Math. Struct. in Comp. Science (2010), *vol.* 20, *pp.* 915–950. © Cambridge University Press 2010
doi:10.1017/S0960129510000253

Connection between logical and algebraic approaches to concurrent systems[†]

NAIJUN ZHAN

State Key Lab. of Comp. Sci., Institute of Software, Chinese Academy of Sciences,
100190, Beijing, P.R. China
Email: znj@ios.ac.cn

Received 4 January 2010; revised 7 May 2010

The logical and algebraic approaches are regarded as two of the dominant methodologies for the development of reactive and concurrent systems. It is well known that the logic approach is more abstract, but lacks compositionality; while the algebraic approach is inherently compositional, but lacks abstractness. However, connecting the two approaches is a major challenge in computer science, and many efforts have been directed to resolving the problem. Linking the algebraic approach to the logical approach has been satisfactorily resolved through the notion of characteristic formulae. But very limited success has been achieved so far in the other direction, as most of the established results have been developed only with respect to a simple semantics, which has usually been strong bisimulation. However, in practice, an observational semantics like weak bisimulation, which is much more complicated, is thought to be more useful. In this paper, we investigate how to connect the logical and algebraic approaches with respect to the observational preorder, which is a generalisation of weak bisimulation that takes divergence into account. We show the following results. First, we prove that the non-deterministic operator of process algebra can be defined in modal and temporal logics (such as the μ-calculus and the Fixpoint Logic with Chop) with respect to the observational preorder (in fact, the kernel of its precongruence). In this way, we can apply the logical approach to the design of a complex system in a compositional way. Second, we present two algorithms for constructing the characteristic formulae for a context-free process up to the preorder and its precongruence, respectively. The effect of this is that all the reductions for processes that are usually done in an algebraic setting can be handled in a logical setting.

1. Introduction

Two of the dominant methodologies for the development of reactive and concurrent systems are the algebraic (Milner 1986; Hoare 1985; Bergstra and Klop 1985) and logical (Pnueli 1977; Kozen 1983; Moszkowski 1986; Zhou *et al.* 1991; Stirling 2001) approaches, but they are completely different. In general, the former is compositional, that is, a complex system can be built by applying algebraic operators defined in the underlying process algebra to some existing subsystems, which means it is easy to find a connection

[†] This work is supported in part by the projects NSFC-60721061, NSFC-90718041, NSFC-60736017, NSFC-60970031 and RCS2008K001.

between the structure of a system to be developed and that of its specification or model. In an algebraic setting, the specifications or models are usually represented as a process term. Therefore, the algebraic approach is suitable for describing simulation properties like synchronisation, asynchronisation, exclusion and so on. But it is difficult to define global properties such as fairness and liveness because it lacks abstractness. In contrast, in a logical framework, a complex system is specified and designed from a global point of view, so the logical approach is appropriate for specifying global properties because of its abstractness. However, the logical approach is not suitable for defining simulation properties as it is hard to find a connection between the structure of a system to be developed and that of its specification.

As argued in Andersen *et al.* (1994), compositionality is very important in developing reactive and concurrent systems for at least the following reasons:

— It allows modular design and verification of complex systems so that the complexity is tractable.

— Following a redesign of a verified system, only the modified parts need to be verified again, rather than starting again from scratch with the whole system.

— Compositionality enables the partial specification of a large system. So, when designing a system or synthesising a process, it is possible to have undefined parts of a process and still be able to reason about it. For example, this technique can be applied to reveal inconsistencies in the specification or to prove that with the choices already taken in the design, no component supplied for the missing parts will ever be able to make the overall system satisfy the original specification.

— Finally, compositionality can allow the *reuse* of verified components so that their previous verification can be used to show that they meet the requirements placed on the components of a large system.

On the other hand, very few verification techniques (see, for example, Paige and Tarjan (1987)) and tools (see, for example, Roscoe (1997)) for use with process algebras have been established and successfully applied in practice. So we would like to find a way to reduce verification problems that may not be handled well in process algebraic settings to logical problems that can be handled using various verification techniques for modal and temporal logics.

However, finding a way to combine the two approaches so that we can capitalise on the advantages of the two approaches and avoid their disadvantages is a challenging problem.

In fact, many attempts have been made to achieve this goal. In particular, relating the algebraic approach to the logical approach has been resolved by constructing characteristic formulae of processes with respect to an underlying semantics. Graf and Sifakis (1986b) first gave a method for defining the characteristic formula of a finite term of CCS up to observational congruence. Steffen and Ingólfsdóttir (1994) refined this work by presenting an approach to defining the characteristic formula for a finite-state process up to some preorders. Müller-Olm (1999) also gave a method for defining the characteristic formula of a context-free process up to a preorder based on its rewriting system.

However, very limited success has been achieved so far in the other direction, as, in general, it is quite difficult to obtain compositionality for a logic. A potential solution to the problem could be either to introduce the underlying operators of process algebras directly into a logic, or to prove the definability of these operators in the logic. The former solution could make the resulting logic complicated and intractable, while the latter is very difficult, in particular, depending on the semantics used. Previous attempts have adopted the first approach. Barringer *et al.* (1984; 1985) discussed the sequential compositionality of linear temporal logic (Pnueli 1977) by introducing the chop (that is, the sequential composition of process algebra) into the logic. Rosner and Pnueli (1986) also investigated some logic properties of the extension. Analogously, Graf and Sifakis (1986a) and Larsen and Thomsen (1988), working independently, investigated non-deterministic compositionality by introducing the non-deterministic operator '$+$' of process algebra directly into modal μ-calculus like logics (Kozen 1983). However, Zhan and Majster-Cederbaum (2005) proved the definability of '$+$' in the modal μ-calculus with respect to strong bisimulation, and therefore concluded that the modal logics proposed in Graf and Sifakis (1986a) and Larsen and Thomsen (1988) can be encoded into the modal μ-calculus. Moreover, Zhan and Wu (2005) extended the result of Zhan and Majster-Cederbaum (2005) to Fixpoint Logic with Chop (FLC) by showing the definability of '$+$' in the logic with respect to strong bisimulation. As a by-product of the compositionality of FLC provided in Zhan and Wu (2005), the paper also presented an algorithm for constructing the characteristic formula of a context-free process up to strong bisimulation directly from its syntax, in contrast to previous work, which derived the characteristic formula of a process up to some equivalences or preorders from its semantics.

All previous attempts to link the logical approach to the algebraic approach have used the strong bisimulation semantics. Strong and weak bisimulations are two important semantics for process algebra (Milner 1986), but in practice, weak bisimulation is thought to be more useful. In addition, and comparatively speaking, weak bisimulation is much more complicated as it abstracts away internal actions, while observable and unobservable actions are not distinguished in strong bisimulation. For example, it is well known that weak bisimulation is not congruent as it is not preserved by the non-deterministic choice '$+$', while strong bisimulation is congruent (Milner 1986). Moreover, divergence cannot be handled in weak bisimulation, for example, $rec\ x.\tau;x+a;\epsilon$ is weakly bisimilar to $a;\epsilon$, even though the first process could engage in infinitely many internal actions τ, and therefore refuse to respond to any a-action. Motivated by this, an observational preorder was introduced as a generalisation of weak bisimulation (Abramsky 1987; Abramsky 1991; Hennessy and Plotkin 1980; Milner 1981). Like weak bisimulation, the observational preorder is not preserved by '$+$', but according to Milner's view, a largest precongruence of the preorder can be obtained automatically. In fact, Aceto and Hennessy (1992) explicitly defined the precongruence of the preorder, another preorder, and established a complete proof system for the congruent preorder.

For all these reasons, it is worth trying to establish a connection between the algebraic and logical approaches with respect to the observational preorder. We will address this issue in this paper. We will first consider the definability of '$+$' with respect to the congruent preorder in FLC, and then link FLC to $\mathrm{BPA}_{\delta}^{\epsilon,\Omega}$ so that we can use FLC to specify and design a complex system in a compositional manner. To this end, we first need to re-interpret the logic with respect to the observational semantics. We will then show the definability of '+' in FLC with respect to the observational semantics, as in Zhan and Wu (2005), though the proof is more involved. Following this, and based on the resulting compositionality of FLC, we will present two algorithms for constructing the characteristic formulae of a context-free process up to the preorder and its precongruence compositionally, respectively. The algorithms are much more complicated than those in Zhan and Wu (2005), since the characteristic formulae up to the preorders cannot be constructed from the syntax of the process.

