# A Proof System for a Unified Temporal Logic

Liang Zhao[1], Xiaobing Wang[1(✉)], Xinfeng Shu[2(✉)], and Nan Zhang[1]

[1] Institute of Computing Theory and Technology and ISN Laboratory,
Xidian University, P.O. Box 177, Xi'an 710071, People's Republic of China
{lzhao,nanzhang}@xidian.edu.cn, xbwang@mail.xidian.edu.cn

[2] School of Computer Science and Technology, Xi'an University of Posts
and Communications, Xi'an 710061, People's Republic of China
shuxf@xupt.edu.cn

**Abstract.** Theorem proving is a widely used approach to the verification of computer systems, and its theoretical basis is generally a proof system for formal derivation of logic formulas. In this paper, we propose a proof system for Propositional Projection Temporal Logic (PPTL) with indexed expressions, which is a unified temporal logic that subsumes the well-used Linear Temporal Logic (LTL). First, the syntax, semantics and logic laws of PPTL that allows indexed expressions are introduced, and the representation of LTL constructs by PPTL formulas is shown. Then, the proof system for the logic is presented which consists of axioms and inference rules for the derivation of both basic constructs and indexed expressions of PPTL. To show the capability of the proof system, several examples of formal proofs are provided. Finally, the soundness of the proof system is demonstrated.

**Keywords:** Theorem proving · Proof system · Temporal Logic · Indexed expression · Soundness

## 1 Introduction

Projection Temporal Logic (PTL) [3] is an extension of Interval Temporal Logic (ITL) [13] by introducing a new projection construct and supporting both finite and infinite timeline. Within the PTL framework, Propositional PTL (PPTL) is proved to have the full regular expressiveness [18], and its decision problem has been solved [5]. Further, Modeling, Simulation and Verification Language (MSVL) [7], an executable subset of PTL armed with a framing technique, is defined as the language for system modeling. Based on these theoretical work, a unified *model checking* [2] approach with PTL is developed for formal verification of computer systems [4,20].

This research is supported by the NSFC Grant Nos. 61751207, 61732013, 61672403, and 61572386.

D.-Z. Du et al. (Eds.): COCOON 2019, LNCS 11653, pp. 663–676, 2019.
https://doi.org/10.1007/978-3-030-26176-4_55

The advantage of the model checking approach is that verification can be done automatically. However, it suffer from the state explosion problem and thus less suitable to verify data intensive applications. Another approach to system verification widely used in practice is *theorem proving* [10], in which a *proof system* for a specific logic, usually a temporal logic, is constructed in terms of axioms and inference rules. To verify whether a computer system satisfies a desired property, both the system and the property are characterized by formulas $S$ and $P$ of the logic, respectively. Then, the problem is to check whether $S \rightarrow P$ can be proved formally by the axioms and inference rules of the proof system. Generally, such a verification process involves human assistance and can be done semi-automatically. The advantage of theorem proving is that it avoids the state explosion problem and can verify both finite-state and infinite-state systems, including data intensive applications.

In the past three decades, a number of proof systems for Liner Temporal Logic (LTL), Computing Tree Logic (CTL) and other temporal logics have emerged [9,11,12]. However, the expressive power of these logics is weaker than ITL or PPTL. Within the ITL community, several researchers have investigated axiomatic systems with different extensions. Rosner and Pnueli [16] present a proof system for a propositional choppy logic with chop, next and until operators. Bowman and Thompson provide a completeness proof and a tableau-based decision procedure for PITL with projection over finite intervals [1]. Moszkowski proposes an axiom system over finite intervals for PITL, and later extends the work to infinite intervals [14]. Besides, two proof systems are formalized for PPTL [8] and PTL [17], respectively.

A recent study [6] extends PPTL with *indexed expressions* that take the form of $\bigvee_{i \in \mathbb{N}} R[i]$. Although indexed expressions are obtained by applying the syntax rules countably infinitely many times, they have definite semantics and certain good properties. Especially, they can equivalently represent the strong until $\mathsf{U}$ and weak until $\mathsf{W}$ constructs of LTL. As a result, PPTL with indexed expressions is a unified temporal logic that involves LTL as one of its subsets.

To employ PPTL and the indexed-expression technique to system verification in the theorem proving approach, we develop a proof system $\Pi$ for the unified logic in this paper. Specifically, $\Pi$ consists of two sub-systems of axioms and inference rules. The first sub-system is provided for formal proof of basic PPTL constructs, such as next, projection, always and chop plus. The second subsystem is designed especially for formal derivation of formulas with indexed expressions. We provide a few examples to show how the proof system $\Pi$ works, and demonstrate its soundness that every formula proved by $\Pi$ is valid.

The paper is organized as follows. The next section introduces PPTL, including indexed expressions and their capability of representing LTL. Then, Sect. 3 presents our proof system in terms of axioms and inference rules and Sect. 4 provides examples of formal proofs with the proof system. In Sect. 5, the soundness of the proof system is demonstrated. Finally, conclusions are drawn in Sect. 6 with a discussion on potential future work.

## 2 Propositional Projection Temporal Logic

We first introduce basic notions of Propositional Projection Temporal Logic (PPTL) [3]. Let $\mathcal{P}$ be a countable set of atomic propositions and $\mathbb{B} = \{tt, \mathit{ff}\}$ the boolean domain. Usually, we use small letters, possibly with subscripts, like $p, q, r_1$, to denote atomic propositions in $\mathcal{P}$ and capital letters, possibly with subscripts, like $P, Q, R_1$, to represent general PPTL formulas. Formally, the formulas of PPTL are inductively defined by the following syntax:

$$\begin{array}{ll} P & ::= q \mid \neg P \mid P \wedge P \mid \bigcirc P \mid (P^{[+]})\,\mathsf{prj}\ P \\ P^{[+]} & ::= P \mid P, P^{[+]} \end{array}$$

where $P^{[+]}$ represents a finite sequence of PPTL formulas separated by commas. For simplicity, some previous publications of PPTL, such as [3,18], use the syntax defined as follows.

$$P ::= q \mid \neg P \mid P_1 \wedge P_2 \mid \bigcirc P \mid (P_1, \ldots, P_m)\,\mathsf{prj}\ P$$

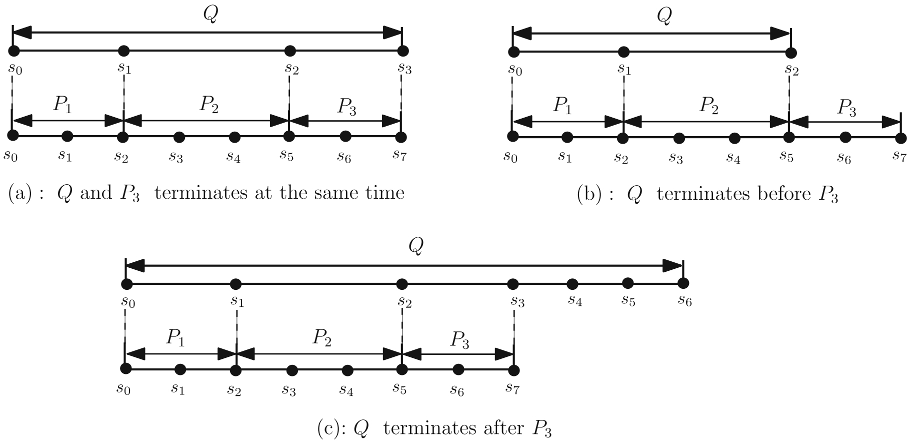
It is trivial to prove that the two definitions are equivalent. Notice that $\bigcirc$ (next), and $\mathsf{prj}$ (projection) are temporal operators, while $\neg$ and $\wedge$ are defined as they are in classical propositional logic. A formula is called a *state formula* if it does not contain any temporal operators.

