ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.19, No.12, December 2008, pp.3122−3133
DOI: 10.3724/SP.J.1001.2008.03122

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

直觉线性μ-演算*

KAZMI Syed Asad Raza[1,2,3], 张文辉[1+]

[1](中国科学院 软件研究所 计算机科学重点实验室,北京 100190)

[2](中国科学院 研究生院 信息与工程学院,北京 100049)

[3](Department of Computer Science, Government College University, Lahore, Pakistan)

Intuitionistic Linear-Time μ-Calculus

KAZMI Syed Asad Raza[1,2,3], ZHANG Wen-Hui[1+]

[1](Laboratory of Computer Science, Institute of Software, The Chinese Academy of Sciences, Beijing 100190, China)

[2](School of Information Science and Engineering, Graduate University, The Chinese Academy of Sciences, Beijing 100049, China)

[3](Department of Computer Science, Government College University, Lahore, Pakistan)

+ Corresponding author: E-mail: zwh@ios.ac.cn

Kazmi SAR, Zhang W. Intuitionistic linear-time μ-calculus. ***Journal of Software*****, 2008,19(12):3122−3133.** http://www.jos.org.cn/1000-9825/19/3122.htm

Abstract: Linear time mu-calculus (μTL) is an extension of linear-time temporal logic (LTL) by fixed points, which is a convenient way to specify and reasoning about reactive systems. As μTL being more expressible than LTL, the properties specified by LTL could be determined by μTL. Similar to the intuitionistic linear-time temporal logic (ILTL), we propose an intuitionistic variant of μTL as intuitionistic linear time mu-calculus (IμTL). We have established a correspondence between IμTL and ILTL, and compared their expressive power. Using IμTL to specify safety and liveness properties, and assumption-guarantee specifications are also discussed.

Key words: propositional linear temporal logic; intuitionistic linear time μ-calculus

摘 要: 线性 mu-演算(μTL)是线性时序逻辑(LTL)的不动点扩展.LTL 是一个便于规范和论证反应式系统的方法.μTL 作为比 LTL 表达能力更强的逻辑,用 LTL 表示的性质度可由μTL 表示.类似于 LTL 的直觉线性时序逻辑(ILTL),提出一种基于直觉解释的μTL,称为直觉μTL(IμTL).确立了 IμTL 和 ILTL 的关系,比较了它们之间的表达能力.讨论了使用 IμTL 与安全性质和活性描述的关系以及描述“假设-保证”规范的问题.

关键词: 命题线性时序逻辑;直觉线性μ-演算

中图法分类号: TP301 **文献标识码**: A

* Supported by the National Natural Science Foundation of China under Grant Nos.60421001, 60573012 (国家自然科学基金); the National Basic Research Program of China under Grant No.2002cb312200 (国家重点基础研究发展计划(973))

Received 2007-08-16; Accepted 2007-12-06

1 Introduction

Temporal logics is a convenient language for the specification of reactive systems[1]. The underlying model of such behaviors possesses infinite nature i.e. a non-terminating sequence of interaction between system and its environment. Sometimes we need to bifurcate the finite and infinite behaviors simultaneously in order to distinguish them. For example safety and liveness properties are two important features of reactive systems, and these properties differ fundamentally in the way they constrain finite and infinite behaviors[2]. We usually observe real systems in finite domain and idealize them in an infinite domain in order to determine whether the observations violate the specifications or not. Various suggestions have been proposed to extend the LTL to finite behavior. In Ref.[3] semantic interpretations of LTL formulas given by weak and strong semantics that differ on finite behaviors. In contrast to above segregation the semantical interpretation of LTL that treats finite and infinite behaviors uniformly is expounded in Ref.[2]. The proposed solution in Ref.[2] is based on prefix-closed sets of finite and infinite behaviors by providing an intuitionistic linear-time temporal logic (ILTL), the intuitionistic variant of LTL. Wolper in Ref.[4] illustrated that some properties are not expressible in LTL, while fixed point treatment discussed in Ref.[5] with an idea that expressive power beyond LTL is necessary. The linear time μ-calculus (μTL) is an extension of standard linear time temporal logic (LTL) by fixed point operators[6] with increased expressibility, and the μTL is more elegant than Wolper's extended temporal logic ETL[4,7] as requiring only single *nexttime* temporal operator, while ETL requires infinite family of operators[8].

The fixed point intervention by extending TL with maximal and minimal fixed point quantifiers, originally advocated by Emerson and Clarke and then by Baringger *et al*.[6], as was done for dynamic logic in Ref.[9] yielding μ-calculus. The propositional μ-calculus is a powerful language for expressing properties of transition systems by using least and greatest fixed points operators[10]. From a theoretical perspective, the status of μ-calculus as the canonical temporal logic for regular requirements is due to the fact that its expressiveness exceeds that of all commonly used temporal logics such as LTL, CTL, and CTL*[11], while equals that of alternating parity tree automata or the bisimulator-closed fragment of monadic second-order theory over trees[12,13]. On the other hand, from a practical standpoint, iterative computation of fixpoints naturally suggests symbolic evaluation, and symbolic model checker such as SMV checks CTL properties of finite-state models by compiling them into μ-calculus formulas[14,15]. As mentioned earlier the temporal logic LTL is built around *nexttime*(X) and *until*(U) operators.

Motivation: The intuitionistic nature of ILTL comes in handy when doing assume-guarantee reasoning, because special temporal operator that have been introduced to reason about assume-guarantee specifications are definable through the intuitionistic implication[2], while our intuitive motivation is the more expressiveness of μTL than the LTL[11]. We propose a variant of μ-calculus in intuitionistic domain as intuitionistic linear-time μ-calculus (IμTL). To express the concurrent system properties like safety and liveness characterized through IμTL in order to chalk out these properties in the underlying Heyting algebra, and to specify that a few properties couldn't be specified in previously presented intuitionistic logic ILTL. Thus, we express properties in a new characterization for properties presentation and their segregation through simultaneous behaviors of finite and infinite nature. In our treatment we provide semantics interpretation of linear-time μ-calculus (μTL) in intuitionistic domain. The proposed intuitionistic linear-time μ-calculus as a variant of μTL encompasses ILTL. We establish a correspondence between ILTL and that of IμTL in order to maintain deducibility of ILTL from I IμTL. We also demonstrate the assumption-guarantee specifications specified in IμTL.

