedge e \sqsubset v)] = \\
(y = 0 \to (z < 0) \vee (z \geq 0 \wedge \psi(-z, 1, v)) \wedge (y = 0 \to \psi(z - 1, 0, v)) \wedge \\
(y = 1 \wedge z \neq 2 \to (z < 1) \vee (z \geq 1 \wedge \psi(z - 1, 1, v)) \wedge \\
(y = 1 \wedge z = 2 \to \top) \wedge (y = 1 \wedge z = 1 \to \top) \wedge \\
(y = 2 \wedge z > y + 1 \to (z < 0) \vee (z \geq 0 \wedge \psi(z, 1, v))) \wedge (y = 2 \to \top) \wedge \\
(y = 3 \wedge z > y + 1 \to \top) \wedge (y = 3 \to (z < 1)) \wedge \\
(0 \leq y \leq 3 \vee \eta_1 \vee \eta_6 \vee (\eta_0 \wedge e \sqsubset v)) \\
\hline
\end{array}
$$

Then it is easily seen that the following hold.

$$\begin{aligned}
\eta_i &\models \varphi_i \ for \ i = 1, 2, 3, 4 \\
\eta_6, \neg\eta_2, \neg\eta_4 &\models [\eta_6] \\
\eta_6, \neg\eta_3 &\models \eta_5 \vee \eta_4 \\
\eta_0, \neg\eta_3 &\models \neg u_x^e \\
\eta_0 &\models \varphi_0 \wedge w_x^e \wedge (e = v \rightarrow ([\eta_1 \vee \eta_6 \vee (\eta_0 \wedge e \sqsubset v)])) \\
\eta_5 &\models (w_1)_x^{e_1} \wedge e_1 = v_1 \rightarrow [\eta_4 \vee (\eta_5 \wedge e_1 \sqsubset_1 v_1)]) \\
\Gamma &\models \eta_0 \vee \eta_1 \vee \eta_6
\end{aligned}$$

By the relativeness condition, we have

$$\begin{aligned}
\eta_i &\vdash \varphi_i \ for \ i = 1, 2, 3, 4 \\
\eta_6, \neg\eta_2, \neg\eta_4 &\vdash [\eta_6] \\
\eta_6, \neg\eta_3 &\vdash \eta_5 \vee \eta_4 \\
\eta_0, \neg\eta_3 &\vdash \neg u_x^e \\
\eta_0 &\vdash \varphi_0 \wedge w_x^e \wedge (e = v \rightarrow ([\eta_1 \vee \eta_6 \vee (\eta_0 \wedge e \sqsubset v)])) \\
\eta_5 &\vdash (w_1)_x^{e_1} \wedge e_1 = v_1 \rightarrow [\eta_4 \vee (\eta_5 \wedge e_1 \sqsubset_1 v_1)]) \\
\Gamma &\vdash \eta_0 \vee \eta_1 \vee \eta_6
\end{aligned}$$

Finally, by applying the rule U, we have the proof of the property.

Proof of (2) For proving (2), we use the rule R with $\Gamma, \varphi_0, ..., \varphi_4$ instantiated to respectively $y = 0 \wedge z \geq 0$, $y = 1$, $y = 0 \vee y = 1$, $z > 0$, $z \leq 0$, $\top$. Let $\eta_0, ..., \eta_4, w, e$ be defined as follows.

$\eta_0 :$	$(y = 1)$
$\eta_1 :$	$(y = 0 \vee y = 1)$
$\eta_2 :$	$(y = 0 \vee y = 1) \wedge (z \geq 0)$
$\eta_3 :$	$(z \leq 0)$
$\eta_4 :$	$\top$
$w :$	$(x \geq 0)$
$e :$	z

Let $\sqsubseteq$ be $\leq$. It is easily seen that $w, \sqsubseteq$ define a well founded set and the following hold.

$$\begin{aligned}
\eta_i &\models \varphi_i \ for \ i = 0, 1, 2, 3, 4 \\
\eta_1 &\models (\eta_2 \vee \eta_3) \wedge \eta_4 \\
\eta_1, \neg\eta_0 &\models [\eta_1] \\
\eta_4 &\models [\eta_4] \\
\eta_2 &\models w_x^e \wedge (e = v \rightarrow ([\eta_3 \vee (\eta_2 \wedge e \sqsubset v)])) \\
\Gamma &\models \eta_1
\end{aligned}$$

By the relativeness condition, we have the corresponding proofs of the above subgoals, and then by the rule R (together with the use of the rule $\wedge$), we have the proof of the property.

5 Proving Negative Satisfiability

In this section, a set of proof rules for negative satisfiability are developed. This set of rules is then proved to be sound and complete for SL formulas.

Definition 16. *$\Gamma \models_N \varphi$, if for every Γ-state s, there is an s-path satisfying $\neg\varphi$.*

This is the same as to say that a Γ state is not a φ state, and therefore the negative satisfiability is essentially the same as applying the existential interpretation to the negated LTL formula.

Proposition 2. *$M \not\models \varphi$ iff there is a satisfiable first order formula ϕ such that $\phi \models \Theta$ and $\phi \models_N \varphi$.*

This proposition is a consequence of the definitions of $M \models \varphi$ and $\Gamma \models_N \varphi$ (with Γ instantiated to $\{\phi\}$). In the following, we present a proof system for $\Gamma \models_N \varphi$.

Lemma 39. *Let η_0 and η_1 be first order formulas. Suppose that $\eta_0 \wedge [\eta_1] \to \eta_1$ holds. Then $\neg\eta_1 \models_N \eta_0 U \eta_1$ holds.*

Proof. Let $N_i = \theta(\neg\eta_i)$ for $i = 0, 1$.

By Lemma 16, $Gr(N_1 \setminus N_0)$ is an $(N_1 \cap N_0)$-weak-bounded subgraph.

Following from Lemma 13, we have $\neg\eta_1 \wedge \eta_0 \models_N \eta_0 U \eta_1$. Since it is easily seen that $\neg\eta_1 \wedge \neg\eta_0 \models_N \eta_0 U \eta_1$ holds, we have $\neg\eta_1 \models_N \eta_0 U \eta_1$. □

Lemma 40. *Let $\eta_0, \eta_1, w \in \mathcal{L}_B$ such that w is a formula with x as the only free variable. Let $e \in \mathcal{T}_B$, $\sqsubseteq$ be a binary relation symbol of P, and v be a variable not appearing in η_0, η_1, e, w. Let $W = \{\sigma(x) \mid I(w)(\sigma)\}$. Suppose that $(W, I_0(\sqsubseteq))$ with $W \subseteq D$ is a well-founded set, and $\forall v.(\neg\eta_0 \to (w^e_x \wedge ([(\eta_1 \wedge (e \sqsubset v \to \eta_0)] \to e \neq v))))$. Then $\neg\eta_0 \vee \neg\eta_1 \models_N (\eta_0 R \eta_1)$ hold.*

Proof. Let $N_i = \theta(\neg\eta_i)$ for $i = 0, 1$.

By Lemma 20, $Gr(N_0 \setminus N_1)$ is an N_1-terminating subgraph. Following from Lemma 11, we have $\neg\eta_0 \wedge \eta_1 \models_N X(\eta_0 R \eta_1)$. Since it implies $\neg\eta_0 \wedge \eta_1 \models_N (\eta_0 R \eta_1)$ and it is easily seen that $\neg\eta_0 \models_N (\eta_0 R \eta_1)$ holds, we have $\neg\eta_0 \vee \neg\eta_1 \models_N (\eta_0 R \eta_1)$. □

Proof Rules Let $B = (F, P)$ be given. Let e (possibly with subscripts) denote a term of the first order logic, w denote a first order formula with x as the only free variable, v denote a variable, η denote a first order formula, and $\sqsubseteq$ denote a binary relation symbol of P. Let ϕ_2, ϕ_3, ϕ_4 denote first order formulas. A set of reduction rules (referred to as NEG-rules) for the negative satisfiability is provided in Table 3.

For the application of the rule involving w, it is required that $w, \sqsubseteq$ define a well-founded set. Similar restriction applies to $w_1, \sqsubseteq_1, w_2, \sqsubseteq_2$ as well. In addition, v, v_1, v_2 are required to be variables not appearing in any places other than those explicitly specified in the rule.

Derived Rules For convenience, we formulate a set of derived rules for the unary operators F, G and the binary operators U, R. The rules are presented in Table 4. The explanation of the derivation is as follow.

$Rule$	$Origin$	$True$	$False$
$\bar{R}_R$	$\bar{R}$	$\phi_2, \phi_3, \phi_4, \eta_3, \eta_5$	
$\bar{U}_U$	$\bar{U}$	η_6, η_7	$\phi_2, \phi_3, \phi_4, \eta_5$
$\bar{R}_G$	$\bar{R}_R$		φ_0
$\bar{U}_F$	$\bar{U}_U$	φ_0, η_0	

Table 3. NEG Rules

$$N \quad \frac{\Gamma \vdash \neg\varphi}{\Gamma \vdash_N \varphi} \qquad \bar{X} \quad \frac{\neg\eta_1 \vdash_N \varphi_1 \qquad \Gamma, [\eta_1] \vdash \bot}{\Gamma \vdash_N X\varphi_1}$$

$$\bar{\wedge} \quad \frac{\neg\eta_0 \vdash_N \varphi_0 \qquad \neg\eta_1 \vdash_N \varphi_1 \qquad \Gamma \vdash \neg\eta_0 \vee \neg\eta_1}{\Gamma \vdash_N \varphi_0 \wedge \varphi_1} \qquad \bar{\vee} \quad \frac{\Gamma \vdash_N \varphi_0 \qquad \Gamma \vdash_N \varphi_1}{\Gamma \vdash_N \varphi_0 \vee \varphi_1}$$

$$\bar{R} \quad \frac{\begin{array}{rcl} \neg\eta_0 & \vdash_N & \varphi_0 \\ \neg\eta_1 & \vdash_N & \varphi_1 \\ \neg\eta_3, \phi_3 & \vdash & \bot \\ \phi_2, [\eta_3] & \vdash & \eta_3 \\ \neg\eta_0 & \vdash & (w_1)_x^{e_1} \wedge ([\eta_1 \wedge \eta_3 \wedge \eta_5 \wedge \phi_4 \wedge (e_1 \sqsubset_1 v_1 \to \eta_0)] \to e_1 \neq v_1) \\ \neg\eta_5 & \vdash & (w_2)_x^{e_2} \wedge ([\phi_4 \wedge (e_2 \sqsubset_2 v_2 \to \eta_5)] \to e_2 \neq v_2) \\ \Gamma, \eta_0, \eta_1, \eta_3, \eta_5, \phi_4 & \vdash & \bot \end{array}}{\Gamma \vdash_N \varphi_0 R(\varphi_1, \phi_2, \phi_3, \phi_4)}$$

$$\bar{U} \quad \frac{\begin{array}{rcl} \neg\eta_0 & \vdash_N & \varphi_0 \\ \neg\eta_1 & \vdash_N & \varphi_1 \\ \neg\eta_1, \eta_0, \eta_6, \phi_3 & \vdash & \bot \\ \neg\eta_1, \eta_5 & \vdash & \bot \\ \neg\eta_5, \phi_4 & \vdash & \bot \\ \neg\eta_1, \eta_7, \phi_3 & \vdash & \bot \\ \eta_0, [\eta_1] & \vdash & \eta_1 \\ [\eta_5] & \vdash & \eta_5 \\ \neg\eta_6 & \vdash & \neg(\eta_1 \vee \phi_2) \wedge (w_1)_x^{e_1} \wedge ([(\eta_1 \vee (\phi_3 \wedge \eta_0)) \wedge (e_1 \sqsubset_1 v_1 \to \eta_6)] \to e_1 \neq v_1) \\ \neg\eta_7 & \vdash & \neg(\eta_5 \vee \phi_2) \wedge (w_2)_x^{e_2} \wedge ([(\eta_5 \vee \phi_3) \wedge (e_2 \sqsubset_2 v_2 \to \eta_7)] \to e_2 \neq v_2) \\ \Gamma, \eta_1 & \vdash & \bot \end{array}}{\Gamma \vdash_N \varphi_0 U(\varphi_1, \phi_2, \phi_3, \phi_4)}$$

5.1 Soundness

In the following, we prove that the proof system is sound for SL formulas.

Lemma 41. *Let ψ be a* UL *formula. If $\pi \models \neg\psi$ and $\pi' \models \neg\psi$, then $\pi_0\pi' \models \neg\psi$.*

Proof. In case ψ is a first order formula, we have $\pi \models \neg\psi$ iff $\pi_0 \models \neg\psi$ iff $\pi_0\pi' \models \neg\psi$. The rest of cases is proved inductively as follows.

Table 4. NEG Derived Rules

$\bar{R}_G$	$\dfrac{\neg\eta_0 \vdash w_x^e \wedge ([\eta_1 \wedge (e \sqsubset v \to \eta_0)] \to e \neq v) \qquad \neg\eta_1 \vdash_N \varphi_1 \qquad \Gamma, \eta_0, \eta_1 \vdash \bot}{\Gamma \vdash_N G\varphi_1}$
$\bar{R}_R$	$\dfrac{\neg\eta_0 \vdash w_x^e \wedge ([\eta_1 \wedge (e \sqsubset v \to \eta_0)] \to e \neq v) \quad \neg\eta_0 \vdash_N \varphi_0 \quad \neg\eta_1 \vdash_N \varphi_1 \quad \Gamma, \eta_0, \eta_1 \vdash \bot}{\Gamma \vdash_N \varphi_0 R \varphi_1}$
$\bar{U}_F$	$\dfrac{\neg\eta_1 \vdash_N \varphi_1 \qquad [\eta_1] \vdash \eta_1 \qquad \Gamma, \eta_1 \vdash \bot}{\Gamma \vdash_N F\varphi_1}$
$\bar{U}_U$	$\dfrac{\neg\eta_0 \vdash_N \varphi_0 \qquad \neg\eta_1 \vdash_N \varphi_1 \qquad \eta_0, [\eta_1] \vdash \eta_1 \qquad \Gamma, \eta_1 \vdash \bot}{\Gamma \vdash_N \varphi_0 U \varphi_1}$

Case 1. $\psi = (\varphi U r)$ where φ is an SL formula and r is a first order formula.

By the premises, we have $\pi \models \neg\psi$ and $\pi' \models \neg\psi$. Then we have $\pi \models \neg r$ and therefore $\pi_0\pi' \models \neg r$. Together with $\pi' \models \neg\psi$, we have $\pi_0\pi' \models \neg\psi$.

Case 2. $\psi = (rU\psi_1)$ where r is a first order formula and ψ_1 is a UL formula.

By the premises, we have $\pi \models \neg\psi$ and $\pi' \models \neg\psi$. Then we have $\pi \models \neg\psi_1$ and $\pi' \models \neg\psi_1$. By the induction hypothesis, we have $\pi_0\pi' \models \neg\psi_1$, and together with $\pi' \models \neg\psi$, we have $\pi_0\pi' \models \neg\psi$.

Case 3. $\psi = (\psi_1 \vee r)$ where r is a first order formula and ψ_1 is a UL formula.

By the premises, we have $\pi \models \neg\psi$ and $\pi' \models \neg\psi$. Then we have $\pi \models \neg\psi_1 \wedge \neg r$ and $\pi' \models \neg\psi_1 \wedge \neg r$. Then we have $\pi_0\pi' \models \neg r$, and by the induction hypothesis, we have $\pi_0\pi' \models \neg\psi_1$, and therefore $\pi_0\pi' \models \neg\psi$.

Case 4. $\psi = (r \vee \psi_1)$ where r is a first order formula and ψ_1 is a UL formula.

This case is similar to the previous one. ☐

Lemma 42. *Let $\varphi U\psi$ be a* UL *formula. If $\pi \models \neg\psi$ and $\pi' \models \neg(\varphi U\psi)$, then $\pi_0\pi' \models \neg(\varphi U\psi)$.*

Proof. By the premises, we have $\pi \models \neg\psi$ and $\pi' \models \neg\psi$. Since ψ is a UL formula, by Lemma 41, $\pi_0\pi' \models \neg\psi$. Since we have $\pi' \models \neg(\varphi U\psi)$, we also have $\pi_0\pi' \models \neg(\varphi U\psi)$. ☐

Lemma 43. *The rule $\bar{U}_U$ is sound for* SL *formulas.*

Proof. Suppose that the premises of the rule hold. We prove $\Gamma \models_N \varphi_0 U\varphi_1$ as follows. In this case, $\varphi_0 U\varphi_1$ is a UL formula.

By the 3rd premise and Lemma 39, we have the following.

$$\neg\eta_1 \models_N \eta_0 U \eta_1$$

Let s be a Γ state.

By the 4th premise, s is a $\neg\eta_1$ state.

Then there is an s-path π such that either every state on the path is a $\neg\eta_1$ state or there is a $k \geq 0$ such that $\pi_0, ..., \pi_k$ are $\neg\eta_1$ states and π_k is a $\neg\eta_0$ state.

Since $\varphi_0 U \varphi_1$ is an SL formula, we have the following two cases.

- (1) φ_0 is an SL formula and φ_1 is a first order formula.
  By the 1st and 2nd premises, (i) every state on π is a $\neg\varphi_1$ state or (ii) there is a $k \geq 0$ such that $\pi_0, ..., \pi_k$ are $\neg\varphi_1$ states and there is a π_k-path π' (not necessarily the same as π^k) such that $\pi' \models \neg\varphi_0$.
  In the former case, π is an s-path satisfying $\neg(\varphi_0 U \varphi_1)$.
  In the latter case, $\pi_0 \cdots \pi_{k-1}\pi'$ is an s-path satisfying $\neg(\varphi_0 U \varphi_1)$.
- (2) φ_0 is a first order formula and φ_1 is a UL formula.
  By the 1st and 2nd premises, (i) starting from every state on π, there is a path (not necessarily a sub-path of π) satisfying $\neg\varphi_1$ or (ii) there is a $k \geq 0$ such that there is a π_i-path satisfying $\neg\varphi_1$ for every $i = 0, ..., k$ and π_k is a $\neg\varphi_0$ state.
  In the former case, by Lemma 28, $\pi \models G(\neg\varphi_1)$, and therefore $\pi \models \neg(\varphi_0 U \varphi_1)$.
  In the latter case, $\pi^k \models \neg(\varphi_0 U \varphi_1)$. By repeatedly using Lemma 42, we have $\pi^i \models \neg(\varphi_0 U \varphi_1)$ for $i = k-1, ..., 0$, and therefore $\pi \models \neg(\varphi_0 U \varphi_1)$.