In the semantics of PTL, formulas are interpreted upon intervals. An *interval* $\sigma = \langle s_0, s_1, \ldots \rangle$ is a non-empty sequence of states, finite or infinite, while a *state* $s$ is a mapping from $\mathcal{P}$ to $\mathbb{B}$. The length of an interval $\sigma$, denoted as $|\sigma|$, is the number of states in $\sigma$ minus one if $\sigma$ is finite; or the smallest infinite ordinal $\omega$ if $\sigma$ is infinite. Let $\mathbb{N}$ denote the set of natural numbers. To have a uniform notation for both finite and infinite intervals, we use *extended natural numbers* as indices, that is $\mathbb{N}_\omega = \mathbb{N} \cup \{\omega\}$, and extend the comparison operators, $=, <, \leq$, to $\mathbb{N}_\omega$ by considering $\omega = \omega$ and for all $i \in \mathbb{N}$, $i < \omega$. Moreover, we write $\preceq$ as $\leq -\{(\omega, \omega)\}$. To simplify definitions, we denote $\sigma$ by $\langle s_0, \cdots, s_{|\sigma|} \rangle$, where $s_{|\sigma|}$ is undefined if $\sigma$ is infinite. With such a notation, $\sigma_{(i..j)}$ $(0 \leq i \preceq j \leq |\sigma|)$ denotes a sub-interval $\langle s_i, \cdots, s_j \rangle$.

To formalize the semantics of the projection construct $\mathsf{prj}$, we define an auxiliary operator $\downarrow$ to get rid of singleton points. For an interval $\sigma$ and natural numbers $i_0 \leq \ldots \leq i_m$ $(m \in \mathbb{N})$, $\sigma \downarrow (i_0, \ldots, i_m)$ denotes the interval obtained from $\sigma$ by preserving only states with non-repeated indices from $i_l$ $(0 \leq l \leq m)$. For example, $\langle s_0, s_1, s_2, s_3, s_4 \rangle \downarrow (0, 0, 2, 2, 2, 3) = \langle s_0, s_2, s_3 \rangle$. In addtion, we use $\sigma \cdot \sigma'$ to denote the *concatenation* of two intervals $\sigma$ and $\sigma'$, provided $\sigma$ is finite.

An *interpretation* is a tuple $\mathcal{I} = (\sigma, k, j)$, where $\sigma = \langle s_0, s_1, \ldots \rangle$ is an interval, $k \in \mathbb{N}$ and $j \in \mathbb{N}_\omega$ with $0 \leq k \leq j \leq |\sigma|$. For a PPTL formula $P$, $\mathcal{I} \models P$ denotes that $\mathcal{I}$ is an interpretation of $P$, defined inductively as follows. Intuitively, it means that $P$ is interpreted over the subinterval $\sigma_{(k..j)}$ of $\sigma$ with the current state being $s_k$.

$$
\begin{array}{ll}
\mathcal{I} \models p & \text{iff } s_k(p) = \ tt \\
\mathcal{I} \models \neg P & \text{iff } \mathcal{I} \not\models P \\
\mathcal{I} \models P_1 \wedge P_2 & \text{iff } \mathcal{I} \models P_1 \text{ and } \mathcal{I} \models P_2 \\
\mathcal{I} \models \bigcirc P & \text{iff } k < j \text{ and } (\sigma, k+1, j) \models P \\
\mathcal{I} \models (P_1, \ldots, P_m) \ \mathsf{prj} \ Q & \text{iff there exist (extended) natural numbers } k = i_0 \leq \ldots \leq i_{m-1} \\
 & \preceq i_m \leq j \text{ such that } (\sigma, i_{l-1}, i_l) \models P_l \text{ for all } 1 \leq l \leq m \\
 & \ \text{and } (\sigma', 0, |\sigma'|) \models Q \text{ for } \sigma' \text{ given by either} \\
 & (1)\ \sigma' \ = \ \sigma \downarrow (i_0, \ldots, i_m) \cdot \sigma_{(i_m+1, \ldots, j)} \quad \text{if } i_m < j, \text{ or} \\
 & (2)\ \sigma' \ \text{ is a prefix of } \sigma \downarrow (i_0, \ldots, i_m) \qquad \text{if } i_m = j.
\end{array}
$$


Q
$s_0$ $s_1$ $s_2$ $s_3$
$P_1$ $P_2$ $P_3$
$s_0$ $s_1$ $s_2$ $s_3$ $s_4$ $s_5$ $s_6$ $s_7$
Q
$s_0$ $s_1$ $s_2$
$P_1$ $P_2$ $P_3$
$s_0$ $s_1$ $s_2$ $s_3$ $s_4$ $s_5$ $s_6$ $s_7$
Q
$s_0$ $s_1$ $s_2$ $s_3$ $s_4$ $s_5$ $s_6$
$P_1$ $P_2$ $P_3$
$s_0$ $s_1$ $s_2$ $s_3$ $s_4$ $s_5$ $s_6$ $s_7$

(a) : $Q$ and $P_3$ terminates at the same time

(b) : $Q$ terminates before $P_3$

(c): $Q$ terminates after $P_3$

**Fig. 1.** Possible interpretations of $(P_1, P_2, P_3)\ \mathsf{prj}\ Q$

The projection construct $(P_1, \ldots, P_m)\ \mathsf{prj}\ Q$ is a key operator of PPTL, which has potential applications for compositional reasoning about concurrent systems. The construct allows formulas $P_1, \ldots, P_m, Q$ to be autonomous, each interpreted in its own interval. Specifically, two different time scales exist, where $P_1, \ldots, P_m$ are interpreted over a series of fine-grained intervals while $Q$ is interpreted over a coarse-grained projected interval. In particular, the sequence of $P_1, \ldots, P_m$ and $Q$ may terminate at different time points. The intuition of $(P_1, P_2, P_3)\ \mathsf{prj}\ Q$ is shown in Fig. 1.