The above investigations will be carried out within FLC and BPA.

FLC was invented by Müller-Olm (Müller-Olm 1999) and is an extension of the μ-calculus to include the chop operator. It is strictly more expressive than the μ-calculus since non-regular properties can be expressed in FLC. The μ-calculus (Kozen 1983) is a popular modal logic because most modal and temporal logics can be defined in it. However, the μ-calculus can only express regular properties (Emerson and Jutla 1991; Janin and Walukiewicz 1996). FLC has attracted increasing attention in computer science because of its expressiveness. For example, Lange and Stirling (2002) and Lange (2002) investigated the issues of FLC model checking on finite-state processes.

Basic Process Algebra was first proposed in Bergstra and Klop (1985) and acts as the core of most process algebras. Most concurrent and reactive programs can be modelled using BPA. In this paper, we adopt a version from Aceto and Hennessy (1992), which is extended by the addition of termination, deadlock and divergence, and is denoted by $\mathrm{BPA}_{\delta}^{\epsilon,\Omega}$.

Some preliminary results of this paper were reported in Zhan (2006).

Structure of the paper

The rest of this paper is structured as follows. Section 2 gives some preliminaries, mainly by introducing $\mathrm{BPA}_{\delta}^{\epsilon,\Omega}$ and FLC. Section 3 is devoted to showing that the choice '+' can be defined in FLC with respect to the observational semantics. Section 4 establishes a connection between the constructors of $\mathrm{BPA}_{\delta}^{\epsilon,\Omega}$ and the connectives of FLC^{+}. In Section 5, we apply the techniques in an example to show the advantages arising from the compositionality of FLC. In Section 6, we sketch how to construct the characteristic formulae up to the observational preorders compositionally. Finally, we present some brief conclusions in Section 7.

2. Preliminaries

In this section, we will cover some preliminary material, which is the basis for all the later discussions. This consists mainly of an introduction to $\mathrm{BPA}_{\delta}^{\epsilon,\Omega}$, adapted from Aceto and Hennessy (1992), and Fixpoint Logic with Chop.

2.1. *Basic Process Algebra with termination, deadlock and divergence* ($\mathrm{BPA}_{\delta}^{\epsilon,\Omega}$)

Let *Act* be a set of (atomic) observable actions, ranged over by $a, b, c, \cdots$, and τ be an unobservable action. We use Act_{τ} to stand for $Act \cup \{\tau\}$, ranged over by $\alpha, \beta, \cdots$. Let

$$\begin{array}{llll}
\text{Act} & \dfrac{}{\alpha \overset{\alpha}{\to} \epsilon} & \text{Rec} & \dfrac{E[rec.xE/x] \overset{\alpha}{\to} E'}{rec\ x.E \overset{\alpha}{\to} E'} \\
\text{Seq1} & \dfrac{E_1 \overset{\alpha}{\to} E_1'}{E_1; E_2 \overset{\alpha}{\to} E_1'; E_2} & \text{Seq2} & \dfrac{E_2 \overset{\alpha}{\to} E_2' \text{ and } \mathcal{T}(E_1)}{E_1; E_2 \overset{\alpha}{\to} E_2'} \\
\text{Nd1} & \dfrac{E_1 \overset{\alpha}{\to} E_1'}{E_1 + E_2 \overset{\alpha}{\to} E_1'} & \text{Nd2} & \dfrac{E_2 \overset{\alpha}{\to} E_2'}{E_1 + E_2 \overset{\alpha}{\to} E_2'}
\end{array}$$

Fig. 1. The operational semantics of $\mathscr{P}^s$

$\mathscr{X} = \{x, y, z, \ldots\}$ be a countable set of process variables. Sequential process terms are generated by the following grammar:

$$E ::= \delta \ \mid \ \epsilon \mid \Omega \mid x \mid \alpha \mid E_1; E_2 \mid E_1 + E_2 \mid rec\ x.E.$$

We denote the above language by $\mathscr{P}^s$. The set of all closed and guarded terms of $\mathscr{P}^s$ corresponds, essentially, to the *basic process algebra* (BPA) with the terminated process ϵ, the deadlocked process δ and the divergent process Ω, denoted $\text{BPA}_\delta^{\epsilon,\Omega}$, and ranged over by $P, Q, \cdots$.

An operational semantics of $\mathscr{P}^s$ can be given in the standard Plotkin style in the form of a transition system $(\mathscr{P}^s, \rightarrow)$ with $\rightarrow \subseteq \mathscr{P}^s \times Act_\tau \times \mathscr{P}^s$ that is the least relation derived from the rules in Figure 1, where $\mathscr{T} \subset \mathscr{P}^s$ is the least set which contains ϵ and is closed under the following rules:

(i) If $\mathscr{T}(E_1)$ and $\mathscr{T}(E_2)$, then $\mathscr{T}(E_1; E_2)$ and $\mathscr{T}(E_1 + E_2)$.
(ii) If $\mathscr{T}(E)$, then $\mathscr{T}(rec\ x.E)$.

Informally, $\mathscr{T}(P)$ indicates that P terminates[†].

Normally, a set of reference rules is not abstract enough to define an appropriate operational semantics for the process algebra under consideration since it cannot identify the sense in which two process terms are equivalent. Thus, various bisimulations or preorders have been proposed to define criteria saying when two processes are equivalent: two examples are strong and weak bisimulation (Milner 1986). The reference rules taken together with different bisimulations or preorders determine different semantics for the process algebra.

For our purposes we will just describe the observational preorder, which generalises weak bisimulation by considering divergence. For an overview of the semantics of process algebra, see van Glabbeek (2001).

In order to define the preorder, we need the following notions. Given an action $\alpha \in Act_\tau$, we use $\widehat{\alpha}$ to denote α if $\alpha \in Act$ and ε otherwise, where ε stands for the empty action. Moreover, $\overset{\varepsilon}{\rightarrow}$ denotes the identity relation over $\mathscr{P}^s$, that is, for any $E \in \mathscr{P}^s$, $E \overset{\varepsilon}{\rightarrow} E$. We

[†] As in Aceto and Hennessy (1992), we adopt the semantics of strict termination in the sense that $P + Q$ is terminated if and only if P and Q are both terminated. This is because using termination to make choice is impractical, and therefore is thought to be not well formed in much of the literature – see, for example, Gorrieri and Rensink (2001).

use $\overset{\alpha}{\Rightarrow}$ to stand for the sequence of transitions $(\xrightarrow{\tau})^{*}\cdot\xrightarrow{\alpha}\cdot(\xrightarrow{\tau})^{*}$ and $\overset{\varepsilon}{\Rightarrow}$ for $(\xrightarrow{\tau})^{*}$. We also use $E\xrightarrow{t}$ to mean $E\xrightarrow{\alpha_1}E_1\xrightarrow{\alpha_2}E_2\cdots\xrightarrow{\alpha_n}E_n$ for some $E_1,\cdots,E_n$, where $t=\alpha_1\cdots\alpha_n\in Act_{\tau}^{*}$. We say that a process term E is weak terminated if $\forall E'.(E\overset{\varepsilon}{\Rightarrow}E'\wedge E'\not\xrightarrow{\tau})\Rightarrow\mathscr{T}(E')$, and denote it by $\mathbb{T}(E)$.

We say that a term E is *convergent*, denoted by $\downarrow(E)$, if and only if E cannot perform an infinite sequence of τ actions, formally, $E\not\xrightarrow{\tau^{\omega}}$. Otherwise, E is said to be *divergent*, written $\uparrow(E)$. We say $\downarrow_{\tau}(E)$ if $\downarrow(E)$, and $\downarrow_{a}(E)$ if $\downarrow(E)$ and for each E', $E\overset{a}{\Rightarrow}E'$ implies $\downarrow(E')$, where $a\in Act$.

Definition 1. Let $\preceq$ be the largest binary relation over $\mathrm{BPA}_{\delta}^{\epsilon,\Omega}$ that for each $P,Q\in\mathrm{BPA}_{\delta}^{\epsilon,\Omega}$, satisfies $P\preceq Q$ if and only if:

— if $\downarrow(P)$, then $\mathbb{T}(P)$ if and only if $\mathbb{T}(Q)$;

— whenever $P\xrightarrow{\alpha}P'$, for some Q', we have $Q\overset{\widehat{\alpha}}{\Rightarrow}Q'$ and $(P'\preceq Q')$;

— if $\downarrow_{\alpha}(P)$, then $\downarrow_{\alpha}(Q)$, and whenever $Q\xrightarrow{\alpha}Q'$, for some P', we have $P\overset{\widehat{\alpha}}{\Rightarrow}P'$ and $P'\preceq Q'$;

where $\alpha\in Act_{\tau}$.