$\square$

Soundness The proof system is sound for the set of simple LTL formulas. This is stated and proved as follows.

Theorem 3. *Let φ be an* SL *formula. If $\Gamma \vdash_N \varphi$, then $\Gamma \models_N \varphi$.*

Proof. We consider the NEG-rules case by case as follows.

Case 1. N.

Suppose $\Gamma \models \neg\varphi$. We prove $\Gamma \models_N \varphi$ as follows.

Let s be a Γ-state. Then for every s-path π we have $\pi \models \neg\varphi$. Therefore there is an s-path π such that $\pi \models \neg\varphi$.

Case 2. $\bar{\wedge}$.

Suppose that $\neg\eta_0 \models_N \varphi_0$, $\neg\eta_1 \models_N \varphi_1$, and $\Gamma \vdash \neg\eta_0 \vee \neg\eta_1$ hold. We prove $\Gamma \models_N \varphi_0 \wedge \varphi_1$ as follows.

Let s be a Γ-state. Then s is a state of $\neg\eta_0 \vee \neg\eta_1$. Then s is a state of $\neg\eta_0$ or s is a state of $\neg\eta_1$. Then there is an s-path π such that $\pi \models \neg\varphi_0$ or there is an s-path π' such that $\pi' \models \neg\varphi_1$.

Therefore there is an s-path satisfying $\neg\varphi_0 \vee \neg\varphi_1$, i.e., $\neg(\varphi_0 \wedge \varphi_1)$.

Case 3. $\bar{\vee}$.

Suppose that $\Gamma \models_N \varphi_0$ and $\Gamma \models_N \varphi_1$ hold. We prove $\Gamma \models_N \varphi_0 \vee \varphi_1$ as follows.

Let s be a Γ-state. Then there is an s-path π such that $\pi \models \neg\varphi_0$ and there is an s-path π' such that $\pi' \models \neg\varphi_1$.

Since $\varphi_0 \vee \varphi_1$ is an SL formula, φ_0 or φ_1 is a first order formula.

Assume that φ_0 is a first order formula (the other case being similar). Then $\pi' \models \neg\varphi_0 \wedge \neg\varphi_1$.

Therefore there is an s-path satisfying $\neg(\varphi_0 \vee \varphi_1)$.

Case 4. $\bar{X}$.

Suppose that we have $\neg\eta_1 \models_N \varphi_1$ and $\Gamma, [\eta_1] \models \bot$. We prove $\Gamma \models_N X\varphi_1$ as follows.

Let s be a Γ-state. Then not every s-successor is an η_1 state, i.e., there is an s-successor s' such that s' is a $\neg\eta_1$ state. Then there is an s'-path satisfying $\neg\varphi_1$. Therefore there is an s-path satisfying $X\neg\varphi_1$. Therefore there is an s-path satisfying $\neg X\varphi_1$.

Case 5. $\bar{R}$.

Suppose that the premises hold. We prove $\Gamma \models_N \varphi_0 R(\varphi_1, \phi_2, \phi_3, \phi_4)$ as follows.

By the 4th premise and Lemma 39, we have the following.

(i) $\neg\eta_3 \models_N \phi_2 U \eta_3$

By 3rd premise and (i), we have (i') $\neg\eta_3 \models_N \phi_2 U \phi_3$.

By the 5th premise, 6th premise, and Lemma 40, we have the following.

(ii) $\neg\eta_0 \vee \neg(\eta_1 \wedge \eta_3 \wedge \eta_5 \wedge \phi_4) \models_N (\eta_0 R(\eta_1 \wedge \eta_3 \wedge \eta_5 \wedge \phi_4))$
(iii) $\neg\eta_5 \vee \neg\phi_4 \models_N (\eta_5 R \phi_4)$

Let s be a Γ-state. We create an s-path satisfying $\neg\varphi_0 U(\neg\varphi_1 \vee (\neg\phi_2 R \neg\phi_3) \vee F\neg\phi_4)$ as follows. By the 7th premise, we have two cases.

- s is a $\neg\eta_1 \vee \neg\eta_3 \vee \neg\eta_5 \vee \neg\phi_4$ state.
  In case s is a $\neg\eta_1$ state, by the 2nd premise, there is an s-path π satisfying $\neg\varphi_1$. Then π is an s-path satisfying $\neg\varphi$.
  In case s is a $\neg\eta_3$ state, by (i'), there is an s-path π satisfying $\neg\phi_2 R \neg\phi_3$, and therefore $\pi \models \neg\varphi$.
  Otherwise, s is a $\neg\eta_5 \vee \neg\phi_4$ state.
  Then by (iii), there is an s-path π satisfying $(F\neg\phi_4)$. Then π is an s-path satisfying $\neg\varphi$.
- s is a $\neg\eta_0$ state.
  By (ii), there are an s-path π and a $k \geq 0$ such that $\pi_0, ..., \pi_{k-1}$ are $\neg\eta_0$ states and π_k is a $\neg\eta_1 \vee \neg\eta_3 \vee \neg\eta_5 \vee \neg\phi_4$ state.
  Similar to the previous case, we have a π_k-path π' satisfying $\neg\varphi$.
  By the 1st premise, $\pi_0, ..., \pi_{k-1}$ are $\neg\varphi_0$ states. Then $\pi_0 \cdots \pi_{k-1}\pi'$ is an s-path satisfying $\neg\varphi$ (since φ_0 is restricted to be a first order formula).

Case 6. $\bar{U}$.

Suppose that the premises hold. We prove $\Gamma \models_N \varphi_0 U(\varphi_1, \phi_2, \phi_3, \phi_4)$ as follows.

Let $\varphi = \varphi_0 U(\varphi_1, \phi_2, \phi_3, \phi_4)$.

If φ is a UL formula, i.e., $\phi_2 = \phi_3 = \phi_4 = \bot$, and $\varphi = \varphi_0 U \varphi_1$, then in this case, the soundness follows from that of $\bar{U}_U$ which has been handled by Lemma 43. Otherwise, φ is an SL formula where $\varphi_0, \varphi_1, \phi_2, \phi_3, \phi_4$ are all first order formulas.

By the 7th premise, 8th premise, and Lemma 39, we have the following.

(i) $\neg\eta_1 \models_N \eta_0 U \eta_1$
(ii) $\neg\eta_5 \models_N \top U \eta_5$

By the 5th premise and (ii), we have (ii') $\neg\eta_5 \models_N F\phi_4$.

By the second part of the 9th premise, the second part of the 10th premise, and Lemma 40, we have the following.

(iii) $\neg\eta_6 \vee \neg(\eta_1 \vee (\phi_3 \wedge \eta_0)) \models_N (\eta_6 R(\eta_1 \vee (\phi_3 \wedge \eta_0)))$
(iv) $\neg\eta_7 \vee \neg(\phi_3 \vee \eta_5) \models_N (\eta_7 R(\phi_3 \vee \eta_5))$

By the first part of the 10th premise, we have $\neg\eta_7 \vee \neg(\phi_3 \vee \eta_5) \models_N ((\phi_2 \vee \eta_5)R(\phi_3 \vee \eta_5))$. By the 5th premise, $\neg\eta_7 \vee \neg(\phi_3 \vee \eta_5) \models_N ((\phi_2 \vee \eta_5)R(\phi_3 \vee \eta_5))$ and $\neg\eta_5 \models_N F\phi_4$, we have the following.

(iv') $\neg\eta_7 \vee \neg(\phi_3 \vee \eta_5) \models_N ((\phi_2 R \phi_3) \vee F\phi_4)$.

Let s be a Γ state.

Let ψ denote $\neg\eta_0 R(\neg\eta_1 \wedge (\neg\phi_2 U \neg\phi_3) \wedge G\neg\phi_4)$. Since φ_0 and φ_1 are first order formulas, by the 1st and 2nd premises, it is sufficient to prove that there is an s-path satisfying ψ. We create such an s-path as follows.

By the 11th premise, s is a $\neg\eta_1$ state.

By (i), there is an s-path π such that either (1) there is a $k \geq 0$ such that $\pi_0, ..., \pi_k$ are $\neg\eta_1$ states and π_k is a $\neg\eta_0$ state, or (2) every state on the path is a $\neg\eta_1$ state. We have two cases.

– (1) There is a $k \geq 0$ such that $\pi_0, ..., \pi_k$ are $\neg\eta_1$ states and π_k is a $\neg\eta_0$ state. Without loss of generality, we may assume that $\pi_0, ..., \pi_{k-1}$ are η_0 states.
  By the 4th and 5th premises, $\pi_0, ..., \pi_k$ are $\neg\phi_4$ states.
  By the 3rd premise, $\pi_0, ..., \pi_{k-1}$ are $\neg\eta_6 \vee \neg\phi_3$ states.
  Then by the first part of the 9th premise, $\pi_0, ..., \pi_{k-1}$ are also $\neg\phi_2 \vee \neg\phi_3$ states.
  It is easily seen that: if we have (a) a π_k-path ζ such that $\zeta \models \neg\phi_3 \wedge G\neg\phi_4$ or (b) a π_k-path ζ such that $\zeta \models ((\neg\phi_2 U \neg\phi_3) \wedge G\neg\phi_4))$, then $\pi_0, ..., \pi_{k-1}\zeta \models \psi$. Then we consider two subcases.
  (1a) π_k is a $\neg\phi_3$ state.
  Since π_k is a $\neg\eta_1$ state, by the 4th premise, π_k is a $\neg\eta_5$ state. By (ii'), there is a π_k-path π' satisfying $\neg F\phi_4$. Then $\pi' \models \neg\phi_3 \wedge G\neg\phi_4$.

Since the condition (a) holds, there is an s-path satisfying ψ.
(1b) π_k is a ϕ_3 state.
By the 6th premise, π_k is a $\neg\eta_7$ state.
By (iv'), there is a π_k-path π' such that $\pi' \models ((\neg\phi_2 U \neg\phi_3) \wedge G\neg\phi_4)$.
Since the condition (b) holds, there is an s-path satisfying ψ.

- (2) Every state on the path is a $\neg\eta_1$ state .
Without loss of generality, we may assume that π_i is an η_0 state for all $i \geq 0$.
By the 3rd, 4th, 5th and 9th premises, π_i is also a $\neg\phi_4$ and $\neg\phi_2 \vee \neg\phi_3$ state for all $i \geq 0$.
If $\neg\phi_3$ appears infinitely many times, we are done.
Otherwise, there is a position j such that for all $i \geq j$, π_i satisfies ϕ_3.
Then by the 3rd premise, π_j is a $\neg\eta_6$ state.
By (iii), there are a π_j-path π' and a $k' \geq 0$ such that $\pi'_0, ..., \pi'_{k'-1}$ are $\neg\phi_2 \wedge \neg\eta_1$ states and $\pi'_{k'}$ is a $\neg\eta_1 \wedge \neg\phi_3$ state or a $\neg\eta_1 \wedge \neg\eta_0$ state.
We consider two subcases.
(2a) $\pi'_{k'}$ is a $\neg\eta_1 \wedge \neg\eta_0$ state.
Then we have an s-path $\pi'' = \pi_0 \cdots \pi_{j-1}\pi'$ such that all the states before the position $\pi'_{k'}$ are $\neg\eta_1$ states, and in addition, $\pi'_{k'}$ is a $\neg\eta_0$ state.
This is exactly the same as the situation considered in case (1), and by the analysis of case (1), there is an s-path satisfying ψ.
(2b) $\pi'_{k'}$ is a $\neg\eta_1 \wedge \neg\phi_3$ state.
Without loss of generality, we may assume that η_0 is satisfied on $\pi'_1, ..., \pi'_{k'}$.
Since $\pi'_0 = \pi_j$ and π_j is a ϕ_3 state, we have that $k' \geq 1$.
Then $\pi'_{k'}$ is used a new starting point replacing the original state s and the process of the construction of a path satisfying ψ is repeated.
The process either stops at a step where we have an s-path π satisfying ψ or it continues to infinity and we have an s-path π' such that every state on the path is a $\neg\eta_1 \wedge \eta_0$ state and $\neg\phi_3$ states appear infinitely many times.
In the former case, we are done.
In the latter case, by the 3rd, 4th, 5th and 9th premises, every state on π' also satisfies $\neg\phi_4$ and $\neg\phi_2 \vee \neg\phi_3$, and in addition $\neg\phi_3$ states appear infinitely many times. This means that π' is an s-path satisfying ψ.

□

5.2 Relative Completeness

In the following, we prove that the proof system is relatively complete for SL formulas.

Definition 17. *Let $\varphi = \varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4)$ and $\varphi' = \varphi_0 R(\varphi_1, \varphi_2, \varphi_3, \varphi_4)$. Then S^N_φ, $S^N_{\varphi'}$ and $S^{N*}_{\varphi'}$ are sets of states defined as follows.*

- *$s \in S^N_\varphi$, if s is a φ_0 state and a φ_3 state and not a φ state.*
- *$s \in S^{N*}_\varphi$, if s is a φ_3 state and not an S^*_φ state.*
- *$s \in S^N_{\varphi'}$, if s is a φ_1 state, a $(\varphi_2 U \varphi_3)$ state, a $G\varphi_4$ state, and not a φ' state.*

The set $S^N_{G\varphi_1}$, where $G\varphi_1$ is a special case of $\varphi_0 R(\varphi_1, \varphi_2, \varphi_3, \varphi_4)$, is defined according to $S^N_{\varphi'}$, that is, $S^N_{G\varphi_1}$ iff s is a φ_1 state and there is an s-path satisfying $\neg G\varphi_1$. It is easily seen that the following hold.

- If $s \in S^N_\varphi$, then s is not a φ_2 state and not a φ state.
- If $s \in S^{N*}_\varphi$, then s is not a φ_2 state and not an $F\varphi_4$ state.
- If $s \in S^N_{\varphi'}$, then s is not a φ_0 state.

Lemma 44. *Suppose that $\phi_0, ..., \phi_4 \in \mathcal{L}_{B,V}$. Let $\varphi = \phi_0 U(\phi_1, \phi_2, \phi_3, \phi_4)$ and $\varphi' = \phi_0 R(\phi_1, \phi_2, \phi_3, \phi_4)$.*

1. *Let $S_1 = S^N_\varphi$ and $Y_1 = \bar{\theta}(\varphi \vee (\phi_3 \wedge \phi_0))$.*
2. *Let $S_2 = S^{N*}_\varphi$ and $Y_2 = \bar{\theta}(\phi_3 \vee F\phi_4)$.*
3. *Let $S_3 = S^N_{\varphi'}$ and $Y_3 = \bar{\theta}(\phi_1) \cup \bar{\theta}(\phi_2 U \phi_3) \cup \bar{\theta}(G\phi_4)$.*

Then for $i \in \{1, 2, 3\}$, $Gr(S_i)$ is Y_i-terminating.

Proof. This lemma follows from the definitions of the respective sets of states in Definition 17. □

Lemma 45. *Suppose that $\varphi = \varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4)$ and $\varphi_0, ..., \varphi_4 \in \mathcal{L}_{B,V}$. Let $\eta_6 = \neg F(S^N_\varphi)$ and $\eta_1 = F(\theta(\varphi))$. Then there are e, w and $\sqsubseteq$ such that they define a well-founded set and*

$$\neg\eta_6 \models w^e_x \wedge (([(\eta_1 \vee (\varphi_3 \wedge \varphi_0)) \wedge (e \sqsubset v \to \eta_6)] \to e \neq v)).$$

Proof. This lemma follows from Lemma 23, with the following instantiation of S and Y.

- $S = S^N_\varphi$ and $F(S) = F(S^N_\varphi) = \neg\eta_6$.
- $Y = \bar{\theta}(\varphi \vee (\varphi_3 \wedge \varphi_0))$ and $F(Y) = \neg(\eta_1 \vee (\varphi_3 \wedge \varphi_0))$.

The conditions in Lemma 23 are ensured Lemma 44(1). □

Lemma 46. *Suppose that $\varphi = \varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4)$ and $\varphi_0, ..., \varphi_4 \in \mathcal{L}_{B,V}$. Let $\eta_7 = \neg F(S^{N*}_\varphi)$ and $\eta_5 = F(\theta(F\varphi_4))$. Then there are e, w and $\sqsubseteq$ such that they define a well-founded set and*

$$\neg\eta_7 \models w^e_x \wedge (([(\eta_5 \vee \varphi_3) \wedge (e \sqsubset v \to \eta_7)] \to e \neq v)).$$

Proof. This lemma follows from Lemma 23, with the following instantiation of S and Y.

- $S = S^{N*}_\varphi$ and $F(S) = F(S^{N*}_\varphi) = \neg\eta_7$.
- $Y = \bar{\theta}(\varphi_3 \vee F\varphi_4)$ and $F(Y) = \neg(\varphi_3 \vee \eta_5)$.

The conditions in Lemma 23 are ensured Lemma 44(2). □

Lemma 47. *Suppose that* $\varphi = \varphi_0 R(\varphi_1, \varphi_2, \varphi_3, \varphi_4)$ *and* $\varphi_0, ..., \varphi_4 \in \mathcal{L}_{B,V}$. *Let* $\eta_0 = \neg F(S^N_\varphi)$, $\eta_3 = F(\theta(\varphi_2 U \varphi_3))$, *and* $\eta_5 = F(\theta(\neg\varphi_4 \vee G\varphi_4))$. *Then there are* e, w *and* $\sqsubseteq$ *such that they define a well-founded set and*

$$\neg\eta_0 \models w^e_x \wedge (([\varphi_1 \wedge \eta_3 \wedge \eta_5 \wedge \varphi_4 \wedge (e \sqsubset v \to \eta_0)] \to e \neq v)).$$

Proof. This lemma follows from Lemma 23, with the following instantiation of S and Y.

- $S = S^N_\varphi$ and $F(S) = F(S^N_\varphi) = \neg\eta_0$.
- $Y = \bar{\theta}(\varphi_1) \cup \bar{\theta}(\varphi_2 U \varphi_3) \cup \bar{\theta}(G\varphi_4)$ and $F(Y) = \neg(\varphi_1 \wedge \eta_3 \wedge \eta_5 \wedge \varphi_4)$.