A formula $P$ is satisfied by an interval $\sigma$, denoted by $\sigma \models P$, if $(\sigma, 0, |\sigma|) \models P$. A formula $P$ is *satisfiable* if $\sigma \models P$ for some $\sigma$ while a formula $P$ is *valid*, denoted by $\models P$, if $\sigma \models P$ for all intervals $\sigma$. The abbreviations such as *tt*, *ff*, $\vee$, $\rightarrow$ and $\leftrightarrow$ are defined as usual. Some derived formulas of PPTL are shown below. They are useful in characterizing various temporal properties.

$$\begin{array}{lll@{\qquad}lll}
\varepsilon & \overset{\text{def}}{=} & \neg \bigcirc tt & P\,;Q & \overset{\text{def}}{=} & (P, Q)\ \mathsf{prj}\ \varepsilon \\
\Diamond P & \overset{\text{def}}{=} & tt\,;P & \Box P & \overset{\text{def}}{=} & \neg\Diamond\neg P \\
P^{+} & \overset{\text{def}}{=} & (P^{[+]})\ \mathsf{prj}\ \varepsilon & P^{*} & \overset{\text{def}}{=} & \varepsilon \vee P^{+} \\
\mathsf{halt}(P) & \overset{\text{def}}{=} & \Box(\varepsilon \leftrightarrow P) & \mathsf{final}(P) & \overset{\text{def}}{=} & \Box(\varepsilon \rightarrow P) \\
\mathsf{keep}(P) & \overset{\text{def}}{=} & \Box(\bigcirc tt \rightarrow P) & \mathsf{rem}(P) & \overset{\text{def}}{=} & \Box(\bigcirc tt \rightarrow \bigcirc P) \\
\mathsf{fin} & \overset{\text{def}}{=} & \Diamond\varepsilon & \mathsf{ln}(n) & \overset{\text{def}}{=} & \begin{cases} \varepsilon & \text{if } n = 0 \\ \bigcirc\mathsf{ln}(n-1) & \text{if } n \geq 1 \end{cases} \\
\mathsf{inf} & \overset{\text{def}}{=} & \Box \bigcirc tt & P \parallel Q & \overset{\text{def}}{=} & P \wedge (Q\,;tt) \vee Q \wedge (P\,;tt)
\end{array}$$

The *empty* formula $\varepsilon$ means that the current state is the last one of the interval, and the *chop* construct $P;Q$ means the sequential composition of $P$ and $Q$. Besides, the *sometimes* construct $\Diamond P$ (resp. *always* construct $\Box P$) indicates $P$ holds at some state (resp. every state) from the current state on. The meaning of the *chop plus* construct $P^{+}$ (resp. *chop star* construct $P^{*}$) is as usual, i.e., $P$ holds repeatedly for one or more (resp. zero or more) times. Then, $\mathsf{halt}(P)$ and $\mathsf{final}(P)$ say that $P$ holds at the last state of the interval, while $\mathsf{halt}(P)$ also requires $P$ holds only at the last state. The formula $\mathsf{keep}(P)$ (resp. $\mathsf{rem}(P)$) means that $P$ holds at every state that has a next (resp. previous) state in the interval. In addition, $\mathsf{fin}$ (resp. $\mathsf{inf}$) indicates the interval is finite (resp. infinite), and $\mathsf{ln}(n)$ claims that the length of the remaining interval is exactly $n$. Finally, the *parallel* construct $P \parallel Q$ means that $P$ and $Q$ are interpreted in parallel.

We denote $\models P \leftrightarrow Q$ by $P \equiv Q$ (*equivalence*), and $\models P \rightarrow Q$ by $P \subset Q$ (*strong implication*). Some logic laws of PPTL are provided as follows, whose proofs can be found in [3].

$$\begin{array}{ll@{\qquad}ll}
\Diamond P & \equiv P \vee \bigcirc\Diamond P & \Box P & \equiv P \wedge \varepsilon \vee P \wedge \bigcirc\Box P \\
P^{+} & \equiv P \vee (P\,;P^{+}) & Q\,;(P_1 \vee P_2) & \equiv (Q\,;P_1) \vee (Q\,;P_2) \\
\Box\neg Q & \equiv \neg\Diamond Q & \mathsf{keep}(P) & \equiv \varepsilon \vee P \wedge \bigcirc\mathsf{keep}(P) \\
\Box P \vee \Box Q & \subset \Box(P \vee Q) & \mathsf{halt}(P) & \equiv P \wedge \varepsilon \vee \neg P \wedge \bigcirc\mathsf{halt}(P) \\
\Box(P \wedge Q) & \equiv \Box P \wedge \Box Q & \mathsf{final}(P) & \equiv P \wedge \varepsilon \vee \bigcirc\mathsf{final}(P) \\
tt & \equiv \mathsf{fin} \vee \mathsf{inf} & \mathsf{rem}(P) & \equiv \varepsilon \vee \bigcirc P \wedge \bigcirc\mathsf{rem}(P) \\
\bigcirc(P \vee Q) & \equiv \bigcirc P \vee \bigcirc Q & \Box(P \wedge \bigcirc tt) & \equiv P \wedge \bigcirc\Box(P \wedge \bigcirc tt) \\
\bigcirc(P \wedge Q) & \equiv \bigcirc P \wedge \bigcirc Q & \Box(P \rightarrow Q) & \subset \Box P \rightarrow \Box Q \\
\bigcirc\neg P & \equiv \bigcirc tt \wedge \neg \bigcirc P & P_1\,;(P_2\,;P_3) & \equiv (P_1\,;P_2)\,;P_3
\end{array}$$

### 2.1 Indexed Expression

Generally, a *well-formed* formula of PPTL is constructed by applying the syntax rules finitely many times. However, some formulas formed by applying the syntax rules countably infinitely many times, such as $\bigvee_{i \in \mathbb{N}} \bigcirc^{i} P$, have definite semantics and good properties.

A recent work [6] studies a kind of such formulas, namely *indexed expressions*, which are of the form $\bigvee_{i\in\mathbb{N}} R[i]$ where $R[i]$ is a well-formed formula with an index $i \in \mathbb{N}$. Specifically, $R[i]$ may contain sub-formulas such as $\bigcirc^i P$, $P^i$ and $P^{(i)}$. For $i \in \mathbb{N}$, $\bigcirc^i P$ is the application of the next operator to $P$ for $i$ times, $P^i$ means $P$ holds repeatedly for $i$ times, while $P^{(i)}$ means $P$ holds at the consecutive $i$ states from the current state on. Formally, they are defined as follows.

$$\bigcirc^i P \stackrel{\text{def}}{=} \begin{cases} P & \text{if } i = 0 \\ \bigcirc \bigcirc^{i-1} P & \text{if } i \geq 1 \end{cases} \qquad P^i \stackrel{\text{def}}{=} \begin{cases} \varepsilon & \text{if } i = 0 \\ P^{i-1} \,;\, P & \text{if } i \geq 1 \end{cases}$$

$$P^{(i)} \stackrel{\text{def}}{=} \begin{cases} tt & \text{if } i = 0 \\ P & \text{if } i = 1 \\ P \wedge \bigcirc P^{(i-1)} & \text{if } i > 1 \end{cases}$$

The semantics of an indexed expression is clear. Let $\mathcal{I}$ be an interpretation.

$$\mathcal{I} \models \bigvee_{i\in\mathbb{N}} R[i] \qquad \text{iff there exists } i \in \mathbb{N} \text{ such that } \mathcal{I} \models R[i]$$

Intuitively, $\bigvee_{i\in\mathbb{N}} R[i]$ means some $R[i]$ holds for $i \in \mathbb{N}$. From now on, we consider PPTL with indexed expressions in that a formula may contain indexed expression(s) as its sub-formula(s). Nevertheless, it is good that indexed expressions do not occur nested, since $R[i]$ in $\bigvee_{i\in\mathbb{N}} R[i]$ is a well-formed formula.

To avoid excessive use of parentheses, we specify the precedence of operators as: 1. $+$, $*$; 2. $\neg$, $\bigcirc$, $\Box$, $\Diamond$, $\mathsf{prj}$; 3. $\wedge$; 4. $\bigvee_{i\in\mathbb{N}}$; 5. $\vee$; 6. $;$; 7. $\|$; 8. $\rightarrow$; 9. $\leftrightarrow$, where 1 = highest and 9 = lowest.