Informally, $P\preceq Q$ means that P and Q are weakly bisimilar except that sometimes P may diverge more frequently than Q. In the absence of divergence, $P\preceq Q$ means that P and Q are weakly bisimilar.

It is obvious that $\preceq$ is a preorder. We use $\approx$ to denote $\preceq\cap\preceq^{-1}$.

It is well known in process algebra circles that the above preorder is not congruent, for example, $a\preceq\tau;a$, but $a+b\not\preceq\tau;a+b$. Also, from the above example, we see that $\approx$ is an equivalence relation, but not congruent. However, following Milner (1986), we have a standard way of associating a precongruence with $\preceq$. Aceto and Hennessy (1992) proved that the implicit congruence associated with $\preceq$ coincides with the preorder defined below, which is denoted by $\preceq^{*}$.

Definition 2. For each $P,Q\in\mathrm{BPA}_{\delta}^{\epsilon,\Omega}$, we have $P\preceq^{*}Q$ if and only if:

— $\forall a\in Act$, whenever $P\xrightarrow{a}P'$, for some Q', we have $Q\overset{a}{\Rightarrow}Q'$ and $P'\preceq Q'$;

— if $P\overset{\tau}{\Rightarrow}P'$, then

(a) $\downarrow(P')$ implies, for some Q', that $Q\overset{\tau}{\Rightarrow}Q'$ and $P'\preceq Q'$;

(b) $\uparrow(P')$ implies, for some Q', that $Q\overset{\varepsilon}{\Rightarrow}Q'$ and $P'\preceq Q'$;

— if $\downarrow_{\alpha}(P)$, then $\downarrow_{\alpha}(Q)$, and whenever $Q\xrightarrow{\alpha}Q'$, for some P', we have $P\overset{\alpha}{\Rightarrow}P'$ and $P'\preceq Q'$;

— if $\downarrow(P)$, then $\mathbb{T}(P)$ if and only if $\mathbb{T}(Q)$;

where $\alpha\in Act_{\tau}$.

Theorem 1 (Aceto and Hennessy 1992). For any $P,Q\in\mathrm{BPA}_{\delta}^{\epsilon,\Omega}$, we have $P\preceq Q$ if and only if $P\preceq^{*}Q$ or $P\preceq^{*}\tau;Q$ or $\tau;P\preceq^{*}Q$.

It is easy to see that $\tau\preceq\epsilon$ but $\tau\not\preceq^{*}\epsilon$. However, $\tau\preceq^{*}\tau;\epsilon$.

In the following, we will use $\approx^*$ to denote $\preceq^* \cap \preceq^{*-1}$. It is easy to see that $\approx^*$ is equivalent as well as congruent.

Aceto and Hennessy (1992) established the following[†] complete proof system for $\preceq^*$ over $\mathrm{BPA}_\delta^{\epsilon,\Omega}$:

A0	$E_1 + E_2 = E_2 + E_1$	A1	$(E_1 + E_2) + E_3 = E_1 + (E_2 + E_3)$
A2	$E + E = E$	A3	$(E_1 + E_2); E_3 = (E_1; E_3) + (E_2; E_3)$
A4	$(E_1; E_2); E_3 = E_1; (E_2; E_3)$	A5	$rec\ x.E = E\{rec\ x.E/x\}$
A6	$E + \delta = E$	A7	$\delta; E = \delta$
A8	$E; \epsilon = E$	A9	$\epsilon; E = E$
A10	$\Omega \leqslant x$	A11	$\tau; (x + \Omega) \leqslant x + \Omega$
A12	$\Omega; x \leqslant \Omega$	A13	$\mu; \tau = \mu$
A14	$\tau; x + x = x$	A15	$\mu; (x + \tau; y) = \mu; (x + \tau; y) + \mu; y.$

It is easy to extend the definitions of the above relations to $\mathscr{P}^s$. For example, let $E_1, E_2 \in \mathscr{P}^s$, and

$$fn(E_1) \cup fn(E_2) \subseteq \{x_1, \cdots, x_n\}.$$

If

$$E_1\{P_1/x_1, \cdots, P_n/x_n\} \preceq E_2\{P_1/x_1, \cdots, P_n/x_n\}$$

for any $P_1, \cdots, P_n \in \mathrm{BPA}_\delta^{\epsilon,\Omega}$, then $E_1 \preceq E_2$.

2.2. *Fixpoint Logic with Chop*

Let $X, Y, Z, \cdots$ range over an infinite set *Var* of *variables*. Let *tt* and *ff* be *propositional constants* as usual, and $\surd$ be another special propositional constant, which is used to indicate whether a process has terminated or not. The formulae of FLC are generated according to the grammar

$$\phi ::= tt \mid ff \mid \surd \mid \tau \mid X \mid [\alpha] \mid \langle\alpha\rangle \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2 \mid \phi_1; \phi_2 \mid \mu X.\phi \mid \nu X.\phi$$

where $X \in Var$ and $\alpha \in Act_\tau$.

Some notation will be defined in the same way as in the modal μ-calculus, for example, *free* and *bound* occurrences of variables, and *closed* and *open* formulae. The two *fixpoint operators* μX and νX are treated as quantifiers. We will use $fn(\phi)$ to stand for all variables that have some free occurrence in ϕ, and $bn(\phi)$ for all variables that have some bound occurrence in ϕ. We use $c\mathscr{FLC}$ to denote the set of all closed formulae of FLC.

FLC is interpreted in the second-order, that is, formulae are interpreted as a *monotonic predicate transformer*, which is a monotonic function with the type $2^{\mathrm{BPA}_\delta^{\epsilon,\Omega}} \to 2^{\mathrm{BPA}_\delta^{\epsilon,\Omega}}$. Here we say that a predicate transformer f is monotonic in the sense that for any given $\mathscr{A}_1 \subseteq \mathscr{A}_2 \subseteq \mathrm{BPA}_\delta^{\epsilon,\Omega}$, we have $f(\mathscr{A}_1) \subseteq f(\mathscr{A}_2)$[‡]. Thus, the chop ; is naturally interpreted as

[†] The proof system for $\mathrm{BPA}_\delta^{\epsilon,\Omega}$ presented in this paper is in fact a little different from the one in Aceto and Hennessy (1992). However, Aceto and Hennessy (1992) pointed out that this variant is still complete.

[‡] In fact, FLC can be interpreted more generally as in Müller-Olm (1999) over a labelled transition system in which some states might not be context-free process terms.

functional composition. We use MPT to represent all the monotonic predicate transformers over $\mathrm{BPA}_\delta^{\epsilon,\Omega}$. The meaning of variables is given by a *valuation* ρ with the type $Var \rightarrow \mathrm{MPT}$. We have that $\rho[X \rightsquigarrow f]$ agrees with ρ except for associating X with f.

Definition 3. The meaning of a formula ϕ, under a valuation ρ, denoted by $[\![\phi]\!]_\rho$, is defined inductively as follows:

$$\begin{aligned}
[\![tt]\!]_\rho(\mathscr{A}) &= \mathrm{BPA}_\delta^{\epsilon,\Omega}\\
[\![ff]\!]_\rho(\mathscr{A}) &= \varnothing\\
[\![\surd]\!]_\rho(\mathscr{A}) &= \{P \in \mathrm{BPA}_\delta^{\epsilon,\Omega} \mid \mathscr{T}(P)\}\\
[\![\tau]\!]_\rho(\mathscr{A}) &= \mathscr{A}\\
[\![X]\!]_\rho(\mathscr{A}) &= \rho(X)(\mathscr{A})\\
[\![[\alpha]]\!]_\rho(\mathscr{A}) &= \{P \in \mathrm{BPA}_\delta^{\epsilon,\Omega} \mid \neg\mathscr{T}(P) \wedge \downarrow(P) \wedge \forall P' \in \mathrm{BPA}_\delta^{\epsilon,\Omega}.P \xrightarrow{\alpha} P' \Rightarrow P' \in \mathscr{A}\}\\
[\![\langle\alpha\rangle]\!]_\rho(\mathscr{A}) &= \{P \in \mathrm{BPA}_\delta^{\epsilon,\Omega} \mid \exists P' \in \mathrm{BPA}_\delta^{\epsilon,\Omega}.P \xrightarrow{\alpha} P' \wedge P' \in \mathscr{A}\}\\
[\![\phi_1 \wedge \phi_2]\!]_\rho(\mathscr{A}) &= [\![\phi_1]\!]_\rho(\mathscr{A}) \cap [\![\phi_2]\!]_\rho(\mathscr{A})\\
[\![\phi_1 \vee \phi_2]\!]_\rho(\mathscr{A}) &= [\![\phi_1]\!]_\rho(\mathscr{A}) \cup [\![\phi_2]\!]_\rho(\mathscr{A})\\
[\![\phi_1 ; \phi_2]\!]_\rho &= [\![\phi_1]\!]_\rho \cdot [\![\phi_2]\!]_\rho\\
[\![\mu X.\phi]\!]_\rho &= \sqcap\{f \in \mathrm{MPT_T} \mid [\![\phi]\!]_{\rho[X \rightsquigarrow f]} \subseteq f\}\\
[\![\nu X.\phi]\!]_\rho &= \sqcup\{f \in \mathrm{MPT_T} \mid [\![\phi]\!]_{\rho[X \rightsquigarrow f]} \supseteq f\}
\end{aligned}$$

where $\mathscr{A} \subseteq \mathrm{BPA}_\delta^{\epsilon,\Omega}$, and $\cdot$ stands for the composition operator over functions.

Note that because ϵ, Ω and δ have different behaviour in the presence of ;, they should be distinguished in FLC. To this end, we interpret $[\alpha]$ differently from the way it is in Müller-Olm (1999). According to our interpretation, $P \models [\alpha]$ only if $\neg\mathscr{T}(P) \wedge \downarrow(P)$, while in Müller-Olm (1999), $P \models [\alpha]$ holds for any $P \in \mathscr{P}^s$. Thus, it is easy to show that ϵ and Ω do not meet $\bigwedge_{\alpha \in Act_\tau}[\alpha];ff$, while $\bigwedge_{\alpha \in Act_\tau}[\alpha];ff$ is the characteristic formula of δ up to $\sim$, which is the largest strong bisimulation.

The set of processes *satisfying* a given closed formula ϕ is $\phi(\mathrm{BPA}_\delta^{\epsilon,\Omega})$. A process P is said to satisfy ϕ if and only if $P \in [\![\phi]\!]_\rho(\mathrm{BPA}_\delta^{\epsilon,\Omega})$ under some valuation ρ, denoted by $P \models_\rho \phi$. If ρ is clear from the context, we just write $P \models \phi$. Also, $\phi \Rightarrow \psi$ means $[\![\phi]\!]_\rho(\mathscr{A}) \subseteq [\![\psi]\!]_\rho(\mathscr{A})$ for any $\mathscr{A} \subseteq \mathrm{BPA}_\delta^{\epsilon,\Omega}$ and any ρ. And $\phi \Leftrightarrow \psi$ means $(\phi \Rightarrow \psi) \wedge (\psi \Rightarrow \phi)$. The other denotations are defined in the standard way.

In order to investigate the observable behaviour of systems, Stirling (2001) introduced observable modalities $\langle\!\langle\rangle\!\rangle$ and $[\![\ ]\!]$ into HML (Hennessy–Milner Logic). Formally, the meaning of $\langle\!\langle\rangle\!\rangle$ is defined as

$$[\![\langle\!\langle\rangle\!\rangle]\!]_\rho(\mathscr{A}) = \{P \mid \exists P'.P \overset{\varepsilon}{\Rightarrow} P' \wedge P' \in \mathscr{A}\}.$$

The meaning of $[\![\ ]\!]$ can be given dually. Stirling pointed out that the two observable modalities are not definable in HML, though they are definable in the modal μ-calculus (Stirling 2001). The following lemma will show how to define the two observable modalities in FLC.

Lemma 1.

(1) $\langle\!\langle\rangle\!\rangle \Leftrightarrow \mu X.\langle\tau\rangle ; X \vee \tau$.
(2) $\llbracket\ \rrbracket \Leftrightarrow \nu X.[\tau] ; X \wedge \tau$.

Let $\langle\!\langle\alpha\rangle\!\rangle \mathrel{\widehat{=}} \langle\!\langle\rangle\!\rangle ; \langle\alpha\rangle ; \langle\!\langle\rangle\!\rangle$ and $\llbracket\alpha\rrbracket \mathrel{\widehat{=}} \llbracket\ \rrbracket ; [\alpha] ; \llbracket\ \rrbracket$ for any $\alpha \in Act_\tau$. We call $\langle\!\langle\alpha\rangle\!\rangle$ and $\llbracket\alpha\rrbracket$ the *weak diamond* α and the *weak box* α, respectively. $\surd\!\!\surd \mathrel{\widehat{=}} \llbracket\ \rrbracket ; \langle\!\langle\rangle\!\rangle ; \surd$, means that any derivative of a process P must terminate after finitely many τ steps, that is $\mathbb{T}(P)$.

Now, let wFLC be the set of formulae generated from the grammar of FLC except that $\langle\!\langle\rangle\!\rangle$ and $\llbracket\ \rrbracket$ are formulae and $[\alpha]$, $\langle\alpha\rangle$ and $\surd$ are replaced by $\llbracket\alpha\rrbracket$, $\langle\!\langle\alpha\rangle\!\rangle$, and $\surd\!\!\surd$, respectively, where $\alpha \in Act$. We use $w\mathscr{FLC}$ to denote the set of closed formulae of wFLC. It is easy to see that $w\mathscr{FLC}$ is a proper subset of $c\mathscr{FLC}$.

In a similar way to Steffen and Ingólfsdóttir (1994), we can show that each $\psi \in w\mathscr{FLC}$ is an invariant of $\preceq$, that is we have the following theorem.

Theorem 2. Given $P, Q \in \mathrm{BPA}_\delta^{\epsilon,\Omega}$, we have $P \preceq Q$ if and only if for any $\psi \in w\mathscr{FLC}$, we have $P \models \psi$ if and only if $Q \models \psi$.

3. Defining the non-deterministic choice '+' in FLC with respect to $\approx^*$

In order to describe the properties of non-deterministic programs using the logical approach in a compositional way, Graf and Sifakis (1986a) and Larsen and Thomsen (1988) introduced the non-deterministic choice '+' from process algebras into modal logics like the μ-calculus, and established Synchronisation Tree Logic (STL) and Modal Process Logic, respectively. Intuitively, $P \models \phi + \psi$ means that there exist P_1 and P_2 such that $P = P_1 + P_2$, $P_1 \models \phi$ and $P_2 \models \psi$, where $=$ stands for a preorder or bisimulation on models. Obviously, the logic depends on the underlying relation on models. In Graf and Sifakis (1986a) and Larsen and Thomsen (1988), '=' is interpreted as strong bisimulation.

Zhan and Majster-Cederbaum (2005) showed that the non-deterministic choice '+' can be defined by disjunction and conjunction in the modal μ-calculus with respect to strong bisimulation. Zhan and Wu (2005) extended the results of Zhan and Majster-Cederbaum (2005) to FLC by showing that '+' is still definable in FLC with respect to strong bisimulation.

In the following section, we will show that '+' can also be derived by conjunction and disjunction in FLC with respect to the observational equivalence $\approx^*$.

3.1. FLC$^+$ *with respect to* $\approx^*$

We will first introduce '+' directly into FLC and establish FLC$^+$ with respect to $\approx^*$. The formulae of FLC$^+$ are defined by the following grammar:

$$\phi ::= p \mid \tau \mid X \mid \langle\alpha\rangle \mid [\alpha] \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2 \mid \phi_1 ; \phi_2 \mid \phi_1 + \phi_2 \mid \mu X.\phi \mid \nu X.\phi$$

where p stands for tt, ff or $\surd$.

Given a valuation ρ, the meaning of $\phi + \psi$ is defined by

$$\llbracket\phi_1 + \phi_2\rrbracket_\rho(\mathscr{A}) = \{P \in \mathrm{BPA}_\delta^{\epsilon,\Omega} \mid P \approx^* P_1 + P_2 \wedge P_1 \in \llbracket\phi_1\rrbracket_\rho(\mathscr{A}) \wedge P_2 \in \llbracket\phi_2\rrbracket_\rho(\mathscr{A})\}. \quad (1)$$

The other constructs are interpreted as in FLC.