We have that $\eta_5 \wedge \varphi_4$ is a representation of the set of $G\varphi_4$ states. The conditions in Lemma 23 are ensured Lemma 44(3). □

Lemma 48. *Suppose that* $\varphi = G\varphi_1$ *is an* SL *formula and* $\varphi_1 \in \mathcal{L}_{B,V}$. *Let* $\eta_0 = \neg F(S^N_{G\varphi_1})$. *Then there are* e, w *and* $\sqsubseteq$ *such that they define a well-founded set and*

$$\neg\eta_0 \models w^e_x \wedge ([\varphi_1 \wedge (e \sqsubset v \to \eta_0)] \to e \neq v).$$

Proof. This lemma is a special case of Lemma 47, with $\varphi_0, \varphi_2, \varphi_3, \varphi_4$ replaced by $\top$. □

Completeness The proof system is relatively complete for the set of simple LTL formulas. This is stated and proved as follows.

Theorem 4. *Let* φ *be an* SL *formula. If* $\Gamma \models_N \varphi$, *then* $\Gamma \vdash_N \varphi$.

Proof by induction on the structure of φ. Suppose that $\Gamma \models_N \varphi$ holds.

Case 1. φ is a first order formula.

The N-rule is applicable.
We have $\Gamma \models_N \varphi$ iff $\Gamma \models \neg\varphi$. Then we have $\Gamma \vdash \neg\varphi$ by the relativeness condition.

Case 2. $\varphi = X\varphi_1$.

The $\bar{X}$-rule is applicable.
We prove that there is an η_1 such that the premises of the rule hold.
Let $\eta_1 = F(\theta(\varphi_1))$.
Then the first premise holds.
Suppose that s is a Γ state.
Then there is an s-path satisfying $X\neg\varphi_1$.
Then there is an s-successor which is not a φ_1 state and therefore s is not an $[\eta_1]$ state.
Therefore the second premise holds.

Case 3. $\varphi = \varphi_0 \wedge \varphi_1$.

The $\bar{\wedge}$-rule is applicable.
Let $\eta_0 = \digamma(\theta(\varphi_0))$ and $\eta_1 = \digamma(\theta(\varphi_0))$.
Then the first and the second premises hold.
Suppose that s is a Γ state.
Then there is an s-path satisfying $\neg(\varphi_0 \wedge \varphi_1)$.
Then there is an s-path satisfying $\neg\varphi_0$ or satisfying $\neg\varphi_1$.
Then s is a state of $\neg\eta_0$ or a state of $\neg\eta_1$.
Therefore s is a state of $\neg\eta_0 \vee \neg\eta_1$.
Therefore the third premise holds.

Case 4. $\varphi = \varphi_0 \vee \varphi_1$.

The $\bar{\vee}$-rule is applicable.
We prove that $\Gamma \vdash_N \varphi_0$ and $\Gamma \vdash_N \varphi_1$ hold.
Suppose that s is a Γ state.
Then there is an s-path satisfying $\neg(\varphi_0 \vee \varphi_1)$.
Then there is an s-path satisfying $\neg\varphi_0$ and $\neg\varphi_1$.
Then there is an s-path satisfying $\neg\varphi_0$ and there is an s-path satisfying $\neg\varphi_1$.
Therefore $\Gamma \vdash_N \varphi_0$ and $\Gamma \vdash_N \varphi_1$ hold.

Case 5. $\varphi = \varphi_0 R(\varphi_1, \phi_2, \phi_3, \phi_4)$.

The $\bar{R}$-rule is applicable.

We prove that there are $\eta_0, \eta_1, \eta_3, \eta_5, e, w$ and $\sqsubseteq$ such that the premises of the rule hold.

Let $\eta_0 = \neg\digamma(S^N_\varphi)$.
Let $\eta_5 = \neg\digamma(S^N_{G\phi_4}) = \digamma(\theta(\neg\phi_4 \vee G\phi_4))$.
Let $\eta_1 = \digamma(\theta(\varphi_1))$.
Let $\eta_3 = \digamma(\theta(\phi_2 U \phi_3))$.
It is easily seen that the 1st, 2nd, 3rd and the 7th premises hold.

Since η_3 is the representation of the set of $\phi_2 U \phi_3$ states, every state that is both a ϕ_2 state and has all the successors in η_3 is also in η_3. Therefore the 4th premise holds.

Regarding the 5th premise, by Lemma 47, there are e_1, w_1 and $\sqsubseteq_1$ such that $\neg\eta_0 \vdash (w_1)^{e_1}_x \wedge ([(\eta_1 \wedge \eta_3 \wedge \eta_5 \wedge \phi_4) \wedge (e_1 \sqsubset_1 v_1 \rightarrow \eta_0)] \rightarrow e_1 \neq v_1)$.

Regarding the 6th premise, by Lemma 48, there are e_2, w_2 and $\sqsubseteq_2$ such that $\neg\eta_5 \models (w_2)^{e_2}_x \wedge ([\phi_4 \wedge (e_2 \sqsubset_2 v_2 \rightarrow \eta_5)] \rightarrow e_2 \neq v_2)$.

Case 6. $\varphi = \varphi_0 U(\varphi_1, \phi_2, \phi_3, \phi_4)$.

The $\bar{U}$-rule is applicable.

We prove that there are $\eta_0, \eta_1, \eta_5, \eta_6, \eta_7, e_1, e_2, w_1, w_2, \sqsubseteq_1$ and $\sqsubseteq_2$ such that the premises of the rule hold.

Let $\eta_0 = \digamma(\theta(\varphi_0))$.
Let $\eta_1 = \digamma(\theta(\varphi))$.
Let $\eta_5 = \digamma(\theta(F\varphi_4))$.
Let $\eta_6 = \neg\digamma(S^N_\varphi)$.

Let $\eta_7 = \neg F(S_\varphi^{N*})$.

It is easily seen that the 1st, 2nd, 3rd, 4th, 5th, 6th and 11th premises hold.

Since η_1 is the representation of the set of φ states, every state that is both an η_0 state and has all the successors in η_1 is also in η_1. Therefore the 7th premise holds.

Since η_5 is the representation of the set of $F\phi_4$ states, every state that has all the successors in η_5 is also in η_5. Therefore the 8th premise holds.

Regarding the 9th premise, it is easily seen that we have $\neg\eta_6 \vdash \neg(\eta_1 \vee \phi_2)$, and by Lemma 45, there are e_1, w_1 and $\sqsubseteq_1$ such that $\neg\eta_6 \vdash (w_1)_x^{e_1} \wedge ([(\eta_1 \vee (\phi_3 \wedge \eta_0) \wedge (e_1 \sqsubset_1 v_1 \to \eta_6)] \to e_1 \neq v_1)$.

Regarding the 10th premise, it is easily seen that we have $\neg\eta_7 \vdash \neg(\eta_5 \vee \phi_2)$, and by Lemma 46, there are e_2, w_2 and $\sqsubseteq_2$ such that $\neg\eta_7 \vdash (w_2)_x^{e_2} \wedge ([(\phi_3 \vee \eta_5) \wedge (e_2 \sqsubset_2 v_2 \to \eta_7)] \to e_2 \neq v_2)$. □

5.3 Examples

In this subsection, we provide an example showing the use of proof rules for negative satisfiability. The reader is referred to Appendix B for additional details.

Example 2. Let the program be the one presented in Fig. 2. This program can be considered as a simplification of the one in Example 1.

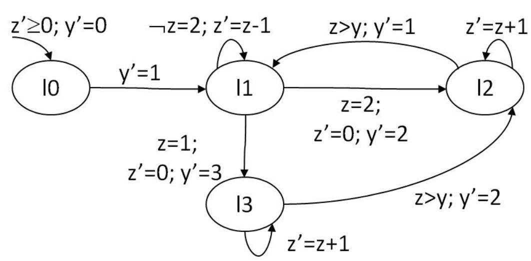

Fig. 2. The Modified Program $P_1' = (\mathcal{L}_1, E_1', Vars_1)$

Verification Goals Suppose that the verification goals are as follows.

$$(1)\ M \not\models ((y \neq 3)\ U\ (z < 0, z < 0, y \neq 2, \bot))$$
$$(2)\ M \not\models ((y = 2 \vee y = 3)\ R\ (y \neq 3, y \neq z, z > y, \top))$$

The verification goals are reformulated as follows.

$$(1')\ y = 0 \wedge z > 0 \models_N ((y \neq 3)\ U\ (z < 0, z < 0, y \neq 2, \bot))$$
$$(2')\ y = 0 \wedge z > 0 \models_N ((y = 2 \vee y = 3)\ R\ (y \neq 3, y \neq z, z > y, \top))$$

Accordingly, we may try to establish the following.

$(1'')\ y = 0 \wedge z > 0 \vdash_N ((y \neq 3)\ U\ (z < 0, z < 0, y \neq 2, \perp))$
$(2'')\ y = 0 \wedge z > 0 \vdash_N ((y = 2 \vee y = 3)\ R\ (y \neq 3, y \neq z, z > y, \top))$

Notice that we have $\Theta = (y = 0 \wedge z \geq 0)$ and $(y = 0 \wedge z > 0) \to \Theta$.

Proof of (1) For proving (1), we use the rule $\bar{U}$ with $\Gamma, \varphi_0, \varphi_1, \phi_2, \phi_3, \phi_4$ instantiated to respectively $y = 0 \wedge z > 0$, $y \neq 3$, $z < 0$, $z < 0$, $y \neq 2$, $\perp$. In order to conveniently define e_1, we have to extend F with a new symbol e_0 with the following interpretation (the reader is referred to Section 6.3 for a discussion on the use of new symbols):

$e_0(z, y) =$ if $(y < 3 \vee z > 3)$ then $3 + z - y$; else $3 - z$.

Let $\eta_0, \eta_1, \eta_5, \eta_6, \eta_7, w_1, e_1, w_2, e_2$ be defined as follows.

$\eta_0:$	$(y \neq 3)$
$\eta_1:$	$\neg(((y = 0 \vee y = 1) \wedge (z > 0)) \vee ((y = 3 \vee y = 2) \wedge (z \geq 0)))$
$\eta_5:$	$\perp$
$\eta_6:$	$\neg(y = 0 \vee y = 1) \wedge (z > 0)$
$\eta_7:$	$\neg(((y = 0 \vee y = 1) \wedge (z > 0)) \vee ((y = 3) \wedge (z \geq 0)))$
$w_1:$	$x \geq 0$
$e_1:$	$z - y$
$w_2:$	$x \geq 0$
$e_2:$	$e_0(z, y)$

Let $\sqsubseteq_1$ and $\sqsubseteq_2$ be $\leq$. It is easily seen that $w_i, \sqsubseteq_i$ define a well-founded set for $i = 1, 2$ and the premises of the rule hold. By the relativeness condition, we have the corresponding proofs of the premises (as subgoals), and then by the rule $\bar{U}$, we have the proof of the property.

Proof of (2) For proving (2), we use the rule $\bar{R}$ with $\Gamma, \varphi_0, \varphi_1, \phi_2, \phi_3, \phi_4$ instantiated to respectively $y = 0 \wedge z > 0$, $y = 2 \vee y = 3$, $y \neq 3$, $z \neq y$, $z > y$, $\top$. Let $\eta_0, \eta_1, \eta_3, \eta_5, w_1, e_1, w_2, e_2$ be defined as follows.

$\eta_0:$	$\neg((y = 0 \vee y = 1) \wedge (z > 0))$
$\eta_1:$	$\neg(y \neq 3)$
$\eta_3:$	$(z > y)$
$\eta_5:$	$\top$
$w_1:$	$(x \geq 0)$
$e_1:$	$(z - y)$
$w_2:$	$(x \geq 0)$
$e_2:$	0

Let $\sqsubseteq_1$ and $\sqsubseteq_2$ be $\leq$. It is easily seen that $w_i, \sqsubseteq_i$ define a well-founded set for $i = 1, 2$ and the premises of the rule hold. By the relativeness condition, we have the corresponding proofs of the premises (as subgoals), and then by the rule $\bar{R}$, we have the proof of the property.

6 CTL* Formulas

Let (B, V) be given. In the following, we present a first order CTL*. The logic was introduced in [8, 12, 13] and the following presentation is similar to the one in [11].

Syntax Let ϕ range over $\mathcal{L}_{B,V}$. The set of CTL* formulas over (B, V) is defined as follows.

$$\begin{aligned} \Phi ::= {} & \phi \mid \neg\Phi \mid \Phi \wedge \Phi \mid \Phi \vee \Phi \mid \Phi \to \Phi \mid \\ & X\,\Phi \mid F\,\Phi \mid G\,\Phi \mid \Phi\,U\,\Phi \mid \Phi\,R\,\Phi \mid E\Phi \mid A\Phi \end{aligned}$$

The operators X, F, G, U, R are called temporal operators, while E and A are called path quantifiers.

Semantics Let the first order Kripke structure $M = \langle I, \rho, \Theta \rangle$ over (B, V) be given.

Definition 18. *Let π denote an infinite path of M. Let φ (possibly with subscripts) denote a CTL* formula. That the path π satisfies φ, denoted $\pi \models_M \varphi$, or simply $\pi \models \varphi$ when M is understood in the context, is defined as follows.*

$\pi \models \varphi$	*if* $\varphi \in \mathcal{L}_{B,V}$ *and* $I(\varphi)(\pi_0) = true$
$\pi \models \neg\varphi$	*if* $\pi \not\models \varphi$
$\pi \models \varphi_0 \vee \varphi_1$	*if* $\pi \models \varphi_0$ *or* $\pi \models \varphi_1$
$\pi \models \varphi_0 \wedge \varphi_1$	*if* $\pi \models \varphi_0$ *and* $\pi \models \varphi_1$
$\pi \models \varphi_0 \to \varphi_1$	*if* $\pi \models \varphi_0$ *then* $\pi \models \varphi_1$
$\pi \models X\varphi$	*if* $\pi^1 \models \varphi$
$\pi \models G\varphi$	*if* $\forall i \geq 0.(\pi^i \models \varphi))$
$\pi \models F\varphi$	*if* $\exists i \geq 0.(\pi^i \models \varphi))$
$\pi \models \varphi_0 U \varphi_1$	*if* $\exists i \geq 0.((\pi^i \models \varphi_1) \wedge \forall j < i.(\pi^j \models \varphi_0))$
$\pi \models \varphi_0 R \varphi_1$	*if* $\forall i \geq 0.(\forall j < i.(\pi^j \not\models \varphi_0) \to (\pi^i \models \varphi_1))$
$\pi \models E\varphi$	*if* $\exists \pi'(\pi_0).(\pi' \models \varphi)$
$\pi \models A\varphi$	*if* $\forall \pi'(\pi_0).(\pi' \models \varphi)$

In addition, we may use the two quinary operators U and R, with the following interpretation.

$$\varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4) \equiv \varphi_0 U(\varphi_1 \vee (\varphi_2 R \varphi_3) \vee F\varphi_4)$$
$$\varphi_0 R(\varphi_1, \varphi_2, \varphi_3, \varphi_4) \equiv \varphi_0 R(\varphi_1 \wedge (\varphi_2 U \varphi_3) \wedge G\varphi_4)$$

Definition 19. *$M \models \varphi$, if $\pi \models \varphi$ for every computation $\pi \in [[M]]$.*

The usual definition of CTL* has a distinction on path formulas and state formulas. Although state formulas are special path formulas, state formulas are used as the primary concept for specification of properties of models. In the above definition, we consider CTL* as an extension of LTL and we do not make a distinction of path formulas and state formulas.

Normal Form A CTL* formula is in the negation normal form (NNF), if the negation $\neg$ is applied only to first order formulas and the formula does not contain the symbol $\rightarrow$. Let NNF(X,U,R,E,A) denote the set of NNF formulas with temporal operators only in $\{X, U, R\}$ where U, R are the two quaternary operators. Let ϕ range over $\mathcal{L}_{B,V}$. The set of NNF(X,U,R,E,A) formulas is defined as follows.

$$\Phi ::= \phi \mid \Phi \wedge \Phi \mid \Phi \vee \Phi \mid X\ \Phi \mid \Phi\ U\ (\Phi, \Phi, \Phi, \Phi) \mid \Phi\ R\ (\Phi, \Phi, \Phi, \Phi) \mid E\Phi \mid A\Phi$$

Every CTL* formula can be transformed into an equivalent one in NNF(X,U,R,E,A). Then without loss of generality, we only consider NNF(X,U,R,E,A) formulas. Formulas not in such a form are considered as an abbreviation of the equivalent ones in NNF(X,U,R,E,A).

6.1 A Proof System

A CTL* formula can be viewed as a generalized LTL formula such that a place for holding a first order formulas in LTL may be used to hold a formula of the forms $E\varphi$ and $A\varphi$. With this view, the relevant definitions regarding LTL can be adapted for CTL*, and we can reuse the RED-rules and NEG-rules presented previously for proving satisfiability and negative satisfiability. That remains is to formulate proof rules for proof goals of the following forms.

$$\begin{array}{l} \Gamma \ \models \ E\varphi \\ \Gamma \ \models \ A\varphi \\ \Gamma \models_N E\varphi \\ \Gamma \models_N A\varphi \end{array}$$

For this purpose, a set of reduction rules are provided in Table 5. The reduction rules are used to reduce a proof of a formula to proofs of simpler ones (by using the rules backwards).

Table 5. Proof Rules: PATH

E	$\dfrac{\Gamma \vdash_N \neg\varphi}{\Gamma \vdash E\varphi}$	A	$\dfrac{\Gamma \vdash \varphi}{\Gamma \vdash A\varphi}$
$\bar{E}$	$\dfrac{\Gamma \vdash \neg\varphi}{\Gamma \vdash_N E\varphi}$	$\bar{A}$	$\dfrac{\Gamma \vdash_N \varphi}{\Gamma \vdash_N A\varphi}$

The Proof System The proof system consists of the set of PATH-rules, the set of RED-rules and the set of NEG-rules in which LTL formulas are replaced by CTL* formulas.

6.2 Soundness and Completeness

Let ϕ range over $\mathcal{L}_{B,V}$. The subset of CTL*, denoted SC, called simple CTL* formulas, is defined as follows, with UC and Φ being auxiliary subsets of SC.

$$
\begin{array}{lll}
\mathrm{SC} & ::= & \mathrm{SC} \vee \Phi \mid \Phi \vee \mathrm{SC} \mid \mathrm{SC} \wedge \mathrm{SC} \mid X(\mathrm{SC}) \mid \Phi\, R\,(\mathrm{SC}, \Phi, \Phi, \Phi) \mid \Phi\, U(\Phi, \Phi, \Phi, \Phi) \mid \mathrm{UC} \\
\mathrm{UC} & ::= & \Phi \mid \mathrm{SC}\, U\,(\Phi) \mid \Phi\, U\,(\mathrm{UC}) \mid \mathrm{UC} \vee \Phi \mid \Phi \vee \mathrm{UC} \\
\Phi & ::= & \phi \mid E(\mathrm{SC}) \mid A(\mathrm{SC})
\end{array}
$$

Lemma 49. *The following hold.*

- $\Gamma \models E\varphi$ *iff* $\Gamma \models_N \neg\varphi$.
- $\Gamma \models A\varphi$ *iff* $\Gamma \models \varphi$.
- $\Gamma \models_N E\varphi$ *iff* $\Gamma \models \neg\varphi$.
- $\Gamma \models_N A\varphi$ *iff* $\Gamma \models_N \varphi$.