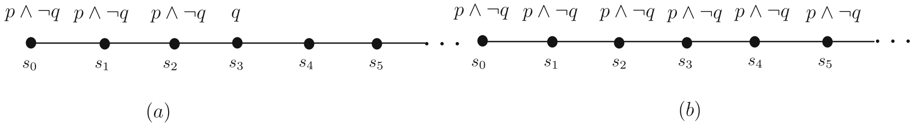


**Fig. 2.** Intuitive meaning of $p \mathsf{U} q$ (see (a)) and $p \mathsf{W} q$ (see (a) or (b))

Indexed expressions of the form $\bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i Q$ are closely related to the recursive equation $X \equiv Q \vee P \wedge \bigcirc X$ [6], shown by the following lemmas.

**Lemma 1.** *The recursive equation* $X \equiv Q \vee P \wedge \bigcirc X$ *has exactly two solutions:* $\bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i Q$ *and* $\bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i Q \vee \Box(P \wedge \bigcirc tt)$.

**Lemma 2.** *Let* $X$ *be a formula satisfying* $X \equiv Q \vee P \wedge \bigcirc X$*, then*

*1.* $X \subset \Diamond Q$ *iff* $X \equiv \bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i Q$*, and*
*2.* $\Box(P \wedge \bigcirc tt) \subset X$ *iff* $X \equiv \bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i Q \vee \Box(P \wedge \bigcirc tt)$.

Many cases of indexed expressions are intrinsically well-formed in that they are equivalent to well-formed formulas. Specifically, we have the following logic laws. Most of the laws are proved using the above lemmas, the others are proved by the fixed-point induction approach [19].

$$\begin{array}{llll}
\bigvee_{i\in\mathbb{N}} \bigcirc^i Q & \equiv \Diamond Q & \bigvee_{i\in\mathbb{N}} Q^i & \equiv Q^* \\
\bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i (P \wedge \varepsilon) & \equiv \Box P \wedge \Diamond \varepsilon & \bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i \varepsilon & \equiv \mathsf{keep}(P) \wedge \Diamond \varepsilon \\
\bigvee_{i\in\mathbb{N}} (\neg P)^{(i)} \wedge \bigcirc^i (P \wedge \varepsilon) & \equiv \mathsf{halt}(P) \wedge \Diamond \varepsilon & \bigvee_{i\in\mathbb{N}} (\bigcirc P)^{(i)} \wedge \bigcirc^i \varepsilon & \equiv \mathsf{rem}(P) \wedge \Diamond \varepsilon
\end{array}$$

$$\begin{array}{ll}
\bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i (P \wedge \varepsilon) \vee \Box(P \wedge \bigcirc tt) & \equiv \Box P \\
\bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i \varepsilon \vee \Box(P \wedge \bigcirc tt) & \equiv \mathsf{keep}(P) \\
\bigvee_{i\in\mathbb{N}} (\neg P)^{(i)} \wedge \bigcirc^i (P \wedge \varepsilon) \vee \Box(\neg P \wedge \bigcirc tt) & \equiv \mathsf{halt}(P) \\
\bigvee_{i\in\mathbb{N}} (\bigcirc P)^{(i)} \wedge \bigcirc^i \varepsilon \vee \Box(\bigcirc P \wedge \bigcirc tt) & \equiv \mathsf{rem}(P)
\end{array}$$

### 2.2 Representing Linear Temporal Logic

Linear Temporal Logic (LTL) [15] is a well-known temporal logic, which is based on a linear-time perspective and defined over an infinite interval. Usually, LTL refers to the propositional subset of LTL which has been widely used in practice. In LTL, the most prominent operators are *strong until* $\mathsf{U}$ and *weak until* $\mathsf{W}$, which is a weak version of $\mathsf{U}$. Their intuitive meanings are shown in Fig. 2 and more details can be found in [2].

We show that both the strong until and weak until operators can be represented as PPTL formulas with indexed expressions. Suppose $(P \,\mathsf{U}\, Q)_{\mathsf{P}}$ and $(P \,\mathsf{W}\, Q)_{\mathsf{P}}$ are PPTL formulas that have the same meaning as $P \,\mathsf{U}\, Q$ and $P \,\mathsf{W}\, Q$, respectively. Then, both $(P \,\mathsf{U}\, Q)_{\mathsf{P}}$ and $(P \,\mathsf{W}\, Q)_{\mathsf{P}}$ satisfy the recursive equation $X \equiv Q \wedge \mathsf{inf} \vee P \wedge \neg Q \wedge \bigcirc X$. In addition, they satisfy $(P \,\mathsf{U}\, Q)_{\mathsf{P}} \subset \Diamond(Q \wedge \mathsf{inf})$ and $\Box(P \wedge \neg Q \wedge \bigcirc tt) \subset (P \,\mathsf{W}\, Q)_{\mathsf{P}}$. According to Lemma 2, we have

$$\begin{array}{l}
(P \,\mathsf{U}\, Q)_{\mathsf{P}} \;\equiv \bigvee_{i\in\mathbb{N}} (P \wedge \neg Q)^{(i)} \wedge \bigcirc^i (Q \wedge \mathsf{inf}) \equiv \mathsf{inf} \wedge \bigvee_{i\in\mathbb{N}} (P \wedge \neg Q)^{(i)} \wedge \bigcirc^i Q, \text{ and} \\
(P \,\mathsf{W}\, Q)_{\mathsf{P}} \equiv \mathsf{inf} \wedge \bigvee_{i\in\mathbb{N}} (P \wedge \neg Q)^{(i)} \wedge \bigcirc^i Q \vee \Box(P \wedge \neg Q \wedge \bigcirc tt).
\end{array}$$

Therefore, we can simply define the two operators in PPTL in the following way.

$$\begin{array}{l}
P \,\mathsf{U}\, Q \overset{\text{def}}{=} \mathsf{inf} \wedge \bigvee_{i\in\mathbb{N}} (P \wedge \neg Q)^{(i)} \wedge \bigcirc^i Q, \text{ and} \\
P \,\mathsf{W}\, Q \overset{\text{def}}{=} \mathsf{inf} \wedge \bigvee_{i\in\mathbb{N}} (P \wedge \neg Q)^{(i)} \wedge \bigcirc^i Q \vee \Box(P \wedge \neg Q \wedge \bigcirc tt).
\end{array}$$

On the other hand, except $\mathsf{U}$ and $\mathsf{W}$, every construct of LTL has a direct counterpart in PPTL. As a result, PPTL with indexed expressions is a unified temporal logic that subsumes LTL.

## 3 Proof System

This section presents the proof system $\Pi$ for PPTL with indexed expressions, consisting of a set of *axioms* and *inference rules*. Each axiom defines a formula that can be directly derived by the system, and each inference rule defines a one-step derivation of a conclusion formula from one or more hypothesis formulas.

A *formal proof* (or *formal derivation*) of a formula $P$ is a sequence of formulas $P_0, \ldots, P_n$ $(n \in \mathbb{N})$ such that $P_n = P$ and each $P_i$ $(0 \leq i \leq n)$ is either an axiom or the conclusion formula of an inference rule, provided every hypothesis formula of the rule has occurred in the preceding formulas $P_0, \ldots, P_{i-1}$. If such a formal proof exists, we say that $P$ is proved by $\Pi$ or $P$ is a *theorem* of $\Pi$, denoted as $\vdash_{\Pi} P$. When there is no confusion, we omit the subscript and simply write $\vdash P$.