Now let w FLC$^+$ be the set of formulae generated from the grammar of FLC$^+$ except that $[\alpha]$, $\langle\alpha\rangle$ and $\surd$ are replaced by $[\![\alpha]\!]$, $\langle\!\langle\alpha\rangle\!\rangle$, and $\surd\!\!\surd$, respectively. In the following, we use $@$ to stand for $\langle\!\langle\alpha\rangle\!\rangle$ or $[\![\alpha]\!]$, and σ for ν or μ.

The following lemma follows directly from the definitions of the semantics of wFLC and wFLC$^+$.

Lemma 2.

N	$\tau;\phi \Leftrightarrow \phi;\tau \Leftrightarrow \phi$	P1	$p;\phi \Leftrightarrow p$
P2	$\phi + ff \Leftrightarrow ff$	P3	$p + p \Leftrightarrow p$
P4	$\langle\!\langle\alpha\rangle\!\rangle; ff \Leftrightarrow ff$	T1	$\surd\!\!\surd \wedge @;\phi \Leftrightarrow ff$
T2	$\surd\!\!\surd + @;\phi \Leftrightarrow ff$	T3	$\surd\!\!\surd \wedge \tau \Leftrightarrow \surd\!\!\surd$
T4	$\surd\!\!\surd + tt \Leftrightarrow \surd\!\!\surd$	T5	$\surd\!\!\surd + \tau \Leftrightarrow \surd\!\!\surd$
S1	$\phi + \psi \Leftrightarrow \psi + \phi$	S2	$(\phi + \psi) + \varphi \Leftrightarrow \phi + (\psi + \varphi)$
SI	$\phi + (\psi \wedge \varphi) \Rightarrow (\phi + \psi) \wedge (\phi + \varphi)$	DC	$(\phi \vee \psi);\varphi \Leftrightarrow (\phi;\varphi) \vee (\psi;\varphi)$
SC	$(\phi + \psi);\varphi \Leftrightarrow (\phi;\varphi) + (\psi;\varphi)$	C	$(\phi;\psi);\varphi \Leftrightarrow \phi;(\psi;\varphi)$
IC	$(\phi \wedge \psi);\varphi \Leftrightarrow (\phi;\varphi) \wedge (\psi;\varphi)$	DB	$\langle\!\langle\alpha\rangle\!\rangle;\phi_1 \wedge [\![\alpha]\!];\phi_2 \Rightarrow \langle\!\langle\alpha\rangle\!\rangle;(\phi_1 \wedge \phi_2)$
DD	$\langle\!\langle\alpha\rangle\!\rangle;\phi_1 \vee \langle\!\langle\alpha\rangle\!\rangle;\phi_2 \Leftrightarrow \langle\!\langle\alpha\rangle\!\rangle;(\phi_1 \vee \phi_2)$		

A formula ϕ is called a *propositional normal form* (PNF for short) if it does not contain any subformula of the form $p;\psi$ or $\tau;\psi$ or $\psi;\tau$.

Lemma 3. For any given formula ϕ, there is another formula ϕ' that is a PNF such that $\phi \Leftrightarrow \phi'$.

Thus, from now on, we assume that all formulae are PNF unless otherwise stated. We will now define what it means for a formula to be a *guard*.

Definition 4.

(1) $@$ and p are guards.
(2) If ϕ and ψ are guards, so are $\phi \wedge \psi$, $\phi \vee \psi$ and $\phi + \psi$.
(3) If ϕ is a guard, so are $\phi;\psi$ and $\sigma X.\phi$, where ψ is any formula of FLC$^+$.

X is said to be *guarded* in ϕ if each occurrence of X is within a subformula ψ that is a guard. If all variables in $fn(\phi) \cup bn(\phi)$ are guarded, then ϕ is called *guarded.* A formula ϕ is said to be *strictly guarded* if ϕ is guarded and for any $X \in fn(\phi) \cup bn(\phi)$, there does not exist a subformula of the form $X + \psi$, $(X \odot \chi) + \psi$, $(X;\varphi) + \chi$ or $(X;\varphi \odot \chi) + \psi$, where $\odot \in \{\vee, \wedge\}$.

Example 1. The formulae $\langle\!\langle\alpha\rangle\!\rangle;X;Y, \nu X.(\langle\!\langle\alpha\rangle\!\rangle \vee \langle\!\langle\beta\rangle\!\rangle);X;(Y + Z), ff;X$ are guarded, but $X, \langle\!\langle\alpha\rangle\!\rangle \wedge X, \mu X.(X + Y) \vee [\![\alpha]\!], \mu X.(\langle\!\langle\alpha\rangle\!\rangle;X \vee \langle\!\langle\beta\rangle\!\rangle);\mu Y.(Y + \langle\!\langle\alpha\rangle\!\rangle)$ are not. $\langle\!\langle\alpha\rangle\!\rangle;X;Y$ and $ff;X$ are strictly guarded, but $\nu X.(\langle\!\langle\alpha\rangle\!\rangle \vee \langle\!\langle\beta\rangle\!\rangle);X;(Y + Z)$ is not.

We will use $\mathscr{L}_{\mathrm{FLC}^+}$ to denote all formulae of FLC$^+$ that are closed and guarded, and $\mathscr{L}_{\mathrm{FLC}}$ for the subset of $c\mathscr{FLC}$ in which all formulae are guarded.

The following lemma states the monotonicity of the semantics, which follows immediately from the definition.

Lemma 4.

(1) If $\phi \Rightarrow \psi$, then $\phi;\varphi \Rightarrow \psi;\varphi$ and $\varphi;\phi \Rightarrow \varphi;\psi$.
(2) If $\phi_1 \Rightarrow \phi_2$ and $\psi_1 \Rightarrow \psi_2$, then $\phi_1 + \psi_1 \Rightarrow \phi_2 + \psi_2$.
(3) For any valuation ρ, ρ' and any $\phi \in \mathscr{L}_{\mathrm{FLC}^+}$, if $\rho \subseteq \rho'$, then $[\![\phi]\!]_\rho \subseteq [\![\phi]\!]_{\rho'}$.
(4) For any $\phi \in \mathscr{L}_{\mathrm{FLC}^+}$, if ρ is a monotonic valuation and $\mathscr{A}_1 \subseteq \mathscr{A}_2$, then $[\![\phi]\!]_\rho(\mathscr{A}_1) \subseteq [\![\phi]\!]_\rho(\mathscr{A}_2)$.

Definition 5. Given a set of processes $\mathscr{A} \subseteq \mathrm{BPA}_\delta^{\epsilon,\Omega}$, $\mathscr{A}$ is said to be *closed* with respect to $\approx^*$ if $\forall P \in \mathscr{A}$ and $\forall Q \in \mathrm{BPA}_\delta^{\epsilon,\Omega}$, $P \approx^* Q$ implies that $Q \in \mathscr{A}$.

In the following, we will use $\mathscr{C}_{\approx^*}$ to denote the set $\{\mathscr{A} \subseteq \mathrm{BPA}_\delta^{\epsilon,\Omega} \mid \mathscr{A}$ is closed with respect to $\approx^*\}$.

We have the following results arising from the above definition.

Lemma 5. If $\mathscr{A}_1, \mathscr{A}_2 \in \mathscr{C}_{\approx^*}$, then:

(1) $\mathscr{A}_1 \cap \mathscr{A}_2$ and $\mathscr{A}_1 \cup \mathscr{A}_2$ are closed with respect to $\approx^*$.
(2) $\{P \in \mathrm{BPA}_\delta^{\epsilon,\Omega} \mid$ if $P \overset{a}{\Rightarrow} P'$ then $P' \in \mathscr{A}_1\}$ is closed with respect to $\approx^*$.
(3) $\{P \in \mathrm{BPA}_\delta^{\epsilon,\Omega} \mid \exists P' \in \mathscr{A}_1.P \overset{a}{\Rightarrow} P'\}$ is closed with respect to $\approx^*$.
(4) $\mathscr{A}_1 + \mathscr{A}_2$ is closed with respect to $\approx^*$, where $\mathscr{A}_1 + \mathscr{A}_2$ denotes the set $\{P \mid \exists P_1 \in \mathscr{A}_1.\exists P_2 \in \mathscr{A}_2.P \approx^* P_1 + P_2\}$.