Proof. These equivalences follows from the definition. □

Soundness The proof system is sound for the set of simple CTL* formulas. This is stated and proved as follows.

Theorem 5. *Let φ be an* SC *formula. If $\Gamma \vdash \varphi$, then $\Gamma \models \varphi$.*

Proof. Due to that there is an interchange between proofs of the forms $\Gamma \vdash \varphi$ and $\Gamma \vdash_N \varphi$ caused by the use of PATH-rules, we strengthen the statement to be the conjunction of the following.

$$
\begin{array}{l}
\text{If } \Gamma \vdash \varphi \text{ then } \Gamma \models \varphi; \\
\text{If } \Gamma \vdash_N \varphi \text{ then } \Gamma \models_N \varphi.
\end{array}
$$

The strengthened statement is proved by showing that every proof rule is sound. For the PATH-rules, the soundness follows from Lemma 49. For the RED-rules and NEG-rules, the reasoning is similar to that of LTL formulas, and is omitted. □

Completeness The proof system is relatively complete for the set of simple CTL* formulas. This is stated and proved as follows.

Theorem 6. *Let φ be an* SC *formula. If $\Gamma \models \varphi$, then $\Gamma \vdash \varphi$.*

Proof. Due to that there is an interchange between proofs of the forms $\Gamma \vdash \varphi$ and $\Gamma \vdash_N \varphi$ caused by the use of PATH-rules, we strengthen the statement to be the conjunction of the following.

$$
\begin{array}{l}
\text{If } \Gamma \models \varphi \text{ then } \Gamma \vdash \varphi; \\
\text{If } \Gamma \models_N \varphi \text{ then } \Gamma \vdash_N \varphi.
\end{array}
$$

The strengthened statement is proved by induction on the structure of φ. For the cases where proof-goals are in the forms of $\Gamma \models E\varphi$, $\Gamma \models A\varphi$, $\Gamma \models_N E\varphi$ and $\Gamma \models_N A\varphi$, the PATH-rules can be used, and the completeness of using these rules follows from Lemma 49. The other forms of proof-goals are handled by RED-rules and NEG-rules, and the reasoning is similar to that of LTL formulas. □

6.3 Discussion on the Use of Symbols

Since the formulation of the auxiliary constructs for the application of the proof rules requires the use of symbols from B, we may have to extend B and interpreted the extra symbols by extending I, in order to be able to formulate appropriate auxiliary constructs.

Let (B, V) be given. Let I be an interpretion of B.

Suppose that $M = \langle I, \rho, \Theta \rangle$ is a Kripke structure over (B, V) and φ is a CTL* formula over (B, V).

Let $M' = \langle I', \rho, \Theta \rangle$ be a Kripke structure over (B', V) where $B' = (F', P')$ is an extension of B and $I' = (D, I'_0)$ is an extension of I. Then the following holds.

Proposition 3. *Let φ be a CTL* formula over (B, V). $M \models \varphi$ iff $M' \models \varphi$.*

This proposition follows from an inductive argument on the structure of formulas, and provides a basis for adding a user-defined theory to the initial first order logic $\mathcal{L}_B$ in order to be able to make convenient formulation of necessary assertions.

7 CTL†

We define a subset of CTL* and present a customized proof system for this subset of CTL*.

Syntax Let ϕ range over $\mathcal{L}_{B,V}$. The set of CTL† formulas over (B, V) is defined as follows.

$$\Phi ::= \phi \mid \neg\Phi \mid \Phi \wedge \Phi \mid AX\,\Phi \mid A(\Phi\, U\,(\Phi, \Phi, \Phi, \Phi)) \mid A(\Phi\, R\,(\Phi, \Phi, \Phi, \Phi))$$

Semantics Let the first order Kripke structure $M = \langle I, \rho, \Theta \rangle$ over (B, V) be given. The semantics of CTL† inherits from that of CTL*. In addition, we have the following definition.

Definition 20. *Let s be a state. $s \models_M \varphi$ (or simply, $s \models \varphi$, when M is understood in the context), if $\pi \models \varphi$ for every s-path π of M.*

Let $sl_U(\pi, \varphi_0, \varphi_1, \varphi_2, \varphi_3, \varphi_4)$ denote the following.

$$\begin{array}{l}
\exists i \geq 0.((\forall j < i.(\pi_j \models \varphi_0)) \wedge (\\
(\pi_i \models \varphi_1) \vee \\
\forall k \geq i.(\forall j \in \{i, ..., k-1\}.(\pi_j \not\models \varphi_2) \rightarrow (\pi_k \models \varphi_3)) \vee \\
\exists k \geq i.(\pi_k \models \varphi_4))).
\end{array}$$

Let $sl_R(\pi, \varphi_0, \varphi_1, \varphi_2, \varphi_3, \varphi_4)$ denote $\neg sl_U(\pi, \neg\varphi_0, \neg\varphi_1, \neg\varphi_2, \neg\varphi_3, \neg\varphi_4)$.

Lemma 50. *Let s be a state. Let φ (possibly with subscripts) denote a CTL† formula. Then the following hold.*

$s \models \varphi$	*iff* $I(\varphi)(s) = true$, *when* $\varphi \in \mathcal{L}_{B,V}$
$s \models \neg\varphi$	*iff* $s \not\models \varphi$
$s \models \varphi_0 \wedge \varphi_1$	*iff* $s \models \varphi_0$ *and* $s \models \varphi_1$
$s \models AX\varphi$	*iff* $\forall\pi(s).(\pi_1 \models \varphi)$
$s \models A(\varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4))$	*iff* $\forall\pi(s).(sl_U(\pi, \varphi_0, \varphi_1, \varphi_2, \varphi_3, \varphi_4))$
$s \models A(\varphi_0 R(\varphi_1, \varphi_2, \varphi_3, \varphi_4))$	*iff* $\forall\pi(s).(sl_R(\pi, \varphi_0, \varphi_1, \varphi_2, \varphi_3, \varphi_4))$

Proof. This lemma follows from Definition 20 and the semantics of CTL* defined in Definition 18. □

Lemma 51. *$M \models \varphi$ iff $s \models \varphi$ for every s that satisfies $s \models \Theta$.*

Proof. This lemma follows from Definition 20 and Definition 19. □

Remarks On Expressiveness The logic CTL† covers CTL, and it is sufficiently expressive that it covers those CTL* formulas and also the formulas with past operators in Section 8.2 of [11]. We have the following correspondences.

Formulas	*Corresponding CTL† Formulas*
$AGF\varphi$	$A(\bot R(\top, \top, \varphi, \top))$
$AFG\varphi$	$A(\top U(\bot, \bot, \varphi, \bot))$
$AG(\varphi_0 U \varphi_1)$	$A(\bot R(\top, \varphi_0, \varphi_1, \top))$
$EFG\varphi$	$\neg A(\bot R(\top, \top, \neg\varphi, \top))$
$EGF\varphi$	$\neg A(\top U(\bot, \bot, \neg\varphi, \bot))$
$AG(\varphi_0 \to X^{-1}(\neg\varphi_0\ U^{-1}\ \varphi_1)$	$A(\varphi_1 R \neg\varphi_0) \wedge AG(\varphi_0 \to AXA(\varphi_1 R \neg\varphi_0))$
$AG(\varphi_0 \to (F^{-1}\varphi_1 \wedge AF\varphi_2))$	$A(\neg\varphi_0 U(\varphi_1, \bot, \neg\varphi_0, \bot)) \wedge AG(\varphi_0 \to AF\varphi_2)$

7.1 A Proof System

In the following, we use Γ and Δ to denote sets of CTL† formulas. For brevity, we sometimes write φ for $\{\varphi\}$, and Γ, φ for $\Gamma \cup \{\varphi\}$.

- A state s is called a φ-state, if $s \models \varphi$.
- A state s is called a Γ-state, if it is a φ-state for every $\varphi \in \Gamma$.

For convenience, the set of φ-states is denoted $\theta(\varphi)$.

Definition 21. *$\Gamma \models \Delta$, if every Γ-state is a φ-state for some $\varphi \in \Delta$.*

Proposition 4. *Let φ be a CTL† formula. $M \models \varphi$ iff $\Theta \models \varphi$.*

This proposition is a consequence of Lemma 51 and the definition of $\Theta \models \varphi$.

Proving First Order Formulas When Γ and Δ are two sets of first order formulas, $\Gamma \models \varphi$ holds iff the conjunction of the formulas of Γ implies the disjunction of the formulas of Δ. We assume that we have an underlying proof system for proving $\Gamma \models \Delta$ in this case.

Proving Temporal Formulas Let $B = (F, P)$ be given. Let e (possibly with subscripts) denote a term of the first order logic, w denote a first order formula with x as the only free variable, v denote a variable, η denote a first order formula, and $\sqsubseteq$ denote a binary relation symbol of P. For brevity, we use $A(U^4_{i=0}\varphi_i)$ to denote $A(\varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4))$. Similarly for $A(R^4_{i=0}\varphi_i)$. A set of reduction rules is provided in Table 6.

For the application of the rule involving both of w and u, it is required that w, u and $\sqsubseteq$ define a weak-well-founded set. For the application of the rule involving w without accompanying u, it is required that $w, \sqsubseteq$ define a well-founded set. Similar restriction applies to $w_1, \sqsubseteq_1, w_2, \sqsubseteq_2$ as well. In addition, v, v_1, v_2 are required to be variables not appearing in any places other than those explicitly specified in the rule. For convenience, these rules are referred to as CTL† rules. The first rules is named $\neg$-left, since it is a $\neg$-rule and the principal formula is on the left of $\vdash$. It is similar for other rules. There are two $\wedge$-left rules. In this case, the first one is referred to as $\wedge$-left-one and the other is referred to as $\wedge$-left-two.

Derived Rules For convenience, we formulate a set of derived rules for the binary operators U, R. The rules are presented in Table 7. The explanation of the derivation is as follow.

Rule	*Origin*	$True$	$False$
R_{LR}	R-left	$\varphi_2, \varphi_3, \varphi_4, \eta_2, \eta_3, \eta_4, \eta_5$	
U_{LU}	U-left	η_6, η_7	$\varphi_2, \varphi_3, \varphi_4, \eta_2, \eta_3, \eta_4, \eta_5$
R_{RR}	R-right	$\varphi_2, \varphi_3, \varphi_4, \eta_3, \eta_4$	η_2
U_{RU}	U-right		$\varphi_2, \varphi_3, \varphi_4, \eta_2, \eta_3, \eta_4, \eta_5, \eta_6, u$

Soundness and Completeness The proofs of soundness and completeness are similar to that in the previous sections. For completeness of the presentation, the soundness and completeness are formulated and proved in the following subsections.

7.2 Soundness

The proof system is sound for $CTL^\dagger$. This is stated and proved as follows.

Theorem 7. *Let Γ, Δ be two sets of $CTL^\dagger$ formulas. If $\Gamma \vdash \Delta$, then $\Gamma \models \Delta$.*

Proof by induction. If Γ and Δ are two sets of first order formulas, by the assumption on that the underlying proof system for the first order logic is sound, we have $\Gamma \vdash \Delta$ implies $\Gamma \models \Delta$. In the following, we prove the soundness of each of the CTL† rules.

Case 1. $\neg$-left.

Table 6. CTL† Rules

$\neg$

$$\frac{\Gamma \vdash \Delta, \varphi}{\Gamma, \neg\varphi \vdash \Delta} \qquad \frac{\Gamma, \varphi \vdash \Delta}{\Gamma \vdash \Delta, \neg\varphi}$$

$\wedge$

$$\frac{\Gamma, \varphi_0 \vdash \Delta}{\Gamma, \varphi_0 \wedge \varphi_1 \vdash \Delta} \qquad \frac{\Gamma, \varphi_1 \vdash \Delta}{\Gamma, \varphi_0 \wedge \varphi_1 \vdash \Delta}$$

$$\frac{\Gamma \vdash \Delta, \varphi_0 \qquad \Gamma \vdash \Delta, \varphi_1}{\Gamma \vdash \Delta, \varphi_0 \wedge \varphi_1}$$

X

$$\frac{\varphi_1 \vdash \eta_1 \qquad \Gamma, [\eta_1] \vdash \Delta}{\Gamma, AX\varphi_1 \vdash \Delta} \qquad \frac{\eta_1 \vdash \varphi_1 \qquad \Gamma \vdash \Delta, [\eta_1]}{\Gamma \vdash \Delta, AX\varphi_1}$$

R

$$\frac{\begin{array}{r@{\;}l} \varphi_i \vdash & \eta_i \quad for\ i \in \{0,1,2,3,4\} \\ \eta_2, [\eta_3] \vdash & \eta_3 \\ \neg\eta_0 \vdash & (w_1)_x^{e_1} \wedge ([\eta_1 \wedge \eta_3 \wedge \eta_5 \wedge \eta_4 \wedge (e_1 \sqsubset_1 v_1 \to \eta_0)] \to e_1 \neq v_1) \\ \neg\eta_5 \vdash & (w_2)_x^{e_2} \wedge ([\eta_4 \wedge (e_2 \sqsubset_2 v_2 \to \eta_5)] \to e_2 \neq v_2) \\ \Gamma, \eta_0, \eta_1, \eta_3, \eta_5, \eta_4 \vdash & \Delta \end{array}}{\Gamma, A(R_{i=0}^4 \varphi_i) \vdash \Delta}$$

$$\frac{\begin{array}{r@{\;}l} \eta_i \vdash & \varphi_i \quad for\ i \in \{0,1,2,3,4\} \\ \eta_1 \vdash & (\eta_2 \vee \eta_3) \wedge \eta_4 \\ \eta_1, \neg\eta_0 \vdash & [\eta_1] \\ \eta_4 \vdash & [\eta_4] \\ \eta_2 \vdash & w_x^e \wedge (e = v \to [\eta_3 \vee (\eta_2 \wedge e \sqsubset v)]) \\ \Gamma \vdash & \Delta, \eta_1 \end{array}}{\Gamma \vdash \Delta, A(R_{i=0}^4 \varphi_i)}$$

U

$$\frac{\begin{array}{r@{\;}l} \varphi_i \vdash & \eta_i \quad for\ i \in \{0,1,2,3,4\} \\ \eta_0, \eta_6, \eta_3 \vdash & \eta_1 \\ \eta_5 \vdash & \eta_1 \\ \eta_4 \vdash & \eta_5 \\ \eta_7, \eta_3 \vdash & \eta_1 \\ \eta_0, [\eta_1] \vdash & \eta_1 \\ [\eta_5] \vdash & \eta_5 \\ \neg\eta_6 \vdash & \neg(\eta_1 \vee \eta_2) \wedge (w_1)_x^{e_1} \wedge ([(\eta_1 \vee (\eta_3 \wedge \eta_0)) \wedge (e_1 \sqsubset_1 v_1 \to \eta_6)] \to e_1 \neq v_1) \\ \neg\eta_7 \vdash & \neg(\eta_5 \vee \eta_2) \wedge (w_2)_x^{e_2} \wedge ([(\eta_5 \vee \eta_3) \wedge (e_2 \sqsubset_2 v_2 \to \eta_7)] \to e_2 \neq v_2) \\ \Gamma, \eta_1 \vdash & \Delta \end{array}}{\Gamma, A(U_{i=0}^4 \varphi_i) \vdash \Delta}$$

$$\frac{\begin{array}{r@{\;}l} \eta_i \vdash & \varphi_i \quad for\ i \in \{0,1,2,3,4\} \\ \eta_6, \neg\eta_2, \neg\eta_4 \vdash & [\eta_6] \\ \eta_6 \vdash & \eta_3, \eta_5, \eta_4 \\ \eta_6, \neg\eta_3 \vdash & \neg u_x^e \\ \eta_0 \vdash & w_x^e \wedge (e = v \to [\eta_1 \vee \eta_6 \vee (\eta_0 \wedge e \sqsubset v)]) \\ \eta_5 \vdash & (w_1)_x^{e_1} \wedge (e_1 = v_1 \to [\eta_4 \vee (\eta_5 \wedge e_1 \sqsubset_1 v_1)]) \\ \Gamma \vdash & \Delta, \eta_0, \eta_1, \eta_6 \end{array}}{\Gamma \vdash \Delta, A(U_{i=0}^4 \varphi_i)}$$

Table 7. CTL† Derived Rules

$$R_{LR} \quad \frac{\varphi_0 \vdash \eta_0 \qquad \varphi_1 \vdash \eta_1 \qquad \neg\eta_0 \vdash w_x^e \wedge ([\eta_1 \wedge (e \sqsubset v \to \eta_0)] \to e \neq v) \qquad \mathit{\Gamma}, \eta_0, \eta_1 \vdash \mathit{\Delta}}{\mathit{\Gamma}, A(\varphi_0 R \varphi_1) \vdash \mathit{\Delta}}$$

$$U_{LU} \quad \frac{\varphi_0 \vdash \eta_0 \qquad \varphi_1 \vdash \eta_1 \qquad \eta_0, [\eta_1] \vdash \eta_1 \qquad \mathit{\Gamma}, \eta_1 \vdash \mathit{\Delta}}{\mathit{\Gamma}, A(\varphi_0 U \varphi_1) \vdash \mathit{\Delta}}$$

$$R_{RR} \quad \frac{\eta_0 \vdash \varphi_0 \qquad \eta_1 \vdash \varphi_1 \qquad \eta_1, \neg\eta_0 \vdash [\eta_1] \qquad \mathit{\Gamma} \vdash \mathit{\Delta}, \eta_1}{\mathit{\Gamma} \vdash \mathit{\Delta}, A(\varphi_0 R \varphi_1)}$$

$$U_{RU} \quad \frac{\eta_0 \vdash \varphi_0 \wedge w_x^e \wedge (e = v \to [\eta_1 \vee (\eta_0 \wedge e \sqsubset v)]) \qquad \eta_1 \vdash \varphi_1 \qquad \mathit{\Gamma} \vdash \mathit{\Delta}, \eta_0 \vee \eta_1}{\mathit{\Gamma} \vdash \mathit{\Delta}, A(\varphi_0 U \varphi_1)}$$

Suppose $\mathit{\Gamma} \models \mathit{\Delta}, \varphi$. We prove $\mathit{\Gamma}, \neg\varphi \models \mathit{\Delta}$ as follows.