Plan: In Section 2, some preliminaries for notations and definitions are given. Section 3 constitutes of the definition of linear-time μ-calculus, and the semantic definitions in classical and intuitionistic logics. The expressive powers of μ TL and IμTL in Boolean and Heyting algebras and the correspondence between IμTL and

that of ILTL are the contents of Section 4. Section 5 consists of definitions of safety and liveness properties in the classical and intuitionistic domains, and an example of safety property in the proposed IμTL is treated, while Section 6 deals with discussion over assumption-guarantee specifications with respect to IμTL. The conclusion regarding intuitionistic linear-time μ-calculus is outlined in the last Section 7.

2 Preliminaries

During the course of development of the problem and its synthesis we will use various notations and definitions, the most of them are defined in this section. The non-empty set of the atomic propositions is taken as $AP=\{p,q,r,...\}$ with its power set as 2^{AP}, $\Sigma=\{a,b,c,...\}$ a set of alphabets, and Σ^{∞} is a set of all non-empty words over Σ. The set Σ^{∞} is further bifurcated into Σ^{*} and Σ^{ω} as the sets of finite length and infinite length words respectively. We have Σ_r as a set of all sets containing r i.e. $\Sigma_r=\{\xi\in 2^{AP}\mid r\in\xi\}$. A behavior is taken as a word in Σ^{∞}. The power set of Σ^{∞} is designated as $P(\Sigma^{\infty})$, and this constitutes a power set lattice $\mathbf{P}(\Sigma^{\infty})=\langle P(\Sigma^{\infty}),\cap,\cup\rangle$ with order $\subseteq$. We designate the elements of this power set lattice $\mathbf{P}(\Sigma^{\infty})$ as languages or properties. We have a closure operator C_l for the mapping of the power set $P(\Sigma^{\infty})$ to itself as $C_l: P(\Sigma^{\infty})\to P(\Sigma^{\infty})$, which is characterized by the properties of inflationary, idempotent, and monotonicity, i.e. for all L_1,L_2 and $L\in\Sigma^{\infty}$, then $L\subseteq C_l(L)$, $C_l(C_l(L))=C_l(L)$ and if $L_1\subseteq L_2$ implies $C_l(L_1)\subseteq C_l(L_2)$ respectively. In addition to above properties the closure operator C_l on Σ^{∞} is distributive over finite joins i.e. $C_l(\varnothing)=\varnothing$ and for all $L_1,L_2\subseteq\Sigma^{\infty}$, $C_l(L_1\cup L_2)=C_l(L_1)\cup C_l(L_2)$, then the closure operator C_l will be a topological closure operator on Σ^{∞}.

In order to chalk out an infinite behavior in some language $L\in\Sigma^{\infty}$ we have a function $f_B: P(\Sigma^{\infty})\to P(\Sigma^{\infty})$ which maps the language L such as $f_B(L)=L\cap\Sigma^{\omega}$ that is a set of infinite behaviors in L. Since mapping f_B preserves infinite joins and meets, and hence it is an endomorphism over the complete lattice $\mathbf{P}(\Sigma^{\infty})$. The range of the function f_B is denoted as R_B, and is defined as $R_B=\{f_B(L)\mid L\subseteq\Sigma^{\infty}\}=P(\Sigma^{\omega})$. Being an endomorphism R_B induces a sublattice of $P(\Sigma^{\infty})$, and which kept the behavior of complete lattice sets. The induced sublattice is given as $\Lambda_B=\langle R_B,\cup,\cap,\Sigma^{\omega},-,\varnothing\rangle$, which is in fact a complete Boolean algebra, where $-$ denotes the complement of the language L such that $-L=\{\omega\in\Sigma^{\omega}\mid\omega\notin L\}$.

We represent $\prec$ as prefix order on Σ^{∞}, for ω, $u\in\Sigma^{\infty}$, if u is a prefix of ω then $u\prec\omega$, while $f_H(\omega)=\{u\in\Sigma^{\infty}\mid u\prec\omega\}$. The mapping $f_H:\Sigma^{\infty}\to P(\Sigma^{\infty})$, maps a behavior Σ^{∞} to language $(P(\Sigma^{\infty}))$, while we could extend the domain of f_H, and define $f_H: P(\Sigma^{\infty})\to P(\Sigma^{\infty})$ which extends the behavior to language. By $f_H(L)$ we mean that $f_H(L)=\bigcup_{\omega\in L} f_H(\omega)$. We say that language L is prefix closed iff $L=f_H(L)$, the set of prefix closed languages. Despite of not preserving all meets R_H induces a complete sublattice of $P(\Sigma^{\infty})$, which turns out to be a complete lattice of sets. Then $\Lambda_H=\langle R_H,\cup,\cap,\Rightarrow,\Sigma^{\infty},\varnothing\rangle$ constitutes a complete Heyting algebra, i.e. for all languages $L_1,L_2\in R_H$ we have a language $L\in R_H$ known to be greatest language as $L=\{\omega\in\Sigma^{\infty}\mid f_H(\omega)\cap L_1\subseteq L_2\}$ such that $L_1\cap L\subseteq L_2$. The language L is a relative pseudo-complement of L_1 and L_2 and is denoted as $L_1\Rightarrow L_2$.

3 Linear-Time μ-Calculus

The language of μ-calculus is formulated from propositions, standard Boolean connectives, least fixed point μ, greatest fixed point ν, and the temporal operator nexttime $\odot$. The set of formulas Ω_μ of the linear time μ-calculus (μTL) is defined by the following convention:

$$\Omega_\mu ::= p\mid\bot\mid\mathrm{T}\mid\psi\wedge\varphi\mid\psi\vee\varphi\mid\odot\psi\mid\mu Z.\psi\mid\nu Z.\psi\mid\psi\to\varphi$$

We have formulas $\varphi,\psi\in\Omega_\mu$, p ranges over atomic propositions, $V=\{X,Y,Z,\ldots\}$ be the set of variables, $\mu Z.\psi$ is the least fixed point for ψ and its corresponding counterpart for greatest fixed point is $\nu Z.\psi$ whereas the variable

Z in $\mu Z.\psi$ and $\nu Z.\psi$ is in the scope of even number of negations. In linear-time μ-calculus we have bounded and free variables and the formulas with free variables are interpreted with respect to an environment $\rho: V \to P(\Sigma^{\infty})$, which maps all free variables to $\varsigma \subseteq \Sigma^{\omega}$.