Specifically, the proof system $\Pi$ is composed of two parts: axioms and inference rules $\Pi_B$ for basic constructs, such as next and projection, and those $\Pi_I$ for indexed expressions, i.e. $\Pi = \Pi_B \cup \Pi_I$.

### 3.1 Axioms and Inference Rules for Basic Constructs

A proof system for basic constructs of PPTL has been proposed in [8], which adopts a relatively complex version of syntax that considers a projection-plus construct $(P_1, \ldots, (P_i, \ldots, P_j)^{\oplus}, \ldots, P_m)\ \mathsf{prj}\ Q$ as a basic construct. Here, we provide $\Pi_B$, an equivalent but more concise presentation of the proof system, based on the current version of syntax considering the projection construct instead of the projection-plus construct.

Let $S$ denote a state formula and $\Omega$ represent a finite sequence of formulas, which is possible the empty sequence $\tau$. For convenience, we define $(\tau)\ \mathsf{prj}\ P$ to be $P$. The set of axioms of $\Pi_B$ are presented as follows.

| | | | |
|---|---|---|---|
| TAU | $\psi$ where $\psi$ is an instance of a propositional tautology | | |
| POF | $(\Omega_1, P_1 \vee P_2, \Omega_2)\ \mathsf{prj}\ Q \leftrightarrow (\Omega_1, P_1, \Omega_2)\ \mathsf{prj}\ Q \vee (\Omega_1, P_2, \Omega_2)\ \mathsf{prj}\ Q$ | | |
| POB | $(\Omega)\ \mathsf{prj}\ (Q_1 \vee Q_2) \leftrightarrow (\Omega)\ \mathsf{prj}\ Q_1 \vee (\Omega)\ \mathsf{prj}\ Q_2$ | | |
| PFN | $(\Omega_1, P_1, P_2, \Omega_2)\ \mathsf{prj}\ Q \leftrightarrow (\Omega_1, P_1 \wedge \mathsf{fin}, P_2, \Omega_2)\ \mathsf{prj}\ Q$ | | |
| PIN | $(\Omega, P \wedge \mathsf{inf})\ \mathsf{prj}\ Q \leftrightarrow (\Omega, P \wedge \mathsf{inf})\ \mathsf{prj}\ (Q \wedge \mathsf{fin})$ | | |
| PSM | $(\Omega_1, S \wedge \varepsilon, P, \Omega_2)\ \mathsf{prj}\ Q \leftrightarrow (\Omega_1, S \wedge P, \Omega_2)\ \mathsf{prj}\ Q$ | | |
| PSF | $(S \wedge P, \Omega)\ \mathsf{prj}\ Q \leftrightarrow S \wedge (P, \Omega)\ \mathsf{prj}\ Q$ | PSB | $(\Omega)\ \mathsf{prj}\ (S \wedge Q) \leftrightarrow S \wedge (\Omega)\ \mathsf{prj}\ Q$ |
| PEF | $(\Omega, \varepsilon)\ \mathsf{prj}\ Q \leftrightarrow (\Omega)\ \mathsf{prj}\ Q$ | PEB | $(P)\ \mathsf{prj}\ \varepsilon \leftrightarrow P$ |
| PNX | $(\bigcirc P, \Omega)\ \mathsf{prj}\ \bigcirc Q \leftrightarrow \bigcirc((P, \Omega)\ \mathsf{prj}\ Q)$ | CPR | $P^{+} \leftrightarrow P \vee (P \wedge \bigcirc tt\ ; P^{+})$ |
| NXN | $\bigcirc \neg P \leftrightarrow \neg(\varepsilon \vee \bigcirc P)$ | NXA | $\bigcirc(P \wedge Q) \leftrightarrow \bigcirc P \wedge \bigcirc Q$ |
| CNX | $\bigcirc P\ ; Q \leftrightarrow \bigcirc(P\ ; Q)$ | CAS | $P_1\ ; (P_2\ ; P_3) \leftrightarrow (P_1\ ; P_2)\ ; P_3$ |
| STN | $P \wedge \Diamond \neg P \to \Diamond(P \wedge \bigcirc \neg P)$ | ALR | $\Box P \leftrightarrow P \wedge (\varepsilon \vee \bigcirc \Box P)$ |

Intuitively, an axiom is a formula that is supposed to be valid. Especially, the validity of a formula $P \leftrightarrow Q$ means that $P$ and $Q$ are equivalent.

The set of inference rules of $\Pi_B$ are presented as follows.

| | | | |
|---|---|---|---|
| MP | $\dfrac{P \quad P \to Q}{Q}$ | SUB | $\dfrac{P(Q) \quad Q \leftrightarrow Q'}{P(Q')}$ |
| NXM | $\dfrac{P \to Q}{\bigcirc P \to \bigcirc Q}$ | PRM | $\dfrac{P \to P' \quad Q \to Q'}{(\Omega_1, P, \Omega_2)\ \mathsf{prj}\ Q \to (\Omega_1, P', \Omega_2)\ \mathsf{prj}\ Q'}$ |
| ALW | $\dfrac{P}{\Box P}$ | CPM | $\dfrac{P \to Q}{P^{+} \to Q^{+}}$ |
| REC | $\dfrac{P \to Q \vee \bigcirc P}{P \to \Diamond Q \vee \Box \bigcirc P}$ | | |

The rule MP is the classic rule of modus ponens for propositional logic. And in the rule SUB, $P(Q)$ denotes a formula $P$ with a sub-formula $Q$, and $P(Q')$ is the formula obtained from $P(Q)$ by substituting $Q$ with $Q'$. Intuitively, an inference rule means: if the hypothesis formulas are all valid, the conclusion formula is also valid. More explanations of these axioms and inference rules can be found in [8].

### 3.2 Axioms and Inference Rules for Indexed Expressions

We propose a proof (sub-)system $\Pi_I$ to reason about PPTL formulas with indexed expressions. The set of axioms of $\Pi_I$ are presented as follows. Here, $P$ denotes a formula without any index.

| | | | |
|---|---|---|---|
| IST | $\bigvee_{i\in\mathbb{N}} Q^i \leftrightarrow Q^*$ | | |
| INS | $R[i] \rightarrow \bigvee_{i\in\mathbb{N}} R[i]$ | INR | $\bigvee_{i\in\mathbb{N}} R[i] \leftrightarrow R[0] \vee \bigvee_{i\in\mathbb{N}} R[i+1]$ |
| INA | $\bigvee_{i\in\mathbb{N}} P \wedge R[i] \leftrightarrow P \wedge \bigvee_{i\in\mathbb{N}} R[i]$ | INO | $\bigvee_{i\in\mathbb{N}}(P \vee R[i]) \leftrightarrow P \vee \bigvee_{i\in\mathbb{N}} R[i]$ |
| INN | $\bigvee_{i\in\mathbb{N}} \bigcirc R[i] \leftrightarrow \bigcirc \bigvee_{i\in\mathbb{N}} R[i]$ | INC | $\bigvee_{i\in\mathbb{N}}(P \,;R[i]) \leftrightarrow P \,;\, \bigvee_{i\in\mathbb{N}} R[i]$ |

Among the axioms, IST indicates that an indexed expression $\bigvee_{i\in\mathbb{N}} Q^i$ can always be replaced by the star construct $Q^*$. In fact, both the formulas mean that $P$ holds repeatedly for zero or more times. Then, INS and INR reflect two standard property of the infinite disjunction operator $\bigvee_{i\in\mathbb{N}}$. In addition, INA, INO, INN and INC indicate that the and, or, next and chop operators are distributive over the infinite disjunction operator, respectively.