Let s be a $\mathit{\Gamma} \cup \{\neg\varphi\}$ state.

If s is a state of some formula of $\mathit{\Delta}$, we are done. Otherwise, by the premise, s is a state of φ, which yields a contradiction. Therefore s is a state of some formulas of $\mathit{\Delta}$.

Case 2. $\neg$-right.

Suppose $\mathit{\Gamma}, \varphi \models \mathit{\Delta}$. We prove $\mathit{\Gamma} \models \mathit{\Delta}, \neg\varphi$ as follows.

Let s be a $\mathit{\Gamma}$-state.

If s is a state of $\neg\varphi$, we are done. Otherwise, by the premise, s is a state of $\mathit{\Delta}$. Therefore s is a state of some formulas of $\mathit{\Delta} \cup \{\neg\varphi\}$.

Case 3. $\wedge$-left.

There are two $\wedge$-left rules.

We only consider $\wedge$-left-one, the other is similar.

Suppose $\mathit{\Gamma}, \varphi_0 \models \mathit{\Delta}$. We prove $\mathit{\Gamma}, \varphi_0 \wedge \varphi_1 \models \mathit{\Delta}$ as follows.

Let s be a $\mathit{\Gamma} \cup \{\varphi_0 \wedge \varphi_1\}$ state.

Then s is a $\mathit{\Gamma} \cup \{\varphi_0\}$-state. By the premise, s is a state of some formulas of $\mathit{\Delta}$. Therefore $\mathit{\Gamma}, \varphi_0 \wedge \varphi_1 \models \mathit{\Delta}$.

Case 4. $\wedge$-right.

Suppose $\mathit{\Gamma} \models \mathit{\Delta}, \varphi_0$ and $\mathit{\Gamma} \models \mathit{\Delta}, \varphi_1$. We prove $\mathit{\Gamma} \models \mathit{\Delta}, \varphi_0 \wedge \varphi_1$ as follows.

Let s be a $\mathit{\Gamma}$-state.

If s is a state of some formula of $\mathit{\Delta}$, we are done. Otherwise, by the premise, s is a state of φ_0 and s is a state of φ_1. Then s is a state of $\varphi_0 \wedge \varphi_1$. Therefore $\mathit{\Gamma} \models \mathit{\Delta}, \varphi_0 \wedge \varphi_1$.

Case 5. X-left.

Suppose that the premises hold. We prove $\Gamma, AX\varphi_1 \models \Delta$ as follows.

Let s be a state of $\Gamma \cup \{AX\varphi_1\}$.

If s is a state of some formula of Δ, we are done. Otherwise, by the second premise, some successor state s' of s is not a state of η_1. By the first premise, s' is not a φ_1 state. Therefore s is not an $AX\varphi_1$ state, which yields a contradiction. Therefore s is a state of some formulas of Δ.

Case 6. X-right.

Suppose that the premises hold. We prove $\Gamma \models \Delta, AX\varphi_1$ as follows.

Let s be a state of Γ.

If s is a state of some formula of Δ, we are done. Otherwise, by the second premise, every successor state of s is an η_1 state. Then by the first premise, every successor state of s is a φ_1 state. Therefore s is an $AX\varphi_1$ state. Therefore s is a state of some formulas of Δ.

Case 7. R-left.

Let $\varphi = A(\varphi_0 R(\varphi_1, \varphi_2, \varphi_3, \varphi_4))$.

Suppose that the premises hold. We prove $\Gamma, \varphi \models \Delta$ as follows.

Let s be a state of $\Gamma \cup \{\varphi\}$.

If s is a state of some formula of Δ, we are done.

Otherwise, suppose that s is not a state of any formula of Δ.

We prove that there is a contradiction, i.e., s is not a state of φ, meaning that there is an s-path satisfying $\neg\varphi_0 U(\neg\varphi_1 \vee (\neg\varphi_2 R \neg\varphi_3) \vee F(\neg\varphi_4))$.

Let ψ denote $\neg\eta_0 U(\neg\eta_1 \vee (\neg\eta_2 R \neg\eta_3) \vee F(\neg\eta_4))$. By the 1st premise, it is sufficient to show that there is an s-path satisfying ψ.

By the 5th premise, s is a state of $\neg\eta_1 \vee \neg\eta_3 \vee (\neg\eta_5 \vee \neg\eta_4) \vee \neg\eta_0$. We consider four cases.

- s is a state of $\neg\eta_1$.
  Then any s-path satisfies ψ.
- s is a state of $\neg\eta_3$.
  By the 2nd premise and Lemma 39, there is an s-path π satisfying $\neg\eta_2 R \neg\eta_3$.
  Then π is an s-path satisfying ψ.
- s is a state of $\neg\eta_5 \vee \neg\eta_4$.
  By the 4th premise and Lemma 40, there is an s-path π satisfying $\neg\eta_5 U \neg\eta_4$.
  Then π satisfies $F\neg\eta_4$.
  Then π is an s-path satisfying ψ.
- s is a state of $\neg\eta_0$.
  By the 3rd premise and Lemma 40, there is an s-path π and a $k \geq 0$ such that π_i is a $\neg\eta_0$ state for $i = 0, ..., k-1$ and π_k is a $\neg(\eta_1 \wedge \eta_3 \wedge \eta_5 \wedge \eta_4)$.
  Then similar to the reasoning in the three previous cases, we have a π_k-path π' satisfying ψ.
  Then $\pi_0 \cdots \pi_{k-1}\pi'$ is an s-path satisfying ψ.

Case 8. R-right.

Let $\varphi = A(\varphi_0 R(\varphi_1, \varphi_2, \varphi_3, \varphi_4))$.

Suppose that the premises hold. We prove $\Gamma \models \Delta, \varphi$ as follows.

Let s be a state of Γ.

If s is a state of some formulas of Δ, we are done.

Otherwise, by the 6th premise, s is a state of η_1.

Let ψ denote $\eta_0 R(\eta_1 \wedge (\eta_2 U \eta_3) \wedge G\eta_4)$. By the 1st premise, it is sufficient to show that every s-path satisfies ψ.

By the 3rd premise and Lemma 24, we have for every s-path π, either every state on the path is an η_1 state or there is a $k \geq 0$ such that $\pi_0, ..., \pi_k$ are η_1 states and π_k is an η_0 state. We have two cases.

- Every state on π is an η_1 state.
  By the 2nd premise, $\pi_0, ..., \pi_k$ are $\eta_4 \wedge (\eta_2 \vee \eta_3)$ states.
  By the 5th premise, every η_2 state leads to an η_3 state, along every direction.
  Then there are infinitely many occurrences of η_3 states on π.
  Therefore $\pi \models \psi$.
- $\pi_0, ..., \pi_k$ are η_1 states and π_k is an η_0 state.
  By the 2nd premise, $\pi_0, ..., \pi_k$ are $\eta_4 \wedge (\eta_2 \vee \eta_3)$ states.
  By the 5th premise, either π_k is an η_3 state or it leads to an η_3 state.
  By the 4th premise, every state on every π_k-path satisfies η_4.
  Therefore $\pi \models \psi$.

Case 9. U-left.

Let $\varphi = A(\varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4))$.

Suppose that the premises hold. We prove $\Gamma, \varphi \models \Delta$ as follows.

Let s be a state of $\Gamma \cup \{\varphi\}$.

If s is a state of some formulas of Δ, we are done. Otherwise, we prove that there is a contradiction, i.e., s is not a state of φ, meaning that there is an s-path satisfying $\neg\varphi_0 R(\neg\varphi_1 \wedge (\neg\varphi_2 U \neg\varphi_3) \wedge G\neg\varphi_4)$.

Let ψ denote $\neg\eta_0 R(\neg\eta_1 \wedge (\neg\eta_2 U \neg\eta_3) \wedge G\neg\eta_5)$. By the 1st premise and the 4th premise, it is sufficient to show that there is an s-path satisfying ψ.

By the 10th premise, s is a state of $\neg\eta_1$.

By the 6th premise and Lemma 39, we have an s-path π such that either (1) there is a $k \geq 0$ such that $\pi_0, ..., \pi_k$ are $\neg\eta_1$ states and π_k is a $\neg\eta_0$ state, or (2) every state on the path is a $\neg\eta_1$ state. We have two cases.

- Case 1:
  $\pi_0, ..., \pi_k$ are $\neg\eta_1$ states and π_k is a $\neg\eta_0$ state.
  Without loss of generality, we may assume that $\pi_0, ..., \pi_{k-1}$ are η_0 states.
  By the 2nd premise, $\pi_0, ..., \pi_{k-1}$ are $\neg\eta_6$ or $\neg\eta_3$ states, and then by the first part of the 8th premise, $\pi_0, ..., \pi_{k-1}$ are $\neg\eta_2$ or $\neg\eta_3$ states.
  By the 5th premise, π_k is a $\neg\eta_3$ state or a $\neg\eta_7$ state.
  We consider two subcases.
  (a) π_k is a $\neg\eta_3$ state.
  Since π_k is a $\neg\eta_1$ state, by the 3rd premise, π_k is a $\neg\eta_5$ state.
  By the 7th premise and Lemma 39, there is a π_k-path π' satisfying $G\neg\eta_5$.

Then π' satisfies $\neg\eta_3 \wedge G\neg\eta_5$.
Then $\pi_0 \cdots \pi_{k-1}\pi'$ is an s-path satisfying ψ.
(b) π_k is a $\neg\eta_7 \wedge \eta_3$ state.
Since π_k is a $\neg\eta_7 \wedge \eta_3$, by the 9th premise and Lemma 40, there is a π_k-path π' satisfying $(\neg\eta_2 \wedge \eta_5)U(\neg\eta_3 \wedge \neg\eta_5)$.
Then by the 7th premise and Lemma 39, this path can be modified to a π_k-path π'' satisfying $(\neg\eta_2 U \neg\eta_3) \wedge G\neg\eta_5$.
Then $\pi_0 \cdots \pi_{k-1}\pi''$ is an s-path satisfying ψ.

– Case 2:
Every state on π is a $\neg\eta_1$ state.
Without loss of generality, we may assume that π_i is an η_0 state for all $i \geq 0$.
By the 2nd premise, every state on π is a $\neg\eta_6$ or $\neg\eta_3$ state.
If there are infinitely many $\neg\eta_3$ state on π, then π is an s-path satisfying ψ.
Otherwise, let π_k be a $\neg\eta_6 \wedge \eta_3$ state.
By the 8th premise and Lemma 40, there is a π_k-path satisfying $(\neg\eta_2 \wedge \neg\eta_1)U((\neg\eta_3 \wedge \neg\eta_1) \vee (\neg\eta_0 \wedge \neg\eta_1))$.
Since by the 3rd premise, a $\neg\eta_1$ state is also a $\neg\eta_5$ state, and then by the 7th premise and Lemma 39, the path π can be modified to a π_k-path π' satisfying $(\neg\eta_2 \wedge \neg\eta_1)U((\neg\eta_3 \wedge \neg\eta_1) \vee (\neg\eta_0 \wedge \neg\eta_1)) \wedge G\neg\eta_5$.
Let $\pi'_{k'}$ be the first $(\neg\eta_3 \wedge \neg\eta_1) \vee (\neg\eta_0 \wedge \neg\eta_1)$ state on π'.
We consider two subcases.
(a) $\pi'_{k'}$ is a $(\neg\eta_0 \wedge \neg\eta_1)$ state.
Since $\pi_0, ..., \pi_{k-1}, \pi'_0, ..., \pi'_{k'}$ are $\neg\eta_1$ state and $\pi'_{k'}$ is a $\neg\eta_0$ state, by the arguments in Case 1, we have an s-path satisfying ψ.
(b) $\pi'_{k'}$ is a $(\neg\eta_3 \wedge \neg\eta_1)$ state.
Without loss of generality, we may assume that η_0 is satisfied on $\pi'_1, ..., \pi'_{k'}$.
Since $\pi'_0 = \pi_k$ and π_k is an η_3 state, we have that $k' \geq 1$.
Then $\pi'_{k'}$ is used a new starting point replacing the original state s and the process of the construction of a path satisfying ψ is repeated.
Either the process stops at some step where we have an s-path satisfying ψ as in one of the previous cases, or it continues to infinity and we have an s-path ζ such that $\neg\eta_1$ and η_0 are satisfied at all positions and $\neg\eta_3$ is satisfied on infinitely many positions, and then $\zeta \models \psi$.

Case 10. U-right.

Let $\varphi = A(\varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4))$.
Suppose that the premises hold. We prove $\Gamma \models \Delta, \varphi$ as follows.
Let s be a state of Γ.
If s is a state of some formulas of Δ, we are done.
Otherwise, suppose that s is not a state of φ, i.e., there is an s-path satisfying $\neg\varphi_0 R(\neg\varphi_1 \wedge (\neg\varphi_2 U \neg\varphi_3) \wedge G\neg\varphi_4)$.
Let ψ denote $\neg\eta_0 R(\neg\eta_1 \wedge (\neg\eta_2 U \neg\eta_3) \wedge G\neg\eta_4)$.
Then by the 1st premise, there is an s-path satisfying ψ.
We prove that there is a contradiction.
By the 7th premise, s is an $\eta_0 \vee \eta_1 \vee \eta_6$ state.

By the 4th and 5th premises and Lemma 25, for every s-path ζ, (i) there is an $m \geq 0$ such that $\zeta_0, ..., \zeta_{m-1}$ are η_0 states and ζ_m is an $\eta_1 \vee \eta_6$ state, or (ii) for all $i \geq 0$ we have that ζ_i is an η_0 state and there is a $l \geq 0$ such that ζ_j is an η_3 state for all $j \geq l$.

Suppose π is an s-path satisfying ψ. We divide the possibility of π into two cases.

- Case 1:
  There is a $k \geq 0$ such that π^k satisfies $\neg\eta_0$, and π^i satisfies $\neg\eta_1$ and $\neg\eta_2 U \neg\eta_3$ for $i = 0, 1, ..., k$, and π^i satisfies $\neg\eta_4$ for $i \geq 0$.
  Let k be the least number such that the above holds.
  This case is inconsistent with condition (ii), and it remains to show that it is inconsistent with (i).
  By the 6th premise, π_i is a $\neg\eta_5$ state for all $i \geq 0$, otherwise, η_4 has to hold somewhere on the path.
  By the third premise, η_6 and $\neg\eta_3$ cannot be satisfied at the same position on the path.
  Since $\pi^i \models \neg\eta_2 U \neg\eta_3$ for $i = 0, 1, ..., k$, η_6 cannot be satisfied at any π_i for $i = 0, 1, ..., k$, otherwise, suppose that π_j satisfies η_6, then by the 2nd premise, η_6 and η_3 has to be satisfied for all $i \geq j$, contradicting to $\pi^j \models \neg\eta_2 U \neg\eta_3$.
  This means that π_i is a $\neg\eta_1 \wedge \neg\eta_6$ state for $i = 0, ..., k$.
  This together with that π_k is a $\neg\eta_0$ state is inconsistent with condition (i).
- Case 2:
  For all $i \geq 0$, we have π^i satisfies $\neg\eta_1$ and $\neg\eta_2 U \neg\eta_3$ and $\neg\eta_4$.
  Since π^i satisfies $\neg\eta_2 U \neg\eta_3$ for all $i \geq 0$, there are infinitely many positions on π satisfying $\neg\eta_3$.
  This is inconsistent with condition (ii).
  In addition, by the arguments similar to that in Case 1, we have that π_i is a $\neg\eta_1 \wedge \neg\eta_6$ state for every $i \geq 0$.
  This is inconsistent with condition (i).

$\square$

7.3 Relative Completeness

Relativeness The relative completeness assumes the expressiveness condition stated in Section 3.2 and the following condition on the underlying first order proof system.

> If Γ and Δ are sets of first order formulas and $\Gamma \vdash \Delta$ is needed as a premise in the proof, then $\Gamma \vdash \Delta$ is provable by the underlying first order proof system when $\Gamma \models \Delta$ holds.

In the following, we prove that the proof system is relatively complete.

Derived Rules For the first, we provide a derived rule for proving conjunctive formulas as follows.

$$\frac{\Gamma, \varphi_0, \varphi_1 \vdash \Delta}{\Gamma, \varphi_0 \wedge \varphi_1 \vdash \Delta}$$

It is easily seen that this rule can be derived from the rules for conjunction.

Definition 22. *Let $\varphi = A(\varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4))$ and $\varphi' = A(\varphi_0 R(\varphi_1, \varphi_2, \varphi_3, \varphi_4))$. Then S^*_φ, S_φ, S^N_φ, S^{N*}_φ and $S^N_{\varphi'}$ are sets of states defined as follows.*

- *$s \in S^*_\varphi$, if s is an $A((\varphi_2 R \varphi_3) \vee F\varphi_4)$ state.*
- *$s \in S_\varphi$, if s is a φ state and not a φ_1 state and not an S^*_φ state.*
- *$s \in S^N_\varphi$, if s is a φ_0 state and a φ_3 state and not a φ state.*
- *$s \in S^{N*}_\varphi$, if s is a φ_3 state and not an S^*_φ state.*
- *$s \in S^N_{\varphi'}$, if s is a φ_1 state, an $A(\varphi_2 U \varphi_3)$ state, an $AG\varphi_4$ state, and not a φ' state.*

The set $S_{A(\varphi_0 U \varphi_1)}$, where $A(\varphi_0 U \varphi_1)$ is a special case of $A(\varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4))$, is defined according to S_φ, that is $s \in S_{A(\varphi_0 U \varphi_1)}$ iff s is an $A(\varphi_0 U \varphi_1)$ s-tate and not a φ_1 state. The set $S^N_{AG\varphi_1}$, where $AG\varphi_1$ is a special case of $A(\varphi_0 R(\varphi_1, \varphi_2, \varphi_3, \varphi_4))$, is defined according to $S^N_{\varphi'}$, that is $s \in S_{AG\varphi_1}$ iff s is a φ_1 state and not an $AG\varphi_1$ state.