Closed Formulas: Variables in the μ-calculus can be either free or bounded by a fixed point operator, a formula is said to be closed if the formula doesn't contain free variables.

Positive and Guarded Formulas: A formula is positive if and only if all negations in the formula appear only before propositions. A μTL formula φ is in guarded form iff every occurrence of the bounded variable $Z \in \varphi^{s}$ is in the scope of some modality operator, where φ^{s} is a subformula of φ. Every formula is equivalent to some positive guarded formula[16].

Proposition 1. If $f_m : P(\Sigma^{\omega}) \to P(\Sigma^{\omega})$ is monotonic with respect to $\subseteq$ then f_m:

1. has a least fixed point given as the set $\bigcap\{L_{\mu} \subseteq \Sigma^{\omega} \mid f_m(L_{\mu}) \subseteq L_{\mu}\}$
2. has a greatest fixed point given as the set $\bigcup\{L_{\nu} \subseteq \Sigma^{\omega} \mid f_m(L_{\nu}) \supseteq L_{\nu}\}$

Proof: We shall prove 1 and leaving 2 by dual reasoning. Let $f_{fp} = \bigcap\{L_{\mu} \subseteq \Sigma^{\omega} \mid f_m(L_{\mu}) \subseteq L_{\mu}\}$, in order to establish L_{fp} is a fixed point i.e. $f_m(L_{fp})=L_{fp}$ we suppose $L \in f_m(L_{fp})$. By definition we have $L \in f_m(L_{\mu})$ for every $L_{\mu} \subseteq \Sigma^{\omega}$ such that $f_m(L_{\mu}) \subseteq L_{\mu}$. Consequently, $L \in L_{\mu}$ for every such language L_{μ}, so L belongs to their intersection too. This means $f_m(L_{fp}) = L_{fp}$.

Next assume $L \in f_{fp}$ but $\mathrm{L} \in f_m(L_{fp})$, and let $L_1 = L_{fp} - \{\mathrm{L}\}$. By monotonicity of f_m we have $f_m(L_1) \subseteq f_m(L_{fp})$ but we have just shown $f_m(L_{fp}) \subseteq f_{fp}$, and since $\mathrm{L} \notin f_m(L_{fp})$. It follows that $f_m(L_{fp}) = L_1$. Therefore, $f_m(L_1) \subseteq L_1$ which means that $L_{fp} \subseteq L_1$ by the definition of L_{fp} which is a *contradiction*. We have shown that L_{fp} is a fixed point of f_m.

Consider any other fixed point $\widetilde{L_{fp}}$. Because $f_m(\widetilde{L_{fp}}) = \widetilde{L_{fp}}$, it follows that $f_m(\widetilde{L_{fp}}) \subseteq \widetilde{L_{fp}}$, and by definition of L_{fp} we know that $\widetilde{L_{fp}} \subseteq \widetilde{L_{fp}}$ which means L_{fp} is the least fixed point.

Proposition 1 guarantees the existence of extreme solutions, which are least and greasiest fixed points of the monotonic function.

3.1 Semantics of LTL in classical interpretation

The semantics of the linear-time μ-calculus (μTL) formulas are inductively defined over infinite words in Σ^{∞} i.e. words belonging to Σ^{ω}. As free variables get bounded under environment ρ, therefore, the semantical interpretation is formulated under that environment.

In order to give the classical semantic interpretation of the linear-time μ-calculus we have the monotonic function $next_c$ defined as $next_c(L) = \Sigma L$. Let $\lambda Z.\psi$ be an explicit representation for variable dependency of the formula ψ in which the variable is Z in this case. Let *Ord* be the set of ordinals.

The semantics of μTL formulas under that the environment ρ is given, and is defined over Boolean algebra Λ_B by interpreting through classical interpretation function I_c^{ρ} given as $I_c^{\rho} : \Omega_{\mu} \to \Lambda_B$:

$$I_c^\rho(T)=\Sigma^\omega$$
$$I_c^\rho(\bot)=\varnothing$$
$$I_c^\rho(\psi\wedge\varphi)=I_c^\rho(\psi)\cap I_c^\rho(\varphi)$$
$$I_c^\rho(\psi\vee\varphi)=I_c^\rho(\psi)\cup I_c^\rho(\varphi)$$
$$I_c^\rho(\psi\to\varphi)=I_c^\rho(-\psi\vee\varphi)$$
$$I_c^\rho(\neg\psi)=-I_c^\rho(\psi)$$
$$I_c^\rho(r)=\Sigma_r\Sigma^\omega=\{\omega\in\Sigma^\omega\mid\exists q\in\Sigma_r,\exists u\in\Sigma^\omega:\omega=qu\}$$
$$I_c^\rho(\odot\psi)=next_c(I_c^\rho(\psi))$$
$$I_c^\rho(Z)=\rho(Z)$$
$$I_c^\rho(\mu Z.\psi)=\bigcup_{n\in Ord}[munext_c^\rho(\lambda Z.\psi)]^n(\varnothing)$$
$$I_c^\rho(\nu Z.\psi)=\bigcap_{n\in Ord}[munext_c^\rho(\lambda Z.\psi)]^n(\Sigma^\omega)$$

with $munext_c^\rho$ defined as $munext_c^\rho(\lambda Z.\psi)(L)=I_c^{\rho\left[\frac{L}{Z}\right]}(\psi)$, and for a limit ordinal n,

$[munext_c^\rho(\lambda Z.\psi)]^n(\varnothing)=\bigcup_{m<n}[munext_c^\rho(\lambda Z.\psi)]^n(\varnothing)$ and $[munext_c^\rho(\lambda Z.\psi)]^n(\Sigma^\omega)=\bigcap_{m<n}[munext_c^\rho(\lambda Z.\psi)]^n(\Sigma^\omega)$.