Proof. The proofs for parts 1, 2 and 3 can be found in Stirling (2001), and the proof for part 4 is straightforward by Definition 5. □

For any set of processes $\mathscr{A} \subseteq \mathrm{BPA}_\delta^{\epsilon,\Omega}$, we can associate with it the following set:

$$\mathscr{A}^d \ \widehat{=}\ \{P \in \mathscr{A} \mid \text{ if } P \approx^* Q \text{ and } Q \in \mathrm{BPA}_\delta^{\epsilon,\Omega} \text{ then } Q \in \mathscr{A}\}.$$

The set $\mathscr{A}^d$ is the largest set that is closed with respect to $\approx^*$ contained in $\mathscr{A}$.

Lemma 6. For any set $\mathscr{A}, \mathscr{A}_i \subseteq \mathrm{BPA}_\delta^{\epsilon,\Omega}$, where $i = 1, 2$, we have:

(1) $\mathscr{A}^d \in \mathscr{C}_{\approx^*}$.
(2) $\mathscr{A}^d \subseteq \mathscr{A}$.
(3) $\mathscr{A}^d = \mathscr{A}$ if $\mathscr{A} \in \mathscr{C}_{\approx^*}$.
(4) $\mathscr{A}_1^d \subseteq \mathscr{A}_2^d$ if $\mathscr{A}_1 \subseteq \mathscr{A}_2$.
(5) $\mathscr{A}_1^d + \mathscr{A}_2^d \subseteq \mathscr{A}^d$ if $\mathscr{A}_1 + \mathscr{A}_2 \subseteq \mathscr{A}$.

Proof. The statements are immediate from the definition. □

Definition 6. We say that $f \in \mathrm{MPT_T}$ preserves $\mathscr{C}_{\approx^*}$ if $f(\mathscr{A}) \in \mathscr{C}_{\approx^*}$ for any $\mathscr{A} \in \mathscr{C}_{\approx^*}$. Also, a valuation ρ is said to preserve $\mathscr{C}_{\approx^*}$ if for any $X \in \mathit{Var}$, we have $\rho(X)$ preserves $\mathscr{C}_{\approx^*}$.

We will use f^d to denote the predicate transfer defined as $f^d(\mathscr{A}) = (f(\mathscr{A}))^d$, and ρ^d for the valuation defined by $\rho^d(X) = (\rho(X))^d$.

From Lemma 6, it is clear that $f \subseteq f'$ implies $f^d \subseteq_{\mathscr{C}_\approx} (f')^d$ for any $f, f' \in \mathrm{MPT_T}$, where $f \subseteq_{\mathscr{C}_{\approx^*}} f'$ means that for any $\mathscr{A} \in \mathscr{C}_{\approx^*}$, we have $f(\mathscr{A}) \subseteq f'(\mathscr{A})$. But the converse is not true in general. Also, from the definition, f^d and ρ^d both preserve $\mathscr{C}_\approx$.

Lemma 7. For any $f \in \mathrm{MPT_T}$, any $\phi \in \mathscr{L}_{\mathrm{FLC}^+}$ and any valuation ρ:

(1) If ρ preserves $\mathscr{C}_{\approx^*}$, so does $[\![\phi]\!]_\rho$.
(2) $[\![\phi]\!]_{\rho^d} \subseteq_{\mathscr{C}_{\approx^*}} f^d$ if $[\![\phi]\!]_\rho \subseteq_{\mathscr{C}_{\approx^*}} f$.
(3) $f^d \subseteq_{\mathscr{C}_{\approx^*}} [\![\phi]\!]_{\rho^d}$ if $f \subseteq_{\mathscr{C}_{\approx^*}} [\![\phi]\!]_\rho$.

Proof. The proof proceeds by simultaneous induction on the structure of ϕ: we will only consider the two interesting cases.

— $\phi = \phi_1 ; \phi_2$

(1) From the induction hypothesis, it is easy to see that $[\![\phi_1]\!]_\rho$ and $[\![\phi_2]\!]_\rho$ preserve $\mathscr{C}_{\approx^*}$. Therefore, $[\![\phi_1]\!]_\rho \cdot [\![\phi_2]\!]_\rho$ also preserves $\mathscr{C}_{\approx^*}$ by Definition 6, namely $[\![\phi_1 ; \phi_2]\!]_\rho$ preserves $\mathscr{C}_{\approx^*}$ according to Definition 3.

(2) From the induction hypothesis for (1), we get that $[\![\phi_1]\!]_{\rho^d}$ and $[\![\phi_2]\!]_{\rho^d}$ preserve $\mathscr{C}_{\approx^*}$. Thus, $[\![\phi_1 ; \phi_2]\!]_{\rho^d}$ also preserves $\mathscr{C}_{\approx^*}$ by Definition 6 and Definition 3. So, for any $\mathscr{A} \in \mathscr{C}_{\approx^*}$, $P \in [\![\phi_1 ; \phi_2]\!]_{\rho^d}(\mathscr{A})$, and any $Q \in \mathrm{BPA}_\delta^{\epsilon,\Omega}$ such that $P \approx^* Q$, it follows that $Q \in [\![\phi_1 ; \phi_2]\!]_{\rho^d}(\mathscr{A})$. On the other hand, we have that $[\![\phi_1 ; \phi_2]\!]_{\rho^d}(\mathscr{A}) \subseteq [\![\phi_1 ; \phi_2]\!]_\rho(\mathscr{A})$ according to Lemma 4(3) because $\rho^d \subseteq \rho$ from Definition 6, so $[\![\phi_1 ; \phi_2]\!]_{\rho^d}(\mathscr{A}) \subseteq f(\mathscr{A})$ since $[\![\phi_1 ; \phi_2]\!]_\rho \subseteq_{\mathscr{C}_{\approx^*}} f$. Hence, $[\![\phi_1 ; \phi_2]\!]_{\rho^d} \subseteq_{\mathscr{C}_{\approx^*}} f^d$.

(3) The proof of this part is similar to the proof of (2).

— $\phi = \mu X.\phi_1$

Assume $g = \sqcap\{f' \in \mathrm{MPT_T} \mid [\![\phi_1]\!]_{\rho[X \rightsquigarrow f']} \subseteq f'\}$.

(1) Since $[\![\phi_1]\!]_{\rho[X \rightsquigarrow g]} \subseteq g$, by induction on (2), we have $[\![\phi_1]\!]_{(\rho[X \rightsquigarrow g])^d} \subseteq_{\mathscr{C}_{\approx^*}} g^d$. On the other hand, it is easy to see that $(\rho[X \rightsquigarrow g])^d =_{\mathscr{C}_{\approx^*}} \rho[X \rightsquigarrow g^d]$ by Definition 6, so $[\![\phi_1]\!]_{\rho[X \rightsquigarrow g^d]} \subseteq_{\mathscr{C}_{\approx^*}} g^d$ by the induction hypothesis. Let g^* be defined as

$$g^*(\mathscr{A}) = \begin{cases} g^d(\mathscr{A}) & \text{if } \mathscr{A} \in \mathscr{C}_{\approx^*}; \\ g(\mathscr{A}) & \text{otherwise.} \end{cases}$$

Applying the induction hypothesis again, it is not hard to show $[\![\phi_1]\!]_{\rho[X \rightsquigarrow g^*]} \subseteq g^*$. So $g = g^*$ by the assumption and Lemma 6(3), hence $[\![\phi]\!]_\rho$ preserves $\mathscr{C}_{\approx^*}$.

(2) By the induction hypothesis for (2), we have $[\![\phi_1]\!]_{\rho^d[X \rightsquigarrow g^d]} \subseteq_{\mathscr{C}_{\approx^*}} g^d$. On the other hand, it is easy to show that $g^d \subseteq_{\mathscr{C}_{\approx^*}} f^d$ using Lemma 6(4), as $[\![\mu X.\phi_1]\!]_\rho = [\![\phi_1]\!]_{\rho[X \rightsquigarrow g]} = g \subseteq f$.

(3) The proof of this part is similar. □

Applying Lemma 7, we can show that FLC$^+$ with respect to $\approx^*$ has the tree model property, that is, we have the following theorem.

Theorem 3. Given $P, Q \in \mathrm{BPA}_\delta^{\epsilon,\Omega}$, if $P \approx^* Q$, then for any closed formula ϕ of wFLC$^+$, we have $P \models \phi$ if and only if $Q \models \phi$.