Lemma 52. *Let $\varphi = A(\varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4))$ and $\varphi' = A(\varphi_0 R(\varphi_1, \varphi_2, \varphi_3, \varphi_4))$.*

1. *Let $S_1 = S_\varphi$, $Y_1 = \theta(\varphi_1) \cup S^*_\varphi$, and $Z_1 = \theta(\varphi_3)$.*
2. *Let $S_2 = S^N_\varphi$ and $Y_2 = \bar\theta(\varphi \vee (\varphi_3 \wedge \varphi_0))$.*
3. *Let $S_3 = S^{N*}_\varphi$ and $Y_3 = \bar\theta(\varphi_3 \vee AF\varphi_4)$.*
4. *Let $S_4 = S^N_{\varphi'}$ and $Y_4 = \bar\theta(\varphi_1) \cup \bar\theta(A(\varphi_2 U \varphi_3)) \cup \bar\theta(AG\varphi_4)$.*

Then $Gr(S_1)$ is a Y_1-bounded Z_1-infinite subgraph, and for $i \in \{2, 3, 4\}$, $Gr(S_i)$ is a Y_i-terminating subgraph.

Proof. The first part of this lemma corresponds to Lemma 36 and Lemma 37, and can be proved in a similar way. The second part corresponds to Lemma 44, and can be proved directly by applying the definition of the respective sets in Definition 22. $\square$

In the following, we present a set of lemmas, numbered from 53 to 59, which correspond to respectively Lemmas 38, 34, 35, 45, 46, 47, 48.

Lemma 53. *Let $\varphi = A(\varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4))$. Let $\eta_0 = \digamma(S_\varphi)$, $\eta_i = \digamma(\theta(\varphi_i))$ for $i = 1, 3$, $\eta_6 = \digamma(S^*_\varphi)$ states. Then there are e, w, u and $\sqsubseteq$ such that the following hold.*

- $\eta_0, \neg\eta_3 \models \neg u^e_x$;
- $\eta_0 \models w^e_x \wedge (e = v \to [\eta_1 \vee \eta_6 \vee (\eta_0 \wedge e \sqsubset v)])$.
- $(\{\sigma(x) \mid I(w)(\sigma)\}, \sqsubseteq)$ *is* $\{\sigma(x) \mid I(w \wedge u)(\sigma)\}$*-well-founded.*

Proof. This lemma follows from Lemma 21, with the following instantiation of S, Z, Y.

- $S = S_\varphi$.
- $Z = \theta(\varphi_3)$.
- $Y = \theta(\varphi_1) \cup S^*_\varphi$.

The conditions in Lemma 21 are ensured by Lemma 52(1). $\square$

Lemma 54. *Let $\varphi = A(\varphi_0 U \varphi_1)$. Let $\eta_0 = \digamma(S_\varphi)$ and $\eta_1 = \digamma(\theta(\varphi_1))$. Then there are e, w and $\sqsubseteq$ such that they define a well-founded set and*

$$\eta_0 \models w^e_x \wedge (e = v \rightarrow [\eta_1 \vee (\eta_0 \wedge e \sqsubset v)]).$$

Proof. This lemma is a special case of Lemma 53, with $\varphi_2, \varphi_3, \varphi_4, \eta_3, \eta_6, u$ replaced by $\perp$. $\square$

Lemma 55. *Let $\varphi = AF\varphi_1$. Let $\eta_0 = \digamma(\theta(\varphi_1 \wedge AF\varphi_1))$ and $\eta_1 = \digamma(\theta(\varphi_1))$. Then there are e, w and $\sqsubseteq$ such that they define a well-founded set and*

$$\eta_0 \models w^e_x \wedge (e = v \rightarrow [\eta_1 \vee (\eta_0 \wedge e \sqsubset v)]).$$

Proof. This lemma is a special case of Lemma 54, with $A(\varphi_0 U \varphi_1)$ replaced by $AF\varphi_1$ and $S_{A(\varphi_0 U \varphi_1)}$ replaced by $\theta(\varphi_1 \wedge AF\varphi_1)$. $\square$

Lemma 56. *Let $\varphi = A(\varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4))$. Suppose that $\eta_6 = \neg\digamma(S^N_\varphi)$, $\eta_i = \digamma(\theta(\varphi_i))$ for $i = 0, 3$, and $\eta_1 = \digamma(\theta(\varphi))$. Then there are e, w and $\sqsubseteq$ such that they define a well-founded set and*

$$\neg\eta_6 \models w^e_x \wedge (([(\eta_1 \vee (\eta_3 \wedge \eta_0)) \wedge (e \sqsubset v \rightarrow \eta_6)] \rightarrow e \neq v)).$$

Proof. This lemma follows from Lemma 23, with the following instantiation of S and Y.

- $S = S^N_\varphi$ and $\digamma(S) = \digamma(S^N_\varphi) = \neg\eta_6$.
- $Y = \bar{\theta}(\varphi \vee (\varphi_3 \wedge \varphi_0))$ and $\digamma(Y) = \neg(\eta_1 \vee (\eta_3 \wedge \eta_0))$.

The conditions in Lemma 23 are ensured by Lemma 52(2). $\square$

Lemma 57. *Let $\varphi = A(\varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4))$. Suppose that $\eta_7 = \neg\digamma(S^{N*}_\varphi)$, $\eta_3 = \digamma(\theta(\varphi_3))$, and $\eta_5 = \digamma(\theta(AF\varphi_4))$. Then there are e, w and $\sqsubseteq$ such that they define a well-founded set and*

$$\neg\eta_7 \models w^e_x \wedge (([(\eta_5 \vee \eta_3) \wedge (e \sqsubset v \rightarrow \eta_7)] \rightarrow e \neq v)).$$

Proof. This lemma follows from Lemma 23, with the following instantiation of S and Y.

- $S = S^{N*}_\varphi$ and $\digamma(S) = \digamma(S^{N*}_\varphi) = \neg\eta_7$.
- $Y = \bar{\theta}(\varphi_3 \vee AF\varphi_4)$ and $\digamma(Y) = \neg(\eta_3 \vee \eta_5)$.

The conditions in Lemma 23 are ensured by Lemma 52(3). $\square$

Lemma 58. *Let* $\varphi = A(\varphi_0 R(\varphi_1, \varphi_2, \varphi_3, \varphi_4))$. *Suppose that* $\eta_0 = \neg F(S^N_\varphi)$, $\eta_i = F(\theta(\varphi_i))$ *for* $i = 1, 4$, $\eta_3 = F(\theta(A(\varphi_2 U \varphi_3)))$, *and* $\eta_5 = F(\theta(\neg\varphi_4 \vee AG\varphi_4))$. *Then there are* e, w *and* $\sqsubseteq$ *such that they define a well-founded set and*

$$\neg\eta_0 \models w^e_x \wedge (([\eta_1 \wedge \eta_3 \wedge \eta_5 \wedge \eta_4 \wedge (e \sqsubset v \to \eta_0)] \to e \neq v)).$$

Proof. This lemma follows from Lemma 23, with the following instantiation of S and Y.

- $S = S^N_\varphi$ and $F(S) = F(S^N_\varphi) = \neg\eta_0$.
- $Y = \bar{\theta}(\varphi_1) \cup \bar{\theta}(A(\varphi_2 U \varphi_3)) \cup \bar{\theta}(AG\varphi_4)$ and $F(Y) = \neg(\eta_1 \wedge \eta_3 \wedge \eta_5 \wedge \eta_4)$.

The conditions in Lemma 23 are ensured by Lemma 52(4). $\square$

Lemma 59. *Let* $\varphi = AG\varphi_1$. *Suppose that* $\eta_0 = \neg F(S^N_{AG\varphi_1})$, *and* $\eta_1 = F(\theta(\varphi_1))$. *Then there are* e, w *and* $\sqsubseteq$ *such that they define a well-founded set and*

$$\eta_0 \models w^e_x \wedge ([\eta_1 \wedge (e \sqsubset v \to \neg\eta_0)] \to e \neq v).$$

Proof. This lemma is a special case of Lemma 58, with $\varphi_0, \varphi_2, \varphi_3, \varphi_4$ replaced by $\top$. $\square$

Completeness The proof system is relatively complete for $CTL^\dagger$. This is stated and proved as follows.

Theorem 8. *Let* Γ, Δ *be two sets of* $CTL^\dagger$ *formulas. If* $\Gamma \models \Delta$, *then* $\Gamma \vdash \Delta$.

Proof. Suppose that $\Gamma \models \Delta$ holds. If Γ and Δ are two sets of first order formulas, we have $\Gamma \vdash \Delta$ by the relativeness condition. The rest of cases is proved by induction on the structure of Γ and Δ as follows.

Case 1. $\Gamma = \Gamma' \cup \{\neg\varphi\}$.

The rule $\neg$-left is applicable.

We have to prove $\Gamma' \models \Delta, \varphi$ under the supposition $\Gamma', \neg\varphi \models \Delta$.

Let s be a state of Γ' .

If s is a state of φ, we are done. Otherwise, s is state of $\Gamma' \cup \{\neg\varphi\}$. Then by the supposition, s is a state of some formula of Δ.

Case 2. $\Gamma = \Gamma' \cup \{\varphi_0 \wedge \varphi_1\}$.

The rule $\wedge$-left is applicable.

Since we have the derived rule for conjunction, it is sufficient to prove $\Gamma', \varphi_0, \varphi_1 \models \Delta$ under the supposition $\Gamma', \varphi_0 \wedge \varphi_1 \models \Delta$.

Let s be a state of $\Gamma' \cup \{\varphi_0, \varphi_1\}$.

Then s is a state of $\Gamma' \cup \{\varphi_0 \wedge \varphi_1\}$. By the supposition, s is a state of some formula of Δ.

Case 3. $\Gamma = \Gamma' \cup \{AX\varphi_1\}$.

The rule X-left is applicable.

We have to prove that there is an η_1 such that the premises the rule hold under the supposition $\Gamma, AX\varphi_1 \models \Delta$.

Let η_1 be the representation of the set of φ_1-states. It is easily seen that the premises hold.

Case 4. $\Gamma = \Gamma' \cup \{A(\varphi_0 R(\varphi_1, \varphi_2, \varphi_3, \varphi_4))\}$.

The rule R-left is applicable.

Let $\varphi = A(\varphi_0 R(\varphi_1, \varphi_2, \varphi_3, \varphi_4))$.

We have to prove that there are $\eta_0, ..., \eta_5, e_1, e_2, w_1, w_2, \sqsubseteq_1$ and $\sqsubseteq_2$ such that the premises of the rule hold under the supposition $\Gamma', \varphi \models \Delta$.

Let $\eta_i = \digamma(\theta(\varphi_i))$ for $i = 1, 2, 4$.

Let $\eta_3 = \digamma(\theta(A(\varphi_2 U \varphi_3)))$.

Let $\eta_0 = \neg\digamma(S^N_\varphi)$.

Let $\eta_5 = \neg\digamma(S^N_{AG\varphi_4}) = \digamma(\theta(\neg\varphi_4 \vee AG\varphi_4))$.

It is easily seen that the 1st premise holds.

Since η_3 is the representation of the set of $A(\varphi_2 U \varphi_3)$ states, every state that is both a φ_2 state and has all the successors in η_3 is also in η_3. Therefore the 2ns premise holds.

Regarding the 3rd premise, by Lemma 58, there are e_1, w_1 and $\sqsubseteq_1$ such that $\neg\eta_0 \models (w_1)^{e_1}_x \wedge ([(\eta_1 \wedge \eta_3 \wedge \eta_5 \wedge \eta_4) \wedge (e_1 \sqsubset_1 v_1 \to \eta_0)] \to e_1 \neq v_1)$.

Regarding the 4th premise, by Lemma 59, there are e_2, w_2 and $\sqsubseteq_2$ such that $\neg\eta_5 \models (w_2)^{e_2}_x \wedge ([\eta_4 \wedge (e_2 \sqsubset_2 v_2 \to \eta_5)] \to e_2 \neq v_2)$.

Let s be a state of Γ.

If it is a state of Δ, then the 5th premise holds. Otherwise, since s is not a state of φ, s is either a state of $\neg\eta_0$, a state of $\neg\eta_1$, a state of $\neg\eta_3$,a state of $\neg\eta_5$, or a state of $\neg\eta_4$. Therefore the 5th premise holds. $\square$

Case 5. $\Gamma = \Gamma' \cup \{A(\varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4))\}$.

The rule U-left is applicable.

Let $\varphi = A(\varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4))$.

We have to prove that there are $\eta_0, ..., \eta_7, e_1, w_1, e_2, w_2$ and $\sqsubseteq_1, \sqsubseteq_2$ such that the premises of the rule hold under the supposition $\Gamma', \varphi \models \Delta$.

Let $\eta_i = \digamma(\theta(\varphi_i))$ for $i = 0, 2, 3, 4$.

Let $\eta_1 = \digamma(\theta(\varphi))$.

Let $\eta_5 = \digamma(\theta(AF\varphi_4))$.

Let $\eta_6 = \neg\digamma(S^N_\varphi)$.

Let $\eta_7 = \neg\digamma(S^{N*}_\varphi)$.

It is easily seen that the 1st, 2nd, 3rd, 4th, 5th and 10th premises hold.

Since η_1 is the representation of the set of φ states, every state that is both an η_0 state and has all the successors in η_1 is also in η_1. Therefore the 6th premise holds.

Since η_5 is the representation of the set of $AF\varphi_4$ states, every state that has all the successors in η_5 is also in η_5. Therefore the 7th premise holds.

Regarding the 8th premise, it is easily seen that we have $\neg\eta_6 \models \neg(\eta_1 \vee \eta_2)$, and by Lemma 56, there are e_1, w_1 and $\sqsubseteq_1$ such that $\neg\eta_6 \models (w_1)^{e_1}_x \wedge ([(\eta_1 \vee (\eta_3 \wedge \eta_0) \wedge (e_1 \sqsubset_1 v_1 \to \eta_6)] \to e_1 \neq v_1)$.

Regarding the 9th premise, it is easily seen that we have $\neg\eta_7 \models \neg(\eta_5 \vee \eta_2)$, and by Lemma 57, there are e_2, w_2 and $\sqsubseteq_2$ such that $\neg\eta_7 \models (w_2)^{e_2}_x \wedge ([(\eta_3 \vee \eta_5) \wedge (e_2 \sqsubset_2 v_2 \to \eta_7)] \to e_2 \neq v_2)$.

Case 6. $\Delta = \Delta' \cup \{\neg\varphi\}$.

The rule $\neg$-right is applicable.

We have to prove $\Gamma, \varphi \models \Delta'$ under the supposition $\Gamma \models \Delta', \neg\varphi$.

Let s be a state of $\Gamma \cup \{\varphi\}$. Since s cannot be a state of $\neg\varphi$, by the supposition, s is a state of some formula of Δ'.

Case 7. $\Delta = \Delta' \cup \{\varphi_0 \wedge \varphi_1\}$.

The rule $\wedge$-right is applicable.

We have to prove $\Gamma \models \Delta', \varphi_0$ and $\Gamma \models \Delta', \varphi_1$ under the supposition $\Gamma \models \Delta', \varphi_0 \wedge \varphi_1$.

Let s be a state of Γ.

If s is a state of some formula of Δ', we are done. Otherwise, by the supposition, s is a state $\varphi_0 \wedge \varphi_1$. Then s is a state of both φ_0 and φ_1.

Case 8. $\Delta = \Delta' \cup \{AX\varphi_1\}$.

The rule X-right is applicable.

We have to prove that there is an η_1 such that the premises of the rule hold under the supposition $\Gamma \models \Delta', AX\varphi_1$.

Let η_1 be the representation of the set of φ_1-states.

It is easily seen that the premises hold.

Case 9. $\Delta = \Delta' \cup \{A(\varphi_0 R(\varphi_1, \varphi_2, \varphi_3, \varphi_4))\}$.

The rule R-right is applicable.

Let $\varphi = A(\varphi_0 R(\varphi_1, \varphi_2, \varphi_3, \varphi_4))$.

We have to prove that there are $\eta_0, ..., \eta_4, e, w$ and $\sqsubseteq$ such that the premises of the rule hold under the supposition $\Gamma \models \Delta', \varphi$.

Let $\eta_i = F(\theta(\varphi_i))$ for $i = 0, 3$.

Let $\eta_1 = F(\theta(\varphi))$.

Let $\eta_2 = F(S_{A(\varphi_2 U \varphi_3)})$.

Let $\eta_4 = F(\theta(AG\varphi_4))$.

It is easily seen that the 1st and 6th premises hold.

Since an η_1 state satisfies $A((\varphi_2 U \varphi_3) \wedge G\varphi_4)$, it satisfies φ_4 and it either satisfies η_3 or satisfies η_2, and therefore the 2nd premise holds.

Since an η_1 state is a φ state, if it is not an φ_0 state, every successor state of the state must be a φ state, and therefore the 3rd premise holds.

Since an η_4 state is an $AG\varphi_4$ state, every successor state of the state must be an $AG\varphi_4$ state, and therefore the 4th premise holds.

By the construction of η_2, we have $\eta_2 \models \varphi_2$, and by Lemma 54, there are e, w and $\sqsubseteq$ such that the 5th premise of the rule hold.

Case 10. $\Delta = \Delta' \cup \{A(\varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4))\}$.

The rule U-right is applicable.

Let $\varphi = A(\varphi_0 U(\varphi_1, \varphi_2, \varphi_3, \varphi_4))$.

We have to prove that there are $\eta_0, ..., \eta_6, e, w, u, \sqsubseteq, e_1, w_1$ and $\sqsubseteq_1$ such that the premises of the rule hold under the supposition $\Gamma \models \Delta', \varphi$.

Let $\eta_0 = \digamma(S_\varphi)$.

Let $\eta_i = \digamma(\theta(\varphi_i))$ for $i = 1, 2, 3, 4$.

Let $\eta_5 = \digamma(\theta(\neg\varphi_4 \wedge AF\varphi_4))$.

Let $\eta_6 = \digamma(S^*_\varphi) = \digamma(\theta(A((\varphi_2 R \varphi_3) \vee F\varphi_4))$.

It is easily seen that the 1st premise holds.

By the construction of η_6, if an η_6 state is not a φ_4 state and not an φ_2 state, then the successors of such a state must still be a η_6 state. Therefore the 2nd premise holds.

By the construction of η_6, if an η_6 state is not a φ_3 state, then it must be an $AF\varphi_4$ state. Therefore the 3rd premise holds.

By the construction of η_0 and by Lemma 53, there are e, w, u and $\sqsubseteq$ such that the 4th and 5th premises of the rule hold.

By the construction of η_5 and η_4, and Lemma 55, there are e_1, w_1 and $\sqsubseteq_1$ such that the 6th premise of the rule holds.