The interpretation function I_c^ρ interprets the modalities over the environment $\rho:V\to P(\Sigma^\omega)$ in which it is implemented. For a closed μTL formula, this interpretation corresponds to the classical meanings that the formula represents the set of ω-words satisfying the formula.

3.2 Intuitionistic interpretation of semantics of LTL

As μTL is semantically expressed in the above section on the same analogy we express the linear-time μ-calculus in linear intuitionistic logic, and it is designated intuitionistic linear-time μ-calculus (IμTL). The IμTL is defined over Heyting algebra Λ_H. In this domain we have the interpretation function I_c^ρ with mapping as $I_i^\rho:\Omega_\mu\to\Lambda_H$, and following corresponding interpretations:

$$I_i^\rho(T)=\Sigma^\infty$$
$$I_i^\rho(\bot)=\varnothing$$
$$I_i^\rho(\psi\wedge\varphi)=I_i^\rho(\psi)\cap I_i^\rho(\varphi)$$
$$I_i^\rho(\psi\vee\varphi)=I_i^\rho(\psi)\cup I_i^\rho(\varphi)$$
$$I_i^\rho(\psi\to\varphi)=I_i^\rho(\psi)\Rightarrow I_i^\rho(\varphi)$$
$$I_i^\rho(\neg\psi)=I_i^\rho(\psi\to\bot)$$
$$I_i^\rho(r)=\Sigma_r\Sigma^\infty=\{\omega\in\Sigma^\infty\mid\exists q\in\Sigma_r,\exists u\in\Sigma^\infty:\omega=qu\}$$
$$I_i^\rho(\odot\psi)=next_i(I_i^\rho(\psi))$$
$$I_i^\rho(Z)=\rho(Z)$$
$$I_i^\rho(\mu Z.\psi)=\bigcup_{n\in Ord}[munext_i^\rho(\lambda Z.\psi)]^n(\varnothing)$$
$$I_i^\rho(\nu Z.\psi)=\bigcap_{n\in Ord}[munext_i^\rho(\lambda Z.\psi)]^n(\Sigma^\infty)$$

Intuitionistic Monotonic Functions: In establishment of intuitionistic variant of μTL for the formulation of intuitionistic linear-time μ-calculus (IμTL) we have corresponding functions $next_i$ and $munext_i^\rho$, and are given below:

Intuitionistic Monotonic $next_i$ Function: For $\sum$ be a set of alphabets, and $next_i$ be a monotonic function, then it generates language inductively as $next_i(L)=\Sigma\cup\Sigma L$ for $L\in R_H$. In defining the language or properties we have Σ^* and Σ^ω as the sets of finite and infinite length words respectively and their superset Σ^∞. Therefore, the properties

we are taking into consideration are only for non-empty words and so the monotonic function $next_i$ is over a non-empty language.

Intuitionistic Monotonic $munext_i^\rho$ Function: In this case we have language $L \in R_H$, and the environment $\rho : V \to P(\Sigma^\infty)$, the monotonic function $munext_i^\rho$ is defined as:

$$munext_i^\rho(\lambda Z.\psi)(L) = I_i^{\rho\left[\frac{L}{Z}\right]}(\psi)$$

Besides the difference in the semantic domains, the classical and intuitionistic semantics interpretation functions differ in interpreting negation, implication, and next operator. These differentiations mainly depend upon the interpretation of μTL over Heyting algebra while μTL is defined over Boolean algebra. Furthermore, the condition for positive occurrences of fixed point variables also remained in the formulas in IμTL.

4 Expressive Power

The sets of behaviors in different logics are compared in order to expedite the comparative expressive power of μTL and that of IμTL. The formulas in the μTL are interpreted over Boolean algebra Λ_B, while the formulas of IμTL are interpreted over Λ_H, the Heyting algebra. Therefore, we cannot compare them directly; rather their corresponding carriers may be compared. As $f_B : P(\Sigma^\infty) \to R_B$ and $f_H : P(\Sigma^\infty) \to R_H$, so first we will compare the semantics in Boolean algebra Λ_B by restricting the intuitionistic semantics to infinite words through f_B, and then by extending the classical semantics into prefixed closed set through f_H for comparison in Heyting algebra Λ_H.

4.1 Expressive power in Boolean algebra Λ_B

In order to compare μTL and IμTL in Boolean algebra we would restrict the intuitionistic semantics to infinite word through f_B. Below is a proposition which relates the formulas in negation normal form for semantics in Boolean and Heyting algebras. Before presenting and proving the proposition, we have a definition and representative interpretation of the symbols.

Suppose φ be a closed formula, then both the interpretation functions $I_c^\rho(\varphi)$ and $I_i^\rho(\varphi)$ in classical domain and in the intuitionistic domain respectively do not depend on ρ. Then we write $I_c(\varphi)$ and $I_i(\varphi)$ for semantics of the closed formulas. Furthermore, a formula is in a negation normal form (NNF) if it does not contain implication nor equivalence, and negation is applied only to atomic propositions.

Proposition 2. If ψ is a closed formula in NNF then $I_c(\psi) = f_B(I_i(\psi))$.

Proof: For the first, since $f_B(L) = L \cap \Sigma^\omega$ preserves arbitrary joins and meets, we have $f_B(\bigcup_i L_i) = \bigcup_i (f_B(L_i))$ and $f_B(\bigcap_i L_i) = \bigcap_i (f_B(L_i))$. For the second, we define $f_B(\rho)$ by $f_B(\rho)(Z) = f_B(\rho(Z))$ (an overloading of the symbol f_B for related meaning). Then an environment ρ in the intuitionistic domain corresponds to an environment $f_B(\rho)$in classical domain. We prove a more general statement $I_c^{f_B(\rho)}(\psi) = f_B(I_i^\rho(\psi))$ by induction on ψ.