The set of inference rules of $\Pi_I$ are presented as follows.

$$\text{INM} \quad \frac{R[i] \rightarrow R'[i]}{\bigvee_{i\in\mathbb{N}} R[i] \rightarrow \bigvee_{i\in\mathbb{N}} R'[i]}$$

$$\text{REF} \quad \frac{R \leftrightarrow Q \vee P \wedge \bigcirc R \qquad R \rightarrow \Diamond Q}{\bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i Q \leftrightarrow R}$$

$$\text{REI} \quad \frac{R \leftrightarrow Q \vee P \wedge \bigcirc R \qquad \Box(P \wedge \bigcirc tt) \rightarrow R}{\bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i Q \vee \Box(P \wedge \bigcirc tt) \leftrightarrow R}$$

Among the inference rules, INM indicates that the infinite disjunction operator is monotonic. Besides, REF and REI are provided for solving $R$ from the recursive biconditional "equation" $R \leftrightarrow Q \vee P \wedge \bigcirc R$. The solution is in the form of an indexed expression, possibly in disjunction with a specific always formula. Intuitively, REF and REI are in accordance with the two cases of Lemma 2 that the recursion is made for finitely many times and for possibly infinitely many times, respectively.

The approach of theorem proving can be applied to verify properties of systems formally. First, both a system and a desired property are specified by PPTL formulas $S$ and $P$, respectively. Then, the system satisfies the property if and only if we can find a formal proof of $\vdash S \rightarrow P$ by the proof system $\Pi$.

## 4 Examples of Formal Proofs

To show the capability of the proof system $\Pi$, we provided a few examples of formal proofs. Notice that once $\vdash P$ is proved, $P$ is a theorem of the system and can be used in the formal proof of other formulas.

*Example 1.* $\vdash \mathsf{keep}(P) \leftrightarrow \varepsilon \vee P \wedge \bigcirc\mathsf{keep}(P)$. The theorem is denoted as T1, whose formal proof is given as follows. Recall that $\varepsilon = \neg \bigcirc tt$ and $\mathsf{keep}(P) = \Box(\bigcirc tt \to P)$.

| | | |
|---|---|---|
| (1) | $\mathsf{keep}(P) \leftrightarrow (\bigcirc tt \to P) \wedge (\varepsilon \vee \bigcirc\mathsf{keep}(P))$ | ALR |
| (2) | $(\bigcirc tt \to P) \wedge (\varepsilon \vee \bigcirc\mathsf{keep}(P)) \leftrightarrow \varepsilon \vee P \wedge \bigcirc\mathsf{keep}(P)$ | TAU |
| (3) | $\mathsf{keep}(P) \leftrightarrow \varepsilon \vee P \wedge \bigcirc\mathsf{keep}(P)$ | SUB (1) (2) |

*Example 2.* $\vdash \Diamond P \leftrightarrow P \vee \bigcirc\Diamond P$. The theorem is denoted as T2, whose formal proof is given as follows. Recall that $\Box P = \neg\Diamond\neg P$ for any formula $P$.

| | | |
|---|---|---|
| (1) | $\neg\Diamond\neg\neg P \leftrightarrow \neg P \wedge (\varepsilon \vee \bigcirc\neg\Diamond\neg\neg P)$ | ALR |
| (2) | $\neg\neg P \leftrightarrow P$ | TAU |
| (3) | $\neg\Diamond P \leftrightarrow \neg P \wedge (\varepsilon \vee \bigcirc\neg\Diamond P)$ | SUB (1) (2) |
| (4) | $(\neg\Diamond P \leftrightarrow \neg P \wedge (\varepsilon \vee \bigcirc\neg\Diamond P)) \to (\Diamond P \leftrightarrow P \vee \neg(\varepsilon \vee \bigcirc\neg\Diamond P))$ | TAU |
| (5) | $\Diamond P \leftrightarrow P \vee \neg(\varepsilon \vee \bigcirc\neg\Diamond P)$ | MP (3) (4) |
| (6) | $\bigcirc\neg\neg\Diamond P \leftrightarrow \neg(\varepsilon \vee \bigcirc\neg\Diamond P)$ | NXN |
| (7) | $\neg\neg\Diamond P \leftrightarrow \Diamond P$ | TAU |
| (8) | $\bigcirc\Diamond P \leftrightarrow \neg(\varepsilon \vee \bigcirc\neg\Diamond P)$ | SUB (6) (7) |
| (9) | $\Diamond P \leftrightarrow P \vee \bigcirc\Diamond P$ | SUB (5) (8) |

*Example 3.* $\vdash \bigvee_{i\in\mathbb{N}} \bigcirc^i Q \leftrightarrow \Diamond Q$. This theorem is denoted as T3, whose formal proof is given as follows.

| | | |
|---|---|---|
| (1) | $\Diamond Q \leftrightarrow Q \vee \bigcirc\Diamond Q$ | T2 |
| (2) | $\Diamond Q \to \Diamond Q$ | TAU |
| (3) | $\bigvee_{i\in\mathbb{N}} \bigcirc^i Q \leftrightarrow \Diamond Q$ | REF (1) (2) |

Intuitively, the indexed expression $\bigvee_{i\in\mathbb{N}} \bigcirc^i Q$ means $Q$ must hold at some state, which is equivalently characterized by the well-formed formula $\Diamond Q$.

*Example 4.* $\vdash \bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i Q \to \Diamond Q$. This theorem is denoted as T4, whose formal proof is given as follows.

| | | |
|---|---|---|
| (1) | $P^{(i)} \wedge \bigcirc^i Q \to \bigcirc^i Q$ | TAU |
| (2) | $\bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i Q \to \bigvee_{i\in\mathbb{N}} \bigcirc^i Q$ | INM |
| (3) | $\bigvee_{i\in\mathbb{N}} \bigcirc^i Q \leftrightarrow \Diamond Q$ | T3 |
| (4) | $\bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i Q \to \Diamond Q$ | SUB (2) (3) |

The intuition of T4 is that the indexed expression $\bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i Q$ implies $Q$ must hold at some state.

*Example 5.* $\vdash \bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i\varepsilon \vee \Box(P \wedge \bigcirc tt) \leftrightarrow \mathsf{keep}(P)$. This theorem is denoted as $\mathsf{T5}$, whose formal proof is given as follows. Recall that $\Diamond P = tt\ ;P = (tt, P)\ \mathsf{prj}\ \varepsilon$ for any formula $P$.

| | | |
|---|---|---|
| (1) | $\mathsf{keep}(P) \leftrightarrow \varepsilon \vee P \wedge \bigcirc\mathsf{keep}(P)$ | T1 |
| (2) | $\neg(\bigcirc tt \rightarrow P) \rightarrow \neg(P \wedge \bigcirc tt)$ | TAU |
| (3) | $\varepsilon \rightarrow \varepsilon$ | TAU |
| (4) | $\Diamond\neg(\bigcirc tt \rightarrow P) \rightarrow \Diamond\neg(P \wedge \bigcirc tt)$ | PRM (2) (3) |
| (5) | $(\Diamond\neg(\bigcirc tt \rightarrow P) \rightarrow \Diamond\neg(P \wedge \bigcirc tt)) \rightarrow (\Box(P \wedge \bigcirc tt) \rightarrow \mathsf{keep}(P))$ | TAU |
| (6) | $\Box(P \wedge \bigcirc tt) \rightarrow \mathsf{keep}(P)$ | MP (4) (5) |
| (7) | $\bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i\varepsilon \vee \Box(P \wedge \bigcirc tt) \leftrightarrow \mathsf{keep}(P)$ | REI (1) (6) |

Intuitively, the formula $\bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i\varepsilon \vee \Box(P \wedge \bigcirc tt)$ with an indexed expression means that the current interval is either finite or infinite and $P$ keeps holding at every non-final state, which is equivalently characterized by the well-formed formula $\mathsf{keep}(P)$.