Let s be a state of Γ.

If it is a state of Δ', then the 7th premise holds. Otherwise, since s is a state of φ, s is either a state of η_1, a state of η_6, or a state of η_0. Therefore the 7th premise holds. □

8 Verification Condition Generation

The verification condition generation process may be supported by a verification condition generation tool. For experimental purpose, such a tool, denoted *vcgtp*, has been developed based on the deduction rules. By providing the necessary auxiliary constructs, the functionality of the tool is to generate premises of proof goals, and to some extend, make simplifications of the premises. In this section, we use Lamport's bakery algorithm for mutual exclusion for two processes [23] as an example to demonstrate the process of proving temporal properties using the verification condition generation approach. The tool and the files containing the model and auxiliary constructs for illustrating the verification condition generation process described in this section are available[3], and the reader may refer to Appendix B for details of the formulation of the algorithm, properties, auxiliary constructs, and axioms in the input language of the tool.

[3] `http://lcs.ios.ac.cn/~zwh/vcgtp/`

Mutual Exclusion The transition relation of the model (i.e. the algorithm) is shown in Fig. 3, in which the constant symbols, function symbols, and predicate symbols are interpreted over natural numbers as usual, and the three constants s_0, s_1, s_2 are interpreted as different numbers.

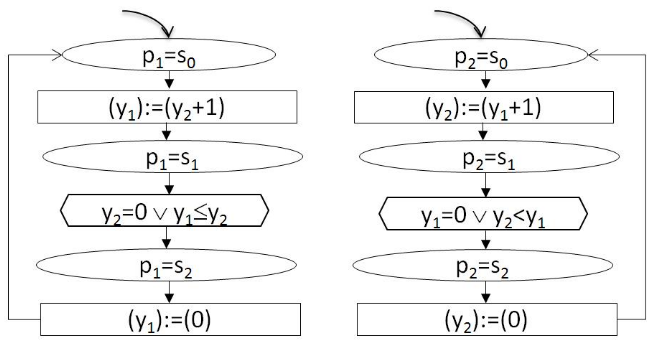

Fig. 3. Lamport's Mutual Exclusion Algorithm

The initial states of the model are characterized by the following formula.

$$(p_1 = s_0 \wedge p_2 = s_0 \wedge y_1 = 0 \wedge y_2 = 0).$$

Properties We consider the following properties. Of these properties, the third one is not satisfied by the algorithm.

(1) $G(\neg(p_1 = s_2 \wedge p_2 = s_2))$
(2) $G(p_1 = s_1 \to F(p_1 = s_2))$
(3) $G(p_1 = s_0 \to F(p_1 = s_2))$
(4) $G(p_1 = s_0 \wedge (FG(p_1 = s_0) \to \perp) \to F(p_1 = s_2))$

Notations For convenience, we write $\varphi_0(p_2, y_2)$ for the following formula (which can be proven to be a safety property of the model).

$$(p_2 = s_0 \vee y_2 > 0) \wedge (p_2 = s_1 \vee p_2 = s_2 \vee y_2 = 0).$$

Some of the proof rules require that we have binary relation symbols such as $\sqsubseteq$, $\sqsubseteq_1$ and $\sqsubseteq_2$. In the following, for brevity, if nothing is explicitly said about these symbols, they are taken to be $\leq$.

Property 1 For proving the property, it is rewritten to be as follows.

$$(p_1 = s_0 \wedge p_2 = s_0 \wedge y_1 = 0 \wedge y_2 = 0) \vdash G(\neg(p_1 = s_2 \wedge p_2 = s_2)).$$

Let η_1 be the conjunction of the following formulas.

$$\boxed{\begin{array}{l} (p_1 = s_1) \vee (p_1 = s_2) \to (y_1 > 0) \\ (p_2 = s_1) \vee (p_2 = s_2) \to (y_2 > 0) \\ \neg((p_2 = s_1) \wedge (p_2 = s_2) \wedge (y_2 = 0 \vee y_1 \leq y_2)) \\ \neg((p_2 = s_2) \wedge (p_2 = s_1) \wedge (y_1 = 0 \vee \neg(y_1 \leq y_2))) \\ \neg(p_1 = s_2 \wedge p_2 = s_2) \end{array}}$$

According to the proof rule for G, initially, three verification conditions are generated, and these conditions can be simplified to *true* using first order reasoning. Therefore the property holds.

Property 2 For proving the property, it is rewritten to be as follows.

$$(p_1 = s_0 \wedge p_2 = s_0 \wedge y_1 = 0 \wedge y_2 = 0) \vdash G(p_1 = s_1 \to F(p_1 = s_2)).$$

(Step 1) Let η_1 be $(p_1 = s_1 \to y_1 > 0) \wedge \varphi_0(p_2, y_2)$.

According to the proof rule for G, three verification subgoals are generated, two of which are first order proof goals that can be simplified to *true* using first order reasoning. There remains the following proof goal.

$$(p_1 = s_1 \to y_1 > 0) \wedge \varphi_0(p_2, y_2) \vdash (p_1 = s_1) \to F(p_1 = s_2).$$

(Step 2) Let η_0, η_1 (for proving the subgoal) be defined as follows.

$$\boxed{\begin{array}{l} \eta_0 : \ \neg(p_1 = s_1) \\ \eta_1 : \ (p_1 = s_1 \wedge y_1 > 0) \wedge \varphi_0(p_2, y_2) \end{array}}$$

According to the proof rule for $\vee$, three verification subgoals are generated, two of which are first order proof goals that can be simplified to *true* using first order reasoning. There remains the following proof goal.

$$(p_1 = s_1 \wedge y_1 > 0) \wedge \varphi_0(p_2, y_2) \vdash F(p_1 = s_2).$$

This step can be skipped by using the option "-skip", i.e., the use of this option in Step 1 would directly produce the above subgoal. In general, if it is possible to automatically construct the auxiliary construct[4], we may be able to skip the intermediate steps.

(Step 3) Let $e_0(p_2, y_1, y_2)$ denote a term with the following interpretation.

$$\boxed{\begin{array}{l} e_0(s_0, y_1, y_2) = 1 \\ e_0(s_2, y_1, y_2) = 2 \\ e_0(s_1, y_1, y_2) = 3, \quad if \ y_2 < y_1 \\ e_0(s_1, y_1, y_2) = 0, \quad if \ y_2 \geq y_1 \end{array}}$$

[4] There has been a lot of research work on automated construction of invariants and ranking functions over well-founded domains, e.g., [27, 3, 4, 1, 18], for automating the verification process. Automated construction of ranking functions over weak well-founded domains may as well help automating the use of some of the proof rules.

Let η_0, η_1, w, e be defined as follows.

$$\boxed{\begin{array}{ll} \eta_0 : & (p_1 = s_1 \wedge y_1 > 0) \wedge \varphi_0(p_2, y_2) \\ \eta_1 : & (p_1 = s_2) \\ w : & x \geq 0 \\ e : & e_0(p_2, y_1, y_2) \end{array}}$$

It is easily seen that w and $\leq$ define a well-founded set.

According to the proof rule for F, three verification conditions are generated, and these conditions can be simplified to *true* using the usual first order reasoning with additionally the following axioms for e_0.

$$\boxed{\begin{array}{rl} e_0(s_2, y_1, y_2) & > e_0(s_0, y_1, 0) \\ e_0(s_0, y_1, 0) & > e_0(s_1, y_1, y_1 + 1) \\ y_1 > y_2 \to e_0(s_1, y_1, y_2) & > e_0(s_2, y_1, y_2) \end{array}}$$

Property 3 In this case, we prove that property 3 does not hold. The proof goal is rewritten to be as follows.

$$(p_1 = s_0 \wedge p_2 = s_0 \wedge y_1 = 0 \wedge y_2 = 0) \vdash_N G(p_1 = s_0 \to F(p_1 = s_2)).$$

(Step 1) Let η_0, η_1, w, e be defined as follows.

$$\boxed{\begin{array}{ll} \eta_0 : & \top \\ \eta_1 : & \neg((p_1 = s_0 \wedge y_1 = 0) \wedge \varphi_0(p_2, y_2)) \\ w : & x \geq 0 \\ e : & 0 \end{array}}$$

According to the proof rule for $\bar{G}$, three verification subgoals are generated, two of which are first order proof goals that can be simplified to *true* using first order reasoning. There remains the following proof goal.

$$((p_1 = s_0 \wedge y_1 = 0) \wedge \varphi_0(p_2, y_2)) \vdash_N (p_1 = s_0) \to F(p_1 = s_2).$$

With the use of the option "-skip", instead of the above proof goal, the following is obtained (the rule $\bar{\nabla}$ is automatically applied in this case).

$$((p_1 = s_0 \wedge y_1 = 0) \wedge \varphi_0(p_2, y_2)) \vdash_N F(p_1 = s_2).$$

(Step 2) Let η_1 (for proving the subgoal) be the following.

$$\neg(p_1 = s_0 \wedge y_1 = 0) \wedge \varphi_0(p_2, y_2).$$

According to the proof rule for $\bar{F}$, three verification conditions are generated, and these conditions can be simplified to *true* using first order reasoning.

Property 4 For proving the property, it is rewritten to be as follows.

$$(p_1 = s_0 \wedge p_2 = s_0 \wedge y_1 = 0 \wedge y_2 = 0) \vdash G(p_1 = s_0 \to (\top U(p_1 = s_2, \bot, p_1 = s_0, \bot))).$$

(Step 1) Let $\eta_1 = \varphi_0(p_2, y_2)$.

According to the proof rule for G (and with the rule $\vee$ automatically applied), three verification subgoals are generated, two of which are first order proof goals that can be simplified to *true* using first order reasoning. After simplification, there remains the following proof goal.

$$(p_1 = s_0) \wedge \varphi_0(p_2, y_2) \vdash (\top U(p_1 = s_2, \bot, p_1 = s_0, \bot)).$$

(Step 2) Let $e_0(p_1, p_2, y_1, y_2)$ denote a term with the following interpretation.

$e_0'(s_0, y_1, y_2)$	$= 1$	
$e_0'(s_2, y_1, y_2)$	$= 2$	
$e_0'(s_1, y_1, y_2)$	$= 3,$	$if\ y_2 < y_1$
$e_0'(s_1, y_1, y_2)$	$= 0,$	$if\ y_2 \geq y_1$
$e_0(s_i, s_j, y_1, y_2)$	$= 4(1-i) + e_0'(s_j, y_1, y_2)$	

Let $\eta_0, ..., \eta_6, w, u, e, w_1, e_1$ be defined as follows.

$\eta_0 :$	$((p_1 = s_0) \vee (p_1 = s_1 \wedge y_1 > 0)) \wedge \varphi_0(p_2, y_2)$
$\eta_1 :$	$(p_1 = s_2)$
$\eta_2, \eta_4, \eta_5, \eta_6 :$	$\bot$
$\eta_3 :$	$(p_1 = s_0)$
$w :$	$x \geq 0$
$u :$	$x > 3$
$e :$	$e_0(p_1, p_2, y_1, y_2)$
$w_1 :$	$x \geq 0$
$e_1 :$	0

Let $\sqsubseteq$ be the following set of pairs.

$$\{(a, b) \mid b \geq 4\} \cup \{(a, b) \mid a \leq b \leq 3\}$$

It is easily seen that $w, u, \sqsubseteq$ define a weak-well-founded set.

According to the proof rule for U, ten verification conditions are generated, and these conditions can be simplified to *true* using the usual first order reasoning with an appropriate set of axioms characterizing e_0.

Summary Numbers of steps for the verification of the 4 properties are shown as follows.

Property	*T/F*	*Steps*
(1) $G(\neg(p_1 = s_2 \wedge p_2 = s_2))$	T	1
(2) $G(p_1 = s_1 \to F(p_1 = s_2))$	T	3(2)
(3) $G(p_1 = s_0 \to F(p_1 = s_2))$	F	3(2)
(4) $G(p_1 = s_0 \wedge (FG(p_1 = s_0) \to \bot) \to F(p_1 = s_2))$	T	3(2)

For each of the 2nd, 3rd and 4th properties, there are 3 steps when we follow the steps of the proof rules, and one of the steps may be skipped automatically. At each step, a number of verification subgoals are generated according to the proof rules, and simplified according to first order reasoning with possibly additional axioms for characterizing the user-defined symbols. Regarding the above steps in this example, either all verification subgoals are dismissed automatically in a step, or there remains one verification subgoal that is used as the verification goal for the next step.

A On Related Works

For reasoning of LTL properties, proof rules have been developed by Manna and Pnueli in [28]. With the proof rules, one may reduce the verification problem to first order reasoning, by providing necessary auxiliary constructs. In the general case, when a verification problem is not handled by these proof rules, a transformation scheme is provided for transforming the problem into a validity problem of a kind of LTL formulas. Although this approach reduces a program verification problem to a validity checking problem of logic formulas, the underlying logic is too strong in the general case, and may not be very much helpful for reducing the complexity of the reasoning. An example of such a transformation is provided in Section A.1.

For reasoning of CTL properties, proof rules have been proposed by Fix and Grumberg in [15], for reducing the verification problem to first order reasoning with provided necessary auxiliary constructs. However, the completeness issue might be a problem. An example is provided in Section A.2.

In [34, 21, 17], Pnueli, Kesten and Gabbay have worked on deductive proof systems for CTL*. The main techniques used in the approach are decomposition and reduction. The use of the rules (backwards) makes a simplification of the property to be proved by increasing the complexity of the program, and therefore it requires more effort to understand the new program in order to be able to construct useful auxiliary constructs for proving a property (the approach reminds the automata-theoretic approach of verification [35] in a way that we first have to make a composition of the program and the property in some way and then check a simpler property of the composition). In addition, the completeness issue might also be a problem. An example is provided in Section A.3.

In [11], Cook et. al. have put the emphasis on automated verification of CTL* properties, and as stated in the paper, it provides a fully automated tool for symbolically proving CTL* properties of infinite-state integer programs, and it has been reported that a set of interesting CTL* properties can be automatically verified in the given case studies. Due to the use of determinization and approximation techniques, not every problem instance can be solved successfully, and the incompleteness due to determinization has been pointed out in [11]. An example is provided in Section A.4.

A.1 Example 1

In this subsection, we provide an example showing how a program verification problem is transformed into a problem of checking the validity of a temporal logic formula, by using the approach provided in [28]. Let the program be the one in Fig. 1.

Property Let $\psi_1 \triangleq (y = 0 \vee y = 1)\, U\, (y = 2 \vee (z = 2\, R\, (y = 3 \vee z < 0)))$. Suppose that we are trying to prove $P_1 \models \psi_1$.

Problem Transformation Let X denote the next operator such that Xz is the value of z at the next state. Let ρ denote the disjunction of the following formulas.

$$
\begin{array}{l}
(y = 0 \wedge Xy = 1 \wedge Xz = -z) \\
(y = 0 \wedge Xy = 0 \wedge Xz = z - 1) \\
(y = 1 \wedge (\neg z = 2) \wedge Xy = 1 \wedge Xz = z - 1) \\
(y = 1 \wedge z = 2 \wedge Xy = 2 \wedge Xz = 0) \\
(y = 1 \wedge z = 1 \wedge Xy = 3 \wedge Xz = 0) \\
(y = 2 \wedge z > y \wedge Xy = 1 \wedge Xz = z) \\
(y = 2 \wedge Xy = 2 \wedge Xz = z + 1) \\
(y = 3 \wedge z > y \wedge Xy = 2 \wedge Xz = z) \\
(y = 3 \wedge Xy = 3 \wedge Xz = z + 1)
\end{array}
$$

Then the task of proving $P_1 \models \psi_1$ may be reduced to proving the validity of the following formula, under the usual interpretation of integers and operations on integers.

$$z \geq 0 \wedge y = 0 \wedge G(\rho) \rightarrow \psi_1.$$

Then it would be desirable to have an approach for reducing such a validity checking problem to first order reasoning. Although in general there is a lack of this kind of approaches, for this particular instance of the problem, there is way to do it (cf. Section 1).

A.2 Example 2

In this subsection, we provide an example showing that there are problem instances that are not handled by the approach provided in [15]. Let the program $P_2 = P_1$ be the one presented in Fig. 1.

Property Let $\psi_2 \triangleq \neg E(\neg((y = 3 \vee y = 2) \wedge z = 0)\, U\, \neg(y = 0 \vee y = 1 \vee z = 0))$. Suppose that we are trying to prove $P_2 \models \psi_2$.

Verification Approach For proving that $P_2 \models \psi_2$, we have to prove that P_2 satisfies $y = 0 \wedge z \geq 0 \rightarrow \psi_2$. The only rule that is applicable is the $\neg EU$ rule, with f_1 and f_2 instantiated to respectively $\neg((y = 3 \vee y = 2) \wedge z = 0)$ and $\neg(y = 0 \vee y = 1 \vee z = 0)$. This means that either we have to establish (1) or we have to find a first order formula η such that (2) holds.

(1) $y = 0 \wedge z \geq 0 \rightarrow \neg f_1 \wedge \neg f_2$
(2) $y = 0 \wedge z \geq 0 \rightarrow \eta$ and $\eta \rightarrow \neg f_2 \wedge AX(\eta \vee (\neg f_1 \wedge \neg f_2)$

It is easily seen that neither of the cases holds.

A.3 Example 3

In this subsection, we provide an example showing that there are problem instances that are not handled by the approach provided in [17]. For this example, a program has five components, a set of variables, a formula representing the initial states, a transition relation, a set of justice conditions and a set of compassion conditions. For brevity, we present the program P_3 we are considering as a graph shown in Fig. 4. The program P_3 can be considered as a simplification of P_1.

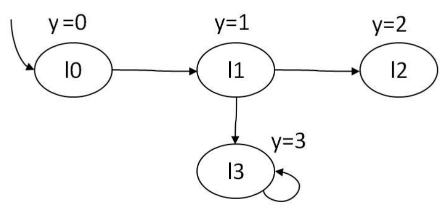

Fig. 4. The Program $P_3 = (V, \Theta, \rho, \emptyset, \emptyset)$

Property Let $\psi_3 \triangleq AXEF(y = 1 \wedge G(y = 1 \vee y = 2))$. Suppose that we are trying to prove $P_3 \models \psi_3$.