- The base cases are obvious i.e. for the constant $\bot$ and $\top$, atomic propositions and negated atomic proposition.
- Conjunction and disjunction are straightforward since f_B distributes over intersection and union.
- For all $L \in R_H$

$next_c(f_B(L)) = \Sigma f_B(L) = f_B(\Sigma \cup \Sigma L) = f_B(next_i(L))$

Therefore, for the next operator $\odot$ we have

$$\begin{aligned} I_c^{\rho}(\odot\psi) &= next_c((I_c^{\rho}(\psi))) \\ &= next_c(f_B(I_i^{\rho}(\psi))) \\ &= f_B(next_i(I_i^{\rho}(\psi))) \\ &= f_B(I_i^{\rho}(\odot(\psi))) \end{aligned}$$

- For all $L \in R_B$ we have

$$munext_c^{f_B(\rho)}(\lambda Z.\psi)(f_B(L)) = I_c^{f_B\rho\left[f_B(L)/Z\right]}(\psi) = I_c^{f_B\left(\rho\left[\frac{L}{Z}\right]\right)}(\psi)$$

$$munext_i^{\rho}(\lambda Z.\psi)(L) = I_i^{\rho\left[\frac{L}{Z}\right]}(\psi)$$

Since $I_c^{f_B\left(\rho\left[\frac{L}{Z}\right]\right)}(\psi) = f_B(I_i^{\rho\left[\frac{L}{Z}\right]}(\psi))$ according to the induction hypothesis, we have

$$munext_c^{f_B(\rho)}(\lambda Z.\psi)(f_B(L)) = f_B(munext_i^{\rho}(\lambda Z.\psi)(L))$$

and the generalization $[munext_c^{f_B(\rho)}(\lambda Z.\psi)]^n(f_B(L)) = f_B([munext_i^{\rho}(\lambda Z.\psi)]^n(L))$ by transfinite induction. Therefore

$$\begin{aligned} I_c^{f_B(\rho)}(\mu Z.\psi) &= \bigcup_{n\in Ord}[munext_i^{f_B(\rho)}(\lambda Z.\psi)]^n(\varnothing) \\ &= \bigcup_{n\in Ord} f_B([munext_i^{\rho}(\lambda Z.\psi)]^n(\varnothing)) \\ &= f_B(\bigcup_{n\in Ord}[munext_i^{\rho}(\lambda Z.\psi)]^n(\varnothing)) \\ &= f_B(I_c^{\rho}(\mu Z.\psi)) \end{aligned}$$

$$\begin{aligned} I_c^{f_B(\rho)}(\nu Z.\psi) &= \bigcap_{n\in Ord}[munext_i^{f_B(\rho)}(\lambda Z.\psi)]^n(\Sigma^{\omega}) \\ &= \bigcap_{n\in Ord} f_B([munext_i^{\rho}(\lambda Z.\psi)]^n(\Sigma^{\infty})) \\ &= f_B(\bigcap_{n\in Ord}[munext_i^{\rho}(\lambda Z.\psi)]^n(\Sigma^{\infty})) \\ &= f_B(I_i^{\rho}(\nu Z.\psi)) \end{aligned}$$

The Proposition 2 reflects that the IμTL is as least expressive as μTL, since every formula in the classical interpretation corresponds to formula in NNF, and the deducibility of formula in prefixed closed set is completely expressible in the μTL domain of infinite behavior.

4.2 Correspondence between ILTL and ILTL

The interpretational algebra of both ILTL and IμTL logics is Heyting algebra Λ_H and their relative correspondence could be established through their modalities e.g. we have $\varphi U\psi$ which is interpreted in ILTL through $Mod_i(\varphi U\psi)$, while this modality could be expressed in fixed points of IμTL. The intuitionistic interpretation function Mod_i for modality $\varphi U\psi$ is given in Ref.[2]:

$$Mod_i(\varphi U\psi) = \bigcup_{n<\omega} until next[Mod_i(\varphi), Mod_i(\psi)]_i^n(\varnothing)$$

and the monotonic function $until next[L_1, L_2]_i$ (with parameters $L_1, L_2 \in R_H$) is defined as:

$$until next[l_1, L_2]_i(L) = L_2 \cup (L_1 \cap next_i(L)) .$$

Let φ be an LTL formula, and we define $g(\varphi)$as follows:

$$\begin{aligned} &g(p) = p \\ &g(-p) = -p \\ &g(\varphi \wedge \psi) = g(\varphi) \wedge g(\psi) \\ &g(\varphi \vee \psi) = g(\varphi) \vee g(\psi) \\ &g(X\psi) = \odot g(\psi) \\ &g(\varphi U\psi) = \mu Z.(g(\psi) \vee (g(\varphi) \wedge \odot Z)) \end{aligned}$$

Proposition 3. Let φ be an LTL formula, then $Mod_i(\varphi) = I_i^{\rho}(g(\varphi))$ for any ρ.

Proof: This proposition can be proved by induction on φ. We only discuss the case of $\varphi U\psi$, the other cases are trivial. For the first, we obtain that $munext_i^{\rho}[\lambda Z.(g(\psi)\vee(g(\varphi)\wedge\odot Z))](L)=I_i^{\rho}(g(\psi))\cup(I_i^{\rho}(g(\varphi))\cap next_i(L))$.

$$untilnext[Mod_i(\varphi),\ Mod_i(\psi)]_i(L)=Mod_i(\psi)\cup(Mod_i(\varphi)\cap next_i(L)).$$

Therefore

$$untilnext[Mod_i(\varphi),Mod_i(\psi)]_i(L)=munext_i^{\rho}[\lambda Z.(g(\psi)\vee(g(\varphi)\wedge\odot Z))](L).$$

Since $g(\psi)$ and $g(\varphi)$ are closed formulas, by induction on the number of applications of *untilnext* we obtain $Mod_i(\varphi U\psi)=I_i^{\rho}(g(\varphi U\psi))$.

The relative correspondence between ILTL and IμTL indicates that the ILTL is deducible from IμTL, and the correlation between the interpretation functions in these logics is well-established.

4.3 Expressive power in heyting algebra Λ_H

In order to compare expressiveness of the logics μTL and IμTL in the domain of Heyting algebra Λ_H of prefixed closed sets of behaviors we have to extend the semantics into prefix-closed sets through f_H. The proposition below relates these domains.