Proof. For any closed ϕ of wFLC$^+$, by Lemma 7, we have that $[\![\phi]\!]$ preserves $\mathscr{C}_{\approx^*}$, so $[\![\phi]\!](\mathrm{BPA}_\delta^{\epsilon,\Omega})$ is closed with respect to $\approx^*$. Thus, $P \in [\![\phi]\!](\mathrm{BPA}_\delta^{\epsilon,\Omega})$ if and only if $Q \in [\![\phi]\!](\mathrm{BPA}_\delta^{\epsilon,\Omega})$ since $P \approx^* Q$. That is, $P \models \phi$ if and only if $Q \models \phi$. □

In order to facilitate proofs by induction on formulae, we need to define a well-founded order on the formulae of FLC$^+$, which we will denote by $<$. To this end, we first define a partial order, denoted by $\prec$, on $\mathrm{FLC}^{+} \times \mathrm{FLC}^{+}$ as follows: $(\phi_1, \phi_2) \prec (\psi_1, \psi_2)$ if and only if $\phi_1 ; \phi_2 \Leftrightarrow \psi_1 ; \psi_2$ and ϕ_1 is a proper subformula of ψ_1. In other words, we assume that the left association of ; has higher precedence. For example, $(\langle a \rangle, \langle b \rangle ; \langle c \rangle) \prec (\langle a \rangle ; \langle b \rangle, \langle c \rangle)$. Then, we say $\phi < \psi$ if and only if either ϕ is a proper subformula of ψ, or $\phi \prec \psi$. It is easy to see that $<$ is well-founded.

3.2. *Defining '+' in FLC with respect to $\approx^*$*

Proving the definability of '+' in FLC with respect to $\approx^*$ is achieved through the following three steps:

(1) We show that in some special cases '+' can be defined essentially by conjunction and disjunction.

(2) We prove that the elimination of '+' in a strictly guarded formula ϕ of FLC^{+} with respect to $\approx^*$ can be reduced to one of the above special cases.

(3) Finally, to complete the proof, we show that for any $\phi \in \mathscr{L}_{\mathrm{FLC}^{+}}$ there exists a strictly guarded formula $\phi' \in \mathscr{L}_{\mathrm{FLC}^{+}}$ such that $\phi \Leftrightarrow \phi'$.

For the first step, we need the following fact.

Fact 1.

(1) For any $P, Q \in \mathrm{BPA}_{\delta}^{\epsilon,\Omega}$ and any valuation ρ, if $P \models_\rho \langle\!\langle \alpha \rangle\!\rangle ; \phi$, then $P + Q \models_\rho \langle\!\langle \alpha \rangle\!\rangle ; \phi$.

(2) If $P \models_\rho \llbracket \alpha \rrbracket ; \phi_1$ and $Q \models_\rho \llbracket \alpha \rrbracket ; \phi_2$, then $P + Q \models_\rho \llbracket \alpha \rrbracket ; (\phi_1 \vee \phi_2)$.

The following lemma claims that in some special cases, '+' can be defined essentially by conjunction and disjunction.

Lemma 8. Let $\{\alpha_1, \cdots, \alpha_n\}$ and $\{\kappa_1, \cdots, \kappa_k\}$ be subsets of $\{\beta_1, \cdots, \beta_m\}$, where $\beta_i \neq \beta_j$ if $i \neq j$ and $n, k \leqslant m$. Assume $\langle \alpha_1, \cdots, \alpha_n \rangle = \langle \beta_1, \cdots, \beta_n \rangle$ and $\langle \kappa_1, \cdots, \kappa_k \rangle = \langle \beta_{l_1}, \cdots, \beta_{l_k} \rangle$, where $l_j \in \{1, \cdots, m\}$ for $j = 1 \cdots k$. Then

$$\left(\bigwedge_{i=1}^{n} \bigwedge_{j=1}^{n_i} \langle\!\langle \alpha_i \rangle\!\rangle ; \phi_{i,j} \wedge \bigwedge_{i=1}^{m} \llbracket \beta_i \rrbracket ; \psi_i \wedge q_1 \right) + \left(\bigwedge_{i=1}^{k} \bigwedge_{j=1}^{k_i} \langle\!\langle \kappa_i \rangle\!\rangle ; \varphi_{i,j} \wedge \bigwedge_{i=1}^{m} \llbracket \beta_i \rrbracket ; \chi_i \wedge q_2 \right)$$

$$\Leftrightarrow \bigwedge_{i=1}^{n} \bigwedge_{j=1}^{n_i} \langle\!\langle \alpha_i \rangle\!\rangle ; (\phi_{i,j} \wedge \psi_i) \wedge \bigwedge_{i=1}^{k} \bigwedge_{j=1}^{k_i} \langle\!\langle \kappa_i \rangle\!\rangle ; (\varphi_{i,j} \wedge \chi_{l_i}) \wedge \bigwedge_{i=1}^{m} \llbracket \beta_i \rrbracket ; (\psi_i \vee \chi_i) \wedge q_1 \wedge q_2$$

where $q_1 \Leftrightarrow tt$ or $q_1 \Leftrightarrow \tau$, and $q_2 \Leftrightarrow tt$ or $q_2 \Leftrightarrow \tau$.

Proof.

($\Rightarrow$) Suppose

$$P \models_\rho \left(\bigwedge_{i=1}^{n} \bigwedge_{j=1}^{n_i} \langle\!\langle \alpha_i \rangle\!\rangle ; \phi_{i,j} \wedge \bigwedge_{i=1}^{m} \llbracket \beta_i \rrbracket ; \psi_i \wedge q_1 \right) + \left(\bigwedge_{i=1}^{k} \bigwedge_{j=1}^{k_i} \langle\!\langle \kappa_i \rangle\!\rangle ; \varphi_{i,j} \wedge \bigwedge_{i=1}^{m} \llbracket \beta_i \rrbracket ; \chi_i \wedge q_2 \right),$$

where ρ is a valuation. By the semantics of FLC$^+$ with respect to $\approx^*$, there exist P_1 and P_2 such that

$$P \approx^* P_1 + P_2, \tag{2}$$

$$P_1 \models_\rho \left(\bigwedge_{i=1}^{n} \bigwedge_{j=1}^{n_i} \langle\!\langle \alpha_i \rangle\!\rangle ; \phi_{i,j} \wedge \bigwedge_{i=1}^{m} \llbracket \beta_i \rrbracket ; \psi_i \right), \tag{3}$$

$$P_2 \models_\rho \left(\bigwedge_{i=1}^{k} \bigwedge_{j=1}^{k_i} \langle\!\langle \kappa_i \rangle\!\rangle ; \varphi_{i,j} \wedge \bigwedge_{i=1}^{m} \llbracket \beta_i \rrbracket ; \chi_i \right). \tag{4}$$

This implies

$$P_1 \models_\rho \bigwedge_{i=1}^{n} \bigwedge_{j=1}^{n_i} \langle\!\langle \alpha_i \rangle\!\rangle ; (\phi_{i,j} \wedge \psi_i) \tag{5}$$

by (3) and DB. Similarly, by (4) and DB, we have

$$P_2 \models_\rho \bigwedge_{i=1}^{k} \bigwedge_{j=1}^{k_i} \langle\!\langle \kappa_i \rangle\!\rangle ; (\varphi_{i,j} \wedge \chi_{l_i}). \tag{6}$$

By (5), (6) and Fact 1(1), it follows that

$$P_1 + P_2 \models \bigwedge_{i=1}^{n} \bigwedge_{j=1}^{n_i} \langle\!\langle \alpha_i \rangle\!\rangle ; (\phi_{i,j} \wedge \psi_i) \wedge \bigwedge_{i=1}^{k} \bigwedge_{j=1}^{k_i} \langle\!\langle \kappa_i \rangle\!\rangle ; (\varphi_{i,j} \wedge \chi_{l_i}). \tag{7}$$

Moreover, it can be shown that

$$P_1 + P_2 \models \bigwedge_{i=1}^{m} \llbracket \beta_i \rrbracket ; (\psi_i \vee \chi_i) \tag{8}$$

from (3), (4) and Fact 1(2). Thus, from (7), (8) and Theorem 3, we have

$$P \models_\rho \bigwedge_{i=1}^{n} \bigwedge_{j=1}^{n_i} \langle \alpha_i \rangle ; (\phi_{i,j} \wedge \psi_i) \wedge \bigwedge_{i=1}^{k} \bigwedge_{j=1}^{k_i} \langle \kappa_i \rangle ; (\varphi_{i,j} \wedge \chi_{l_i}) \wedge \bigwedge_{i=1}^{m} [\beta_i](\psi_i \vee \chi_i) \wedge q_1 \wedge q_2.$$