*Example 6.* $\vdash P\,\mathsf{U}\,Q \leftrightarrow \mathsf{inf} \wedge \bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i Q$. This theorem is denoted as $\mathsf{T6}$, whose formal proof is given as follows. Recall that $P\,\mathsf{U}\,Q = \mathsf{inf} \wedge \bigvee_{i\in\mathbb{N}}(P \wedge \neg Q)^{(i)} \wedge \bigcirc^i Q$.

| | | |
|---|---|---|
| (1) | $\bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i Q \leftrightarrow Q \vee \bigvee_{i\in\mathbb{N}} P \wedge \bigcirc P^{(i)} \wedge \bigcirc\bigcirc^i Q$ | INR |
| (2) | $\bigvee_{i\in\mathbb{N}} P \wedge \bigcirc P^{(i)} \wedge \bigcirc\bigcirc^i Q \leftrightarrow P \wedge \bigvee_{i\in\mathbb{N}} \bigcirc P^{(i)} \wedge \bigcirc\bigcirc^i Q$ | INA |
| (3) | $\bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i Q \leftrightarrow Q \vee P \wedge \bigvee_{i\in\mathbb{N}} \bigcirc P^{(i)} \wedge \bigcirc\bigcirc^i Q$ | SUB (1) (2) |
| (4) | $\bigcirc(P^{(i)} \wedge \bigcirc^i Q) \leftrightarrow \bigcirc P^{(i)} \wedge \bigcirc\bigcirc^i Q$ | NXA |
| (5) | $\bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i Q \leftrightarrow Q \vee P \wedge \bigvee_{i\in\mathbb{N}} \bigcirc(P^{(i)} \wedge \bigcirc^i Q)$ | SUB (3) (4) |
| (6) | $\bigvee_{i\in\mathbb{N}} \bigcirc(P^{(i)} \wedge \bigcirc^i Q) \leftrightarrow \bigcirc\bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i Q$ | INN |
| (7) | $\bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i Q \leftrightarrow Q \vee P \wedge \bigcirc\bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i Q$ | SUB (5) (6) |
| (8) | $Q \vee P \wedge \bigcirc\bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i Q$<br>$\leftrightarrow Q \vee P \wedge \neg Q \wedge \bigcirc\bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i Q$ | TAU |
| (9) | $\bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i Q \leftrightarrow Q \vee P \wedge \neg Q \wedge \bigcirc\bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i Q$ | SUB (7) (8) |
| (10) | $\bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i Q \rightarrow \Diamond Q$ | T4 |
| (11) | $\bigvee_{i\in\mathbb{N}}(P \wedge \neg Q)^{(i)} \wedge \bigcirc^i Q \leftrightarrow \bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i Q$ | REF (9) (10) |
| (12) | $(\bigvee_{i\in\mathbb{N}}(P \wedge \neg Q)^{(i)} \wedge \bigcirc^i Q \leftrightarrow \bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i Q)$<br>$\rightarrow (P\,\mathsf{U}\,Q \leftrightarrow \mathsf{inf} \wedge \bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i Q)$ | TAU |
| (13) | $P\,\mathsf{U}\,Q \leftrightarrow \mathsf{inf} \wedge \bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i Q$ | MP (11) (12) |

$\mathsf{T6}$ indicates that the representation of $P\,\mathsf{U}\,Q$ can be simplified by replacing the indexed expression $\bigvee_{i\in\mathbb{N}}(P \wedge \neg Q)^{(i)} \wedge \bigcirc^i Q$ with a relatively concise one $\bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i Q$. Intuitively, the former indexed expression means that $P$ holds until $Q$ holds for the first time, and the latter indexed expression means that $P$ holds until sometimes $Q$ holds. These meanings are actually equivalent.

## 5 Soundness

An observation about the examples presented in the previous section is that many theorems of the proof system $\Pi$ coincide with the logic laws of PPTL.

For instance, $\bigvee_{i\in\mathbb{N}} \bigcirc^i Q \leftrightarrow \Diamond Q$ is a theorem (T3), and there is a logic law $\bigvee_{i\in\mathbb{N}} \bigcirc^i Q \equiv \Diamond Q$ which means the formula $\bigvee_{i\in\mathbb{N}} \bigcirc^i Q \leftrightarrow \Diamond Q$ is valid.

In fact, this is a universal phenomenon. We are going to show that the proof system $\Pi$ is sound, i.e., each theorem proved by $\Pi$ is valid.

For this, we first establish the soundness of axioms and inference rules of $\Pi$. On the one hand, each axiom is a valid formula. On the other hand, the conclusion formula of each inference rule is valid, provided all the hypothesis formulas are valid.

**Theorem 1 (Soundness of Axioms and Inference Rules).** *Each axiom or inference rule of $\Pi$ is sound, in that*

1. *$\models P$ if $P$ is an axiom of $\Pi$, and*
2. *$\models P$ if $\dfrac{P_1 \quad \cdots \quad P_n}{P}$ is an inference rule of $\Pi$ $(n \geq 1)$ and $\models P_i$ for each $1 \leq i \leq n$.*

The proof of Theorem 1 is presented in the Appendix of this paper.

As a natural deduction of Theorem 1, every formula proved by $\Pi$ is valid. That is, the proof system $\Pi$ is sound.

**Theorem 2 (Soundness of$\Pi$).** *For each PPTL formula $P$, $\vdash P$ implies $\models P$.*

*Proof.* $\vdash P$ means there is a formal proof $P_1, \ldots, P_n$ $(n \geq 1)$ with $P_n = P$. According to Theorem 1, $\models P_i$ for each $1 \leq i \leq n$. This involves $\models P$. □

## 6 Conclusions

In this paper, we develop a proof system $\Pi$ for PPTL with indexed expressions, which is a unified temporal logic that subsumes the well-used LTL. Specifically, $\Pi$ consists of axioms and inference rules for formal derivation of both basic PPTL constructs and indexed expressions. We provide a few examples to show how the proof system works. In addition, we demonstrate $\Pi$ is sound in that every formula proved by $\Pi$ is valid.

In the near future, we are going to prove the completeness of $\Pi$, i.e., every valid formula can also be proved formally by $\Pi$. This may be achieved by studying the normal form of indexed expressions and then making structural induction based on the normal form. We also plan to explore more meaningful styles of indexed expressions other than $\bigvee_{i\in\mathbb{N}} Q^i$ and $\bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i Q$, including their logic laws and relation with specific recursive equations. Which styles of indexed expressions have equivalent well-formed formulas is still an open question.

## Appendix

This appendix presents the proof of Theorem 1.