Proposition 4. There is no closed μTL formula ψ with $f_H(I_c(\psi))=\Sigma=I_i(\odot\perp)$.

Proof: Let $\psi\in\Omega_{\mu}$, and $I_c(\psi)=\varnothing$ then $f_H(I_i(\psi))=\varnothing\neq\Sigma$. Otherwise there is $\omega\in I_c(\psi)$, so $f_H(I_c(\psi))\neq\Sigma$ because $\omega\in f_H(I_c(\psi))$ and $\omega\in\Sigma^{\omega}$.

This reflects IμTL is more expressive than its counterpart in the classical domain i.e. μTL.

5 Safety and Liveness in Classical and Intuitionistic Domain

The safety and liveness properties are the most fundamental properties of reactive systems, and characterized by elimination of bad happening and eventuality of good happening respectively. In the classical domain Alpern and Schneider[17] give topological characterization in which safety properties are closed sets and liveness properties are dense sets. The topological characterization has been extended by various researchers e.g. Gumm presented the notion of safety and liveness in the more abstract setting of Boolean algebras[18]. We have safety and liveness in terms of topology on $\sum^{\omega}$ for $\sum$ be a finite, the properties constitute a topology known as Cantor topology on $\sum^{\omega}$. This topology is induced by the topological closure operator Cl_c on $\sum^{\omega}$. The closure operator $Cl_c:P(\Sigma^{\omega})\to P(\Sigma^{\omega})$ is defined as $Cl_c(L)=\{\omega\in\Sigma^{\omega}\mid f_H(\omega)\cap\Sigma^{*}\subseteq f_H(L)\}$ for all $L\subseteq\Sigma^{\omega}$. We have $L\in R_B$ as a classical safety property if L is closed that is $Cl_c(L)=L$ and a classical liveness property if L is dense that is $Cl_c(L)=\sum^{\omega}$[2].

The underlying algebra of IμTL is Heyting algebra Λ_H. In order to express the notion of safety and liveness properties in Λ_H, an analogous to Cl_c, a closure operator Cl_i in the intuitionistic domain is established as $Cl_i:P(\Sigma^{\infty})\to P(\Sigma^{\infty})$ by defining $Cl_i(L)=\{\omega\in\Sigma^{\infty}\mid f_H(\omega)\cap\Sigma^{*}\subseteq f_H(L)\}$. It turns out that Cl_i is a topological closure operator on $\sum^{\infty}$ and induces Scott topology on it if $\sum$ is countable. Thus, the corresponding properties in intuitionistic domain are defined as $Cl_i(L)=L$ a safety property and $Cl_i(L)=\Sigma^{\infty}$ a liveness property for $L\in R_H$. The closure operator Cl_i is algebraically definable in Λ_H as for all $L\in R_H$, $Cl_i(L)=\{\omega\in\Sigma^{\infty}\mid f_H(\omega)\cap\Sigma^{*}\subseteq f_H(L)\}=\Sigma^{*}\Rightarrow L$. Therefore, L is an intuitionistic safety property iff $\Sigma^{*}\Rightarrow L=\Sigma^{\omega}$ iff $\Sigma^{*}\subseteq L$ iff $\Sigma^{*}\cup L=L$. The following proposition defines the generalized safety property characteristics[2].

Proposition 5. Let $\omega\in\Sigma^{\omega}$ let $L,L_1,L_2\in R_H$ and let $L\subseteq R_H$

1. $\sum^{\infty}$ is an intuitionistic safety property.
2. $\varnothing$ is an intuitionistic safety property.
3. $f_H(\omega)$ is an intuitionistic safety property.

4. If L_1 and L_2 are intuitionistic safety properties then so is $L_1 \cup L_2$.

5. If all $L \in \mathrm{L}$ are intuitionistic safety properties then so is $\bigcap_{L\in \mathrm{L}} L$.

6. If L_2 is an intuitionistic safety property then so is $L_1 \Rightarrow L_2$.

7. If L is an intuitionistic safety property then so is $-L = L \Rightarrow \varnothing$.

5.1 Mutual exclusion problem as a safety property in IμTL

In order to manifest IμTL implications, we have chosen an example regarding a trivial CSP solution to the mutual exclusion problem.

$$P_1 := *[l_o : \langle C_1; \overline{c}\rangle; l_1\langle N_1; \overline{c}\rangle]\|$$
$$P_2 := *[m_o : \langle N_2; \overline{c}\rangle; m_1\langle C_2; \overline{c}\rangle]$$

with C_1 and C_2 are the critical sections for the processes P_1 and P_2 respectively. The mutual exclusion property in this case is a safety property which requires $at\ l_o \wedge at\ m_1$ never holds. The solution proposed in Ref.[19] demonstrates that in P_1 we may visit l_o after an even number of communications, and in P_2 we may visit m_1 only after an odd number of communications. It is illustrated in Ref.[4] that this property cannot be expressed in LTL. These properties can be specified in μTL while by saying that l_o cannot hold at odd moments instead of saying that at l_o may hold at even moments, we have[5]

$$\odot(\nu Z.(-at\, l_o \wedge \odot\odot Z)).$$

Analogously, it is stated that at m_1 does not hold at even moments, and is interpreted by the formula

$$\nu Z.(-at\ m_1 \wedge \odot\odot Z).$$

In order to illustrate that this is an intuitionistic safety property, we have to show that the set of traces represented by the formula satisfies requirements for safety property as mentioned in Proposition 5. We first prove a lemma as follows.

Lemma 6. If L is an intuitionistic safety property, then $next_i(L) = \Sigma \cup \Sigma L$ is also a safety property.

Proof: Suppose that L is a safety property then $Cl_i(L)=L$. For proving $\Sigma\cup\Sigma L$ is a safety property, we need to prove that $Cl_i(\Sigma \cup \Sigma L) \subseteq \Sigma \cup \Sigma L$. Obviously, we have $\Sigma \cup \Sigma L \subseteq Cl_i(\Sigma \cup \Sigma L)$. The remaining is to prove that $Cl_i(\Sigma \cup \Sigma L) \subseteq \Sigma \cup \Sigma L$. Let $\omega \in Cl_i(\Sigma \cup \Sigma L)$. Either $\omega \in Cl_i(\Sigma)$ or $\omega \in Cl_i(\Sigma L) \setminus Cl_i(\Sigma)$. In the former case, we have $\omega\in\Sigma$ In the latter case, let $\omega = \sigma\omega'$ where $\sigma \in \Sigma$. Then $\omega' \in Cl_i(L) = L$. Therefore, $\omega\in\Sigma L$. This concludes the proof.