Verification Approach For proving that $P_3 \models \psi_3$, we have to handle the path formula $G(y = 1 \vee y = 2)$. The only rule we can use is the Basic-Path rule. The use of this rule reduces the proof of $P_3 \models (y = 0) \Rightarrow \psi_3$ to a proof of $P_3 \mid\mid\mid T[G(y = 1 \vee y = 2)] \models (y = 0) \Rightarrow AXEF(y = 1 \wedge x_{G(y=1 \vee y=2)})$, where $T[G(y = 1 \vee y = 2)]$ is the tester for $G(y = 1 \vee y = 2)$.

The Tester The tester is presented in Fig. 5. For brevity, the Boolean variable $x_{G(y=1 \vee y=2)}$ is written as x.

The Parallel Composition The parallel composition $P_3 \mid\mid\mid T[G(y = 1 \vee y = 2)]$ has 16 states, i.e., there are 4 possibilities for the values of y, and 2 possibilities for each of the two Boolean variables. The 8 states that satisfy $\mathcal{E}r$ are not fair ones. The other 8 states that satisfy $\neg \mathcal{E}r$ and the transitions between these states are presented in Fig. 6.

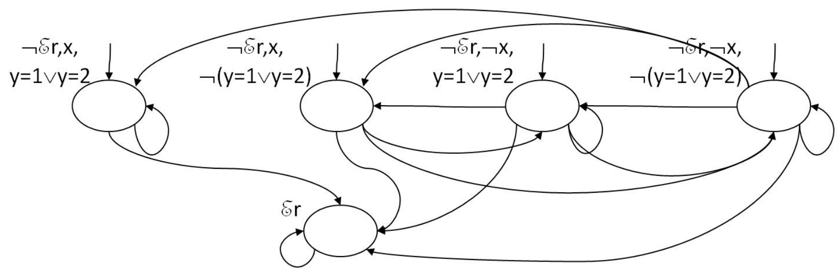

Fig. 5. $T[G(y = 1 \vee y = 2)] = (V \cup \{\mathcal{E}r, x\}, \Theta', \rho', \{x \vee \neg(y = 1 \vee y = 2), \neg\mathcal{E}r\}, \emptyset)$

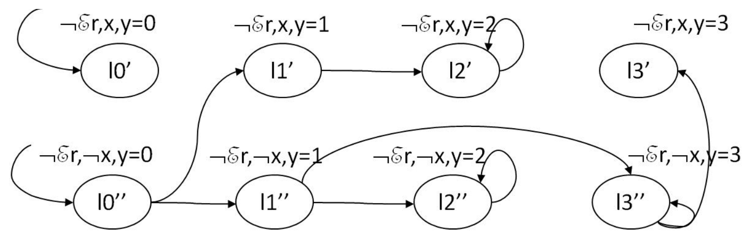

Fig. 6. Parts of $P_3 \mid\mid\mid T[G(y = 1 \vee y = 2)]$

We have two fair paths: one looping on l_2' and one looping on l_3''. Since l_1'' does not satisfy $EF(y = 1 \wedge x_{G(y=1\vee y=2)})$, it is easily verified that the following does not hold.

$$P_3 \mid\mid\mid T[G(y = 1 \vee y = 2)] \models (y = 0) \Rightarrow AXEF(y = 1 \wedge x_{G(y=1\vee y=2)}).$$

Therefore $P_3 \models \psi_3$ cannot be proved by reduction to the above verification goal.

A.4 Example 4

In this subsection, we provide an example showing that there are problem instances that are not well-handled by the approach provided in [11]. The incompleteness has already been discussed in [11]. The purpose of this subsection is to provide a simple example demonstrating the problem. Let the program P_4 be the one in Fig. 7. This is the same as P_3 in the previous subsection, presented in a slightly different form.

The determinized program P_D is shown in Fig. 8 with $vars_D = Vars \cup \{n_1, n_2\}$. The two new variables are introduced for the determinization of the program.

Then for checking a property, we have to restrict the attention to the states that satisfy $EG\,true$. The set of states that satisfied $EG\,true$ is specified as

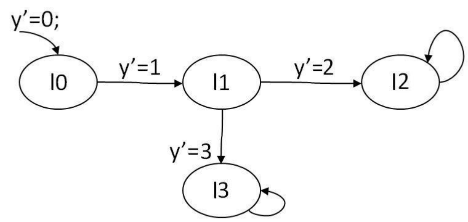

Fig. 7. The Program $P_4 = (\mathcal{L}, E, Vars)$

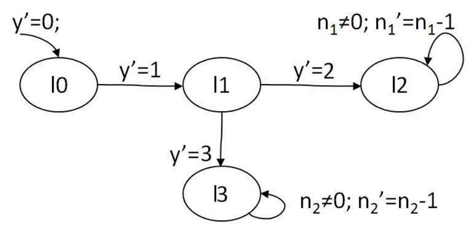

Fig. 8. The Program $P_D = (\mathcal{L}, E_D, Vars_D)$

follows.

$CTL(P_D, EG\,true) =$
$(y = 0 \vee y = 1) \wedge (n_1 < 0 \vee n_2 < 0) \vee (y = 2 \wedge n_1 < 0) \vee (y = 3 \wedge n_2 < 0)$.

Property Let $\psi_4 \triangleq AXEF(y = 1 \wedge G(y = 1 \vee y = 2))$. Suppose that we are trying to prove $P_4 \models \psi_4$.

Verification Approach For each subformula φ of ψ_4, we calculate $ProveCTL^*(\varphi, P, P_D)$, and obtain the following.

φ	$ProveCTL^*(\varphi, P, P_D)$
$y = 1$	$(y = 1, false)$
$y = 1 \vee y = 2$	$(y = 1 \vee y = 2, false)$
$G(y = 1 \vee y = 2)$	$(y = 2, false)$
$y = 1 \wedge G(y = 1 \vee y = 2)$	$(false, true)$
$EF(y = 1 \wedge G(y = 1 \vee y = 2))$	$(false, true)$
$AXEF(y = 1 \wedge G(y = 1 \vee y = 2))$	$(false, false)$

The calculation implies that we have not found any state that satisfies ψ_4. On the other hand, the set of states that satisfy ψ_4, in fact, include the state specified by $y = 0$ when the program under the consideration is P_4, and the states specified by $y = 0 \wedge n_1 < 0$ when the program under the consideration is P_D.

B Details of Verification using VCGTP

In this section, we present the input to the tool for Example 1 in Section 4, Example 2 in Section 5 and the mutual exclusion example in Section 8.

B.1 Example 1

The model of the transition system in the example in Section 4 is as follows.

```
VAR
     y:int;
     z:int;
TRANS
     y=0:             (y,z):=(1,0-z);
     y=0:             (y,z):=(0,z-1);
     y=1&!(z=2):      (y,z):=(1,z-1);
     y=1&z=2:         (y,z):=(2,0);
     y=1&z=1:         (y,z):=(3,0);
     y=2&z>y:         (y,z):=(1,z);
     y=2:             (y,z):=(2,z+1);
     y=3&z>y:         (y,z):=(2,z);
     y=3:             (y,z):=(3,z+1);
```

Proving the 1st Property For this purpose, the transition system is appended by the following that contains the specification of the property, auxiliary constructs and axioms for characterizing the user-defined function symbol.

```
SPEC
     y=0&z>=0 |- ((y=0|y=1)U(y=2,z=2,(y=3|z<0),FALSE));
AUX
     eta0:   (y=0)|(y=1&z>=0);
     eta1:   (y=2);
     eta2:   (z=2);
     eta3:   (y=3|z<0);
     eta4:   FALSE;
     eta5:   FALSE;
     eta6:   (y=3&z<=2)|(y=1&z<0);
     w:      ((even(x)=1)|x>=0);
     u:      ((even(x)=1)&x<0);
     e:      e0(z,y);
     w1:     (x>=0);
     e1:     0;
AXIOM
     !(z>=0)|e0(z,1)>=0;
     !(z>=0)|e0(z,0)>=0;
     (e0(z-1,1)<e0(z,1));
     (e0(z-1,0)<e0(z,0));
     (e0(0-z,1)<e0(z,0));
     (even:e0(z,0))=1;
```

Suppose that the name of the input file is "me1p1s1.vvm", then the command for verification condition generation is as follows.

```
./vcgtp me1p1s1.vvm
```

The output indicates that all subgoals have been dismissed and therefore the property holds.

Proving the 2nd Property For this purpose, the transition system is appended by the following that contains the specification of the property, and auxiliary constructs.

```
SPEC
     y=0&z>=0 |- (y=1)R((y=0|y=1),z>0,z<=0,TRUE);
AUX
     eta0:   (y=1);
     eta1:   (y=0|y=1);
     eta2:   (y=0|y=1)&z>0;
     eta3:   (z<=0);
     eta4:   (TRUE);
     w:      (x>=0);
     e:      (z);
```

B.2 Example 2

The model of the transition system in the example in Section 5 is as follows.

```
VAR
     y:int;
     z:int;
TRANS
     y=0:            (y,z):=(1,z);
     y=1&!(z=2):     (y,z):=(1,z-1);
     y=1&z=2:        (y,z):=(2,0);
     y=1&z=1:        (y,z):=(3,0);
     y=2&z>y:        (y,z):=(1,z);
     y=2:            (y,z):=(2,z+1);
     y=3&z>y:        (y,z):=(2,z);
     y=3:            (y,z):=(3,z+1);
```

Falsifying the 1st Property For this purpose, the transition system is appended by the following that contains the specification of the property (for negative satisfiability), auxiliary constructs and axioms for characterizing the user-defined function symbol.

```
SPEC
     y=0&z>0 |# ((y!=3)U(z<0,z<0,y!=2,FALSE));
AUX
     eta0:   (y!=3);
     eta1:   !(((y=0|y=1)&z>0)|((y=3|y=2)&z>=0));
```

```
     eta5:   (FALSE);
     eta6:   !(((y=0|y=1)&z>0));
     eta7:   !(((y=0|y=1)&z>0)|(y=3&z>=0));
     w1:     (x>=0);
     e1:     (z-y);
     w2:     (x>=0);
     e2:     (e0(z,y));
AXIOM
     !(z>=0)|e0(z,0)>=0;
     !(z>=0)|e0(z,1)>=0;
     !(z>=0)|e0(z,3)>=0;
     !(z>=0&z<=3)|(e0(z+1,3)<e0(z,3));
     e0(z,1)<e0(z,0);
     e0(z-1,1)<e0(z,1);
     e0(0,3)<e0(1,1);
```

Falsifying the 2nd Property For this purpose, the transition system is appended by the following that contains the specification of the property (for negative satisfiability), and auxiliary constructs.

```
SPEC
     y=0&z>0 |# ((y=2|y=3)R(y!=3,z!=y,(z>y),TRUE);
AUX
     eta0:   !((y=0|y=1)&z>0);
     eta1:   !(y=3);
     eta3:   (z>y);
     eta5:   (TRUE);
     w1:     (x>=0);
     e1:     (z-y);
     w2:     (x>=0);
     e2:     0;
```

B.3 Mutual Exclusion

The model of the transition system in the example in Section 8 is as follows.

```
VAR
     p1: {s0,s1,s2};
     p2: {s0,s1,s2};
     y1: nat;
     y2: nat;
TRANS
     p1=s0:                   (p1,y1):=(s1,y2+1);
     p1=s1&(y2=0|y1<=y2):     (p1):=(s2);
     p1=s2:                   (p1,y1):=(s0,0);
     p2=s0:                   (p2,y2):=(s1,y1+1);
     p2=s1&(y1=0|!(y1<=y2)): (p2):=(s2);
     p2=s2:                   (p2,y2):=(s0,0);
```

Preparation of the rest of the contents for input to the verification condition generation tool is in accordance with the description in Section 8 using the format presented in the previous subsections for verification and falsification of temporal properties. A characterization of the function symbol e_0 used for proving the 4th property, which was not explicitly given in Section 8, is presented as follows.

		$e_0(s_1, s_0, y_1, 0)$	$\sqsubset$	4
		$e_0(s_1, s_1, y_1, y_2)$	$\sqsubset$	4
		$e_0(s_1, s_2, y_1, y_2)$	$\sqsubset$	4
		$e_0(s_0, s_1, y_1, y_1 + 1)$	$\sqsubset$	$e_0(s_0, s_0, y_1, 0)$
		$e_0(s_0, s_2, 0, y_2)$	$\sqsubset$	$e_0(s_0, s_1, 0, y_2)$
		$e_0(s_0, s_0, y_1, 0)$	$\sqsubset$	$e_0(s_0, s_2, y_1, y_2)$
		$e_0(s_0, s_2, y_1, y_2)$	$\sqsubset$	$e_0(s_0, s_1, y_1, y_2)$
		$e_0(s_1, s_0, 1, 0)$	$\sqsubset$	$e_0(s_0, s_0, y_1, 0)$
		$e_0(s_1, s_2, y_2 + 1, y_2)$	$\sqsubset$	$e_0(s_0, s_2, y_1, y_2)$
		$e_0(s_1, s_1, y_2 + 1, y_2)$	$\sqsubset$	$e_0(s_0, s_1, y_1, y_2)$
		$e_0(s_1, s_0, y_1, 0)$	$\sqsubset$	$e_0(s_1, s_2, y_1, y_2)$
		$e_0(s_1, s_1, y_1, y_1 + 1)$	$\sqsubset$	$e_0(s_1, s_0, y_1, 0)$
$y_1 > y_2$	$\rightarrow$	$e_0(s_1, s_2, y_1, y_2)$	$\sqsubset$	$e0(s_1, s_1, y_1, y_2)$

Notice that if the domain is specified as integers instead of natural numbers, we may need additional axioms for dismissing the verification conditions.

References

1. R. Bagnara, F. Mesnard, A. Pescetti and E. Zaffanella. A new look at the automatic synthesis of linear ranking functions. Information and Computation (2012) 215: 47-67.
2. J. A. Bergstra and J. V. Tucker. Expressiveness and the completeness of Hoares logic, J. Comput. System Sci. (1982) 25: 267-284.
3. D. Beyer, T. A. Henzinger, R. Majumdar and A. Rybalchenko. Invariant synthesis for combined theories. VMCAI 2007: 378-394.
4. A. Bradley and Z. Manna. Property-directed incremental invariant generation. Form Asp Comp (2008) 20(4-5): 379-405.
5. M. Brockschmidt, B. Cook, S. Ishtiaq, H. Khlaaf and N. Piterman. T2: Temporal property verification. TACAS 2016: 387-393.
6. F. Buccafurri, T. Eiter, G. Gottlob and N. Leone. On ACTL formulas having linear counterexamples. Journal of Computer and System Sciences (2001) 62: 463-515.
7. C.-L. Chang and R. C.-T. Lee. Symbolic logic and mechanical theorem proving. Academic Press. 1973.
8. E. M. Clarke and E. Allen Emerson. Design and synthesis of synchronization skeletons using branching-time temporal logic. Logic of Programs 1981: 52-71.
9. S. A. Cook. Soundness and completeness of an axiom system for program verification, SIAM J. Comput. (1978) 7: 70-90.
10. B. Cook, H. Khlaaf and N. Piterman. On automation of CTL* verification for infinite-state systems. CAV (1) 2015: 13-29.
11. B. Cook, H. Khlaaf and N. Piterman. Verifying increasingly expressive temporal logics for infinite-state systems. J. ACM (2017) 64, 2, Article 15.

12. E. Allen Emerson and E. M. Clarke. Using branching time temporal logic to synthesize synchronization skeletons. Sci. Comput. Program. (1982) 2(3): 241-266.
13. E. Allen Emerson and J. Y. Halpern. "Sometimes" and "Not Never" revisited: on branching versus linear time temporal logic. J. ACM (1986) 33(1): 151-178.
14. M. Fitting. First-order logic and automated theorem proving. Springer. 1996.
15. L. Fix and O. Grumberg. Verification of temporal properties. J. Log. Comput. (1996) 6(3): 343-361.
16. R. W. Floyd. Assigning meanings to programs. Proceedings of the American Mathematical Society Symposia on Applied Mathematics, 1967, Vol. 19, pp. 19-31.
17. D. M. Gabbay and A. Pnueli. A sound and complete deductive system for CTL* verification. Logic Journal of the IGPL (2008) 16(6): 499-536.
18. L. Gonnord, D. Monniaux and G. Radanne. Synthesis of ranking functions using extremal counterexamples. PLDI 2015: 608-618.
19. E. Pascal Gribomont. A programming logic for formal concurrent systems. CONCUR 1990: 298-313.
20. C. A. R. Hoare. An axiomatic basis for computer programming. Communications of the ACM (1969) 12(10): 576-580.
21. Y. Kestena and A. Pnueli. A compositional approach to CTL* verification. Theoretical Computer Science (2005) 331: 397-428.
22. D. Kozen and J. Tiuryn. On the completeness of propositional Hoare logic, Inform. Sci. (2001) 139: 187-195.
23. L. Lamport. A new solution of Dijkstra's concurrent programming problem. Commun. ACM (1974) 17(8): 453-455.
24. J. Loeckx and K. Sieber. The foundation of program verification. John Wiley & Sons Ltd. 1984.
25. S. S. Owicki and D. Gries. Verifying properties of parallel programs: An axiomatic approach. Commun. ACM (1976) 19(5): 279-285.
26. S. S. Owicki and D. Gries. An axiomatic proof technique for parallel programs I. Acta Informatica (1976) 6(4): 319-340.
27. A. Podelski and A. Rybalchenko: A complete method for the synthesis of linear ranking functions. VMCAI 2004: 239-251.
28. Z. Manna and A. Pnueli. How to cook a temporal proof system for your pet language. Acm Sigact-sigplan Symposium on Principles of Programming Languages, 1983, pp. 141-154.
29. Z. Manna and A. Pnueli. Completing the temporal picture. Theoretical Computer Science (1991) 83(1): 97-130.
30. Z. Manna and A. Pnueli. Temporal verification of reactive systems: Safety. Springer. 1995.
31. Z. Manna and A. Pnueli. Temporal verification of reactive systems: Response. Essays in Memory of Amir Pnueli 2010: 279-361.
32. D. A. Peled. Deductive software verification. In: Software Reliability Methods, pp. 179-214. Springer. 2001.
33. A. Pnueli. The temporal logic of programs. FOCS 1977: 46-57.
34. A. Pnueli and Y. Kesten. A deductive proof system for CTL*. CONCUR 2002, LNCS 2421, pp. 24-40.
35. M. Y. Vardi and P. Wolper. An automata-theoretic approach to automatic program verification. LICS 1986: 332-344.
36. Z. Xu, Y. Sui and W. Zhang. Completeness of Hoare logic with inputs over the standard model. Theoretical Computer Science (2016) 612: 23-28.