*Proof.* We only need to prove the soundness of axioms and inference rules in $\Pi_I$. The soundness of axioms and inference rules in $\Pi_B$ has been proved in [8].

(IST) For any interval $\sigma$, we have

$$\begin{aligned}
&\sigma \models \textstyle\bigvee_{i\in\mathbb{N}} Q^i\\
\Longleftrightarrow\ &\sigma \models Q^i \text{ for some } i \in \mathbb{N}\\
\Longleftrightarrow\ &\sigma \models \varepsilon \text{ or } \sigma \models Q^i \text{ for some } i \geq 1\\
\Longleftrightarrow\ &\sigma \models \varepsilon \text{ or } \sigma \models Q^+
\end{aligned}$$

which indicates $\sigma \models \bigvee_{i\in\mathbb{N}} Q^i \leftrightarrow Q^*$. Recall that $Q^* = \varepsilon \vee Q^+$.

(INS) For any interval $\sigma$, we have

$$\begin{aligned}
&\sigma \models R[i]\\
\Longrightarrow\ &\sigma \models R[i] \text{ for some } i \in \mathbb{N}\\
\Longleftrightarrow\ &\sigma \models \textstyle\bigvee_{i\in\mathbb{N}} R[i]
\end{aligned}$$

which indicates $\sigma \models R[i] \to \bigvee_{i\in\mathbb{N}} R[i]$.

(INR) For any interval $\sigma$, we have

$$\begin{aligned}
&\sigma \models \textstyle\bigvee_{i\in\mathbb{N}} R[i]\\
\Longleftrightarrow\ &\sigma \models R[i] \text{ for some } i \in \mathbb{N}\\
\Longleftrightarrow\ &\sigma \models R[0] \text{ or } \sigma \models R[i+1] \text{ for some } i \in \mathbb{N}\\
\Longleftrightarrow\ &\sigma \models R[0] \text{ or } \sigma \models \textstyle\bigvee_{i\in\mathbb{N}} R[i+1]
\end{aligned}$$

which indicates $\sigma \models \bigvee_{i\in\mathbb{N}} R[i] \leftrightarrow R[0] \vee \bigvee_{i\in\mathbb{N}} R[i+1]$.

(INA) For any interval $\sigma$, we have

$$\begin{aligned}
&\sigma \models \textstyle\bigvee_{i\in\mathbb{N}} P \wedge R[i]\\
\Longleftrightarrow\ &\sigma \models P \wedge R[i] \text{ for some } i \in \mathbb{N}\\
\Longleftrightarrow\ &\sigma \models P \text{ and } \sigma \models R[i] \text{ for some} i \in \mathbb{N}\\
\Longleftrightarrow\ &\sigma \models P \text{ and } \sigma \models \textstyle\bigvee_{i\in\mathbb{N}} R[i]
\end{aligned}$$

which indicates $\sigma \models \bigvee_{i\in\mathbb{N}} P \wedge R[i] \leftrightarrow P \wedge \bigvee_{i\in\mathbb{N}} R[i]$. The proofs of (INO), (INN) and (INC) are similar.

(INM) Suppose $\models R[i] \to R'[i]$. Then, for any interval $\sigma$, $\sigma \models R[i]$ implies $\sigma \models R'[i]$. So, for any interval $\sigma$, $\sigma \models R[i]$ for some $i \in \mathbb{N}$ implies $\sigma \models R'[i]$ for some $i \in \mathbb{N}$, which means $\sigma \models \bigvee_{i\in\mathbb{N}} R[i]$ implies $\sigma \models \bigvee_{i\in\mathbb{N}} R'[i]$, or equivalently $\sigma \models \bigvee_{i\in\mathbb{N}} R[i] \to \bigvee_{i\in\mathbb{N}} R'[i]$.

(REF) Suppose $\models R \leftrightarrow Q \vee P \wedge \bigcirc R$ and $\models R \to \Diamond Q$. Then, $R \equiv Q \vee P \wedge \bigcirc R$ and $R \subset \Diamond Q$. According to Lemma 2, $\bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i Q \equiv R$, which means $\models \bigvee_{i\in\mathbb{N}} P^{(i)} \wedge \bigcirc^i Q \leftrightarrow R$. The proof of (REI) is similar. □

## References

1. Bowman, H., Thompson, S.J.: A decision procedure and complete axiomatization of finite interval temporal logic with projection. J. Logic Comput. **13**(2), 195–239 (2003)
2. Clarke, E.M., Grumberg, O., Peled, D.A.: Model Checking. The MIT Press, Cambridge (2000)
3. Duan, Z.: Temporal Logic and Temporal Logic Programming. Science Press, Beijing (2006)
4. Duan, Z., Tian, C.: A unified model checking approach with projection temporal logic. In: Liu, S., Maibaum, T., Araki, K. (eds.) ICFEM 2008. LNCS, vol. 5256, pp. 167–186. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-88194-0_12
5. Duan, Z., Tian, C.: A practical decision procedure for propositional projection temporal logic with infinite models. Theoret. Comput. Sci. **554**, 169–190 (2014)
6. Duan, Z., Tian, C., Zhang, N., Ma, Q., Du, H.: Index set expressions can represent temporal logic formulas. Theoret. Comput. Sci. (2018). https://doi.org/10.1016/j.tcs.2018.11.030
7. Duan, Z., Yang, X., Koutny, M.: Framed temporal logic programming. Sci. Comput. Program. **70**(1), 31–61 (2008)
8. Duan, Z., Zhang, N., Koutny, M.: A complete proof system for propositional projection temporal logic. Theoret. Comput. Sci. **497**, 84–107 (2013)
9. French, T., Reynolds, M.: A sound and complete proof system for QPTL. In: Advances in Modal logic 2002, pp. 127–148 (2002)
10. Kanso, K., Setzer, A.: A light-weight integration of automated and interactive theorem proving. Math. Struct. Comput. Sci. **26**(01), 129–153 (2016)
11. Kesten, Y., Pnueli, A.: Complete proof system for QPTL. J. Logic Comput. **12**(5), 701–745 (2002)
12. Manna, Z., Pnueli, A.: Completing the temporal picture. Theoret. Comput. Sci. **83**(1), 91–130 (1991)
13. Moszkowski, B.C.: Executing Temporal Logic Programs. Cambridge University, Cambridge (1986)
14. Moszkowski, B.C.: A complete axiom system for propositional interval temporal logic with infinite time. Log. Methods Comput. Sci. **8**(3) (2012)
15. Pnueli, A.: The temporal logic of programs. In: Proceedings of the 18th Annual IEEE Symposium on Foundations of Computer Science, pp. 46–57. IEEE Computer Society (1977)
16. Rosner, R., Pnueli, A.: A choppy logic. In: LICS 1986, pp. 306–313 (1986)
17. Shu, X., Duan, Z.: A decision procedure and complete axiomatization for projection temporal logic. Theor. Comput. Sci. (2017). https://doi.org/10.1016/j.tcs.2017.09.026
18. Tian, C., Duan, Z.: Expressiveness of propositional projection temporal logic with star. Theoret. Comput. Sci. **412**, 1729–1744 (2011)
19. Winskel, G.: The Formal Semantics of Programming Languages: An Introduction. The MIT Press, Cambridge (1993)
20. Zhang, N., Duan, Z., Tian, C.: Model checking concurrent systems with MSVL. Sci. China: Inf. Sci. **59**(11), 101–118 (2016)