Proposition 7. If φ is a closed formula and $I_i(\varphi)$ is an intuitionistic safety property, then $\nu Z.(\varphi \wedge \odot\odot Z)$ is an intuitionistic safety property.

Proof: Since $I_i(\nu Z.(\varphi \wedge \odot\odot Z)) = \bigcap_{n\in Ord}[munext_i^{\rho}(\lambda Z.(\varphi \wedge \odot\odot Z))]^n(\Sigma^{\infty})$, according to Proposition 5, it is sufficient to prove that $[munext_i^{\rho}(\lambda Z.(\varphi \wedge \odot\odot Z))]^n(\Sigma^{\infty})$ is a safety property for all n. For n=0, we have

$$[munext_i^{\rho}(\lambda Z.(\varphi \wedge \odot\odot Z))]^n(\Sigma^{\infty}) = I_i(\varphi) \wedge next_i(next_i(\Sigma^{\infty})).$$

Since $I_i(\varphi)$ and Σ^{∞} are safety properties, according to Lemma 6 and Proposition 5, $[munext_i^{\rho}(\lambda Z.(\varphi \wedge \odot\odot Z))]^n(\Sigma^{\infty})$ is a safety property for n=0. Assume $[munext_i^{\rho}(\lambda Z.(\varphi \wedge \odot\odot Z))]^n(\Sigma^{\infty})$ is a safety property for n=k. Let $L = [munext_i^{\rho}(\lambda Z.(\varphi \wedge \odot\odot Z))]^n(\Sigma^{\infty})$. Then

$$[munext_i^{\rho}(\lambda Z.(\varphi \wedge \odot\odot Z))]^{k+1}(\Sigma^{\infty}) = [munext_i^{\rho}(\lambda Z.(\varphi \wedge \odot\odot Z))](L) = I_i(\varphi) \wedge next_i(next_i(L)).$$

Since $I_i(\varphi)$ and L are safety properties, according to Lemma 6 and Proposition 5, $[munext_i^{\rho}(\lambda Z.(\varphi \wedge \odot\odot Z))]^{k+1}(\Sigma^{\infty})$ is a safety property. This proves that $[munext_i^{\rho}(\lambda Z.(\varphi \wedge \odot\odot Z))]^n(\Sigma^{\infty})$ is a safety property for all n according to Proposition 5.

Clearly, the negation of a proposition represents an intuitionistic safety property. The above proposition and lemma illustrate that both $\nu Z.(-at\ m_1 \wedge \odot\odot Z)$ and $\odot(\nu Z.(-at\ l_o \wedge \odot\odot Z))$ are intuitionistic safety properties.

6 IμTL Perspectives for Assume-Guarantee Specifications

An assumption/guarantee specification of a system composed of an assumption part and a guarantee part, the former specifies the assumptions regarding environment of a system, while later specifies the properties by the system if the environment obeys the assumptions. If a reactive system satisfies a specification S and in an environment that satisfies an assumption A then this specification sometimes written as $A \Rightarrow S$. In a composed system i.e. one satisfying $A \Rightarrow S$ while other $S \Rightarrow A$, this implication has some problem depicted in Ref.[20]. The solution proposed in Ref.[21], while this formulation is elaborated and extended in various contexts in Refs.[22–24]. By employing linear-temporal logic of Manna and Pnueli[25] the solution to composition has been proposed in Ref.[20] with aspect of formulation concerning the handling of assumption/guarantees with internal handing, which simply are existential quantified variables in LTL.

In context of Heyting algebra of prefix-closed sets of finite behaviors, it has been illustrated in Ref.[23] for a suitable notion of concurrency an assumption/guarantee specifications $\varphi \xrightarrow{+} \psi$ corresponds to an intuitionistic implication $\varphi \xrightarrow{+} \psi$. This gives rise to composition rules based on conjunction of intuitionistic implication. Afterwards a more general interpretation of the operator $\xrightarrow{+}$ is provided in Ref.[26]. The interpretation again can be reduced to intuitionistic implication. The interpretation of the operator $\xrightarrow{+}$ over Heyting algebra Λ_H of prefix-closed set is given as for $\varphi, \psi \in \Omega_\mu$:

$$I_i(\varphi \xrightarrow{+} \psi) = \{\omega \in \Sigma^\infty \mid \forall \nu \in f_H(\omega) : \widetilde{f_H}(\nu) \subseteq I_i(\varphi)\ implies\ \nu \in I_i(\psi)\}$$

where $\widetilde{f_H}(\nu) : \Sigma^\infty \to R_H$ maps behaviors to their sets of proper prefixes i.e. $\widetilde{f_H}(\nu) = f_H(\nu) \setminus \{\nu\}$. Since the interpretation function for ILTL deducible from the interpretation function in IμTL, therefore, A-G specifications are interpretable both in IμTL and ILTL. The connective $\xrightarrow{+}$ introduced in Ref.[9] has interpretation in IμTL as:

$$I_i(\varphi \xrightarrow{+} \psi) = I_i((\psi \to \varphi) \to \psi).$$

Hence in Λ_H, A-G specifications are merely short hands for intuitionistic implication. The circular dependency of assumption/guarantee specifications is dealt in Ref.[25], and concise soundness proofs of various proof rules regarding circular dependent assumption/guarantee specifications are established. The composition rules for A-G specs are that they essentially only admit circular dependencies on safety properties. In classical linear temporal logic this is dealt through decomposition theorem Ref.[2], while disallowing circular dependencies on the liveness parts[17,27]. Thus, a similar, decomposition theorems for intuitionistic domain are conjectured, and for ILTL given in Ref.[2]. In Section 4.2 a correspondence between IμTL and ILTL is established, which could be implemented when dealing with A-G spec. In ILTL illustration of A-G spec the specification formula is taken as a formula belonging to LTL.

7 Conclusions

IμTL, an intuitionistic variant of linear-time μ-calculus, has been presented in this paper. It is capable to specify set of finite and infinite behaviors simultaneously. The proposed logic IμTL also interprets ILTL, the already presented variant of LTL in intuitionistic domain. A correspondence has been established between these logics i.e. IμTL and ILTL, this shows that all properties of a system which are interpretable by ILTL are also deducible through proposed logic i.e. IμTL. Therefore, IμTL encompasses all the properties of the ILTL, and in addition to these IμTL interprets intuitionistic safety properties defined over fixed point operators. Since these properties are

not expressible through LTL and consequently ILTL may not express them as well. Therefore, the expressibility of the most fundamental properties of the reactive systems like safety and liveness properties are demonstrated in the intuitionistic domain and elegantly illustrated in the proposed IμTL. The assumption/guarantee specification is also expressed in IμTL, and since the underlying formulas in case ILTL belong to LTL which is less expressive than μTL. Therefore, IμTL deals with formulas which are more expressive.

Acknowledgments: The authors thank anonymous referees for their comments that helped improving this paper.

References:

[1] Pnueli A. The temporal semantics of concurrent programs. Theoretical Computer Science, 1981,(13):45−60.

[2] Maier P. Intuitionistic LTL and a new characterization of safety and liveness. In: Proc. of the 18th Int'l Workshop CSL 2004, the 13th Annual Conf. of the EACSL. LNCS 3210, Berlin: Springer-Verlag, 2004. 295−309.

[3] Eisner C, Fisman D, Havlicek J, Lustig Y, Mclsaac A, Van Campenhout D. Reasoning with temporal logic on truncated paths. In: Proc. of the 15th Int'l Conf. on Computer Aided Verification (CAV). LNCS 2725, Springer-Verlag, 2003. 27−39.

[4] Wolper P. Temporal logic can be more expressive. Information and Control, 1983,56:72−99.

[5] Vardi MY. A temporal fixpoint calculus. In: Proc. of the 15th ACM SIGPLAN-SIGACT Symp. on Principles of Programming Languages. San Diego, 1988. 250−259.

[6] Barringer H, Kuiper R, Pnueli A. A really abstract concurrent model and its temporal logic. In: Proc. of the 13th ACM POPL. 1986.

[7] Wolper P. Synthesis of communicating processes from temporal logic specifications [Ph.D. Thesis]. Stanford University, 1982.

[8] Kaivola R. Axiomatising linear time μ-calculus. In: Proc. of the 6th Int'l Concurrency Theory, 1995,962:423−437.

[9] Kozen D. Results on the propositional μ-calculus. Proc. of the 9th Int'l Colloq. on Automata, Languages and Programming. 1982. 384−359.

[10] Clarke Jr EM, Grumberg O, Peled DA. Model Checking. The MIT Press, 1999.

[11] Alur R, Chudhuri S, Madhusudan P. A fixedpoint calculus for Local and Global Program Flows. In: Proc. of the POPL2006. 2006.

[12] Emerson EA, Jutla CS. Tree automata, mu-calculus, and determinacy. In: Proc. of the 32nd IEEE Symp. on Foundations of Computer Science. 1991. 368−377.

[13] Janin D, Walukiewicz I. On the expressive completeness of the propositional mu-calculus with respect to monadic second-order logic. In: Proc. of the CONCUR'96, the 7th Int'l Conf. on Concurrency Theory. LNCS 1119, Springer-Verlag, 1996. 263−277.

[14] Burch JR, Clarke EM, Dill DL, Hwang LJ, McMillan KL. Symbolic model checking: 10^{20} states and beyond. Information and Computation, 1992,98(2):142−170.

[15] McMillan KL. Symbolic Model Checking: An Approach to the State Explosion Problem. Kluwer Academic Publisher, 1993.

[16] Christian Dax. Games for linear Time μ-Calculus [Ph.D. Thesis]. Theoretical Computer Science Ludwig-Maximilian-University Munich, 2006.

[17] Alpern B, Schneider FB. Defining liveness. Information Processing Letters, 1985,21(4):181−185.

[18] Gumm HP. Another glance at the alpern-schineider characterization of safety and liveness in concurrent executions. Information Processing Letters, 1993,47(6):291−294.

[19] Lichtenstein O, Pnueli A. Checking that finite-state concurrent programs satisfy their linear specification. In: Proc. of the 12th ACM Symp. on the Principles of Programming Languages. 1985. 97−107.

[20] Jonsson B, Tsay YK. Assumption/Guarantee specifications in linear-time temporal logic. Theoretical Computer Science, 1996,167:47−72.

[21] Misra J, Chandy KM. Proofs of networks of processes. IEEE Trans. on Software Engineering, 1981,7(4):417−426.

[22] Abadi M, Lamport L. Composing specifications. ACM Trans. on Programming Languages and Systems, 1983,15(1):73−132,.

[23] Abadi M, Lamport L. Conjoining specifications. Technical Report 118, SRC DEC, 1993.

[24] Abadi M, Plotkin GD. A logical view of composition. Theoretical Computer Science, 1993,114(1):3−30.

[25] Manna Z, Pnueli A. The Temporal Logic of Reactive and Concurrent Systems: Specification. Springer-Verlag, 1992.

[26] Abadi M, Merz S. An abstract account of composition. In: Proc. of the 20th Int'l Symp. on Mathematical Foundations of Computer Science (MFCS). LNCS 969, Springer-Verlag, 1995. 499−508.

[27] Alpern B, Schneider FB. Recognizing safety and liveness. Distributed Computing, 1987,2(3):117−126.

KAZMI Syed Asad Raza was born in 1965. He is Ph.D. research scholar at the Institute of Software, the Chinese Academy of Sciences. His research areas are formal methods, quantum computing and embedded systems.

ZHANG Wen-Hui was born in 1963. He is a professor at the Institute of Software, the Chinese Academy of Sciences. His research areas are formal methods and software reliability for developing high quality software.