($\Leftarrow$) Assume

$$\begin{aligned} P \models_\rho & \bigwedge_{i=1}^{n} \bigwedge_{j=1}^{n_i} \langle\!\langle \alpha_i \rangle\!\rangle ; (\phi_{i,j} \wedge \psi_i) \wedge \\ & \bigwedge_{i=1}^{k} \bigwedge_{j=1}^{k_i} \langle\!\langle \kappa_i \rangle\!\rangle ; (\varphi_{i,j} \wedge \chi_{l_i}) \wedge \\ & \bigwedge_{i=1}^{m} \llbracket \beta_i \rrbracket ; (\psi_i \vee \chi_i) \wedge q_1 \wedge q_2, \end{aligned} \tag{9}$$

where ρ is a valuation. It is easy to prove that $P \approx^* \Sigma_{i=1}^{l} \Sigma_{j=1}^{i_{\alpha_i}} (\tau)^{n_{j,1}} ; \alpha_i ; (\tau)^{n_{j,2}} ; P_{i,j}$, where: $n_{j,1}, n_{j,2} \in \mathbb{N}$; τ^n stands for $\overbrace{\tau ; \ldots ; \tau}^{n}$ with $\tau^n = \varepsilon$ if $n = 0$; $l \geqslant m$; and for any $1 \leqslant i, j \leqslant l$, if $i \neq j$, then $\alpha_i \neq \alpha_j$. So we have

$$\Sigma_{i=1}^{l}\Sigma_{j=1}^{i_{\alpha_i}}(\tau)^{n_{j,1}};\alpha_i;(\tau)^{n_{j,2}};P_{i,j} \models_\rho \bigwedge_{i=1}^{n}\bigwedge_{j=1}^{n_i}\langle\!\langle\alpha_i\rangle\!\rangle;(\phi_{i,j}\wedge\psi_i) \tag{10}$$

by Theorem 3. This implies that for each $1 \leqslant i \leqslant n$ and $1 \leqslant j \leqslant n_i$, there exist $1 \leqslant r_i \leqslant l$ and $1 \leqslant h_j \leqslant i_{\alpha_{r_i}}$ such that $\alpha_{r_i} = \alpha_i$ and $P_{r_i,h_j} \models_\rho \phi_{i,j} \wedge \psi_i$. Let

$$P' \mathrel{\widehat{=}} \Sigma_{i=1}^{n}\Sigma_{j=1}^{n_i}(\tau)^{n_{j,1}};\alpha_{r_i};(\tau)^{n_{j,2}};P_{r_i,h_j}.$$

It is obvious that

$$P' \models_\rho \bigwedge_{i=1}^{n}\bigwedge_{j=1}^{n_i}\langle\!\langle\alpha_i\rangle\!\rangle\phi_{i,j} \wedge \bigwedge_{i=1}^{m}[\![\beta_i]\!]\psi_i \wedge q_1. \tag{11}$$

Similarly, we get that for each $1 \leqslant i \leqslant k$ and $1 \leqslant j \leqslant k_i$, there exist $1 \leqslant r_i \leqslant l$ and $1 \leqslant h_j \leqslant i_{\alpha_{r_i}}$ such that $\alpha_{r_i} = \kappa_i$ and $P_{r_i,h_j} \models \varphi_{i,j} \wedge \chi_i$. Let

$$P'' \mathrel{\widehat{=}} \Sigma_{i=1}^{k}\Sigma_{j=1}^{n_i}(\tau)^{n_{j,1}};\alpha_{r_i};(\tau)^{n_{j,2}};P_{r_i,h_j}.$$

It is easy to show that

$$P'' \models_\rho \bigwedge_{i=1}^{k}\bigwedge_{j=1}^{k_i}\langle\!\langle\kappa_i\rangle\!\rangle;\varphi_{i,j} \wedge \bigwedge_{i=1}^{m}[\![\beta_i]\!];\chi_i \wedge q_2. \tag{12}$$

Then we partition $\Sigma_{i=1}^{l}\Sigma_{j=1}^{i_{\alpha_i}}(\tau)^{n_{j,1}};\alpha_i;(\tau)^{n_{j,2}};P_{i,j}$ into two parts P' and P'' by the following algorithm. For all $1 \leqslant i \leqslant l$, we perform the following steps:

(1) If $\alpha_i = \beta_j$ for some $j \in \{1, \cdots, m\}$, let

$$I_1 \mathrel{\widehat{=}} \{h \mid P_{i,h} \models \psi_j\}$$

and

$$I_2 \mathrel{\widehat{=}} \{h \mid P_{i,h} \models \chi_j\}.$$

Since

$$P \models [\![\beta_j]\!];(\psi_j \vee \chi_j),$$

it is clear that $I_1 \cup I_2 = \{1, \cdots, i_{\alpha_i}\}$.
Otherwise, let $I_1 \widehat{=} \{1, \cdots, i_{\alpha_i}\}$ and $I_2 = \varnothing$.

(2) Let

$$P' := P' + \sum_{h \in I_1}(\tau)^{n_{j,1}};\alpha_i;(\tau)^{n_{j,2}};P_{i,h}$$

and

$$P'' := P'' + \sum_{h \in I_2}(\tau)^{n_{j,1}};\alpha_i;(\tau)^{n_{j,2}};P_{i,h}.$$

Because for all $1 \leqslant i, j \leqslant m$, if $i \neq j$, we have $\beta_i \neq \beta_j$, it is easy to show that (11) and (12) remain invariant during the partitioning.

In addition, it is easy to see that $P' + P'' \approx^* P$. Therefore, from Theorem 3,

$$P \models_\rho \left(\bigwedge_{i=1}^{n} \bigwedge_{j=1}^{n_i} \langle\!\langle \alpha_i \rangle\!\rangle ; \phi_{i,j} \wedge \bigwedge_{i=1}^{m} [\![\beta_i]\!] ; \chi_i \wedge q_1\right) + \left(\bigwedge_{i=1}^{k} \bigwedge_{j=1}^{k_i} \langle\!\langle \kappa_i \rangle\!\rangle ; \varphi_{i,j} \wedge \bigwedge_{i=1}^{m} [\![\beta_i]\!] ; \chi_i \wedge q_2\right).$$

□

The following corollary follows immediately from Lemma 8.

Corollary 1.

(1) $[\![\alpha]\!] ; \phi_1 + [\![\alpha]\!] ; \phi_2 \Leftrightarrow [\![\alpha]\!] ; (\phi_1 \vee \phi_2)$.
(2) $[\![\alpha]\!] ; \phi_1 + [\![\beta]\!] ; \phi_2 \Leftrightarrow tt$.
(3) $\langle\!\langle \alpha \rangle\!\rangle ; \phi_1 + \langle\!\langle \beta \rangle\!\rangle ; \phi_2 \Leftrightarrow \langle\!\langle \alpha \rangle\!\rangle ; \phi_1 \wedge \langle\!\langle \beta \rangle\!\rangle ; \phi_2$.
(4) $(\langle\!\langle \alpha \rangle\!\rangle ; \phi_1 \wedge [\![\alpha]\!] ; \phi_2) + tt \Leftrightarrow \langle\!\langle \alpha \rangle\!\rangle ; (\phi_1 \wedge \phi_2)$.
(5) $\langle\!\langle \alpha \rangle\!\rangle ; \phi_1 + [\![\alpha]\!] ; \phi_2 \Leftrightarrow \langle\!\langle \alpha \rangle\!\rangle ; \phi_1$.
(6) $\langle\!\langle \alpha \rangle\!\rangle ; \phi_1 + [\![\beta]\!] \phi_2 \Leftrightarrow \langle\!\langle \alpha \rangle\!\rangle \phi_1$.

We can now complete the second step by proving the following lemma.

Lemma 9. For any ϕ of FLC$^+$, if ϕ is strictly guarded, there exists ϕ' in which no $+$ occurs such that $\phi' \Leftrightarrow \phi$ and ϕ' is also strictly guarded.

Proof. The proof proceeds by induction on the structure of ϕ – we will only give the interesting case of $\phi = \phi_1 + \phi_2$.

Let $\phi = \phi_1 + \phi_2$. Since ϕ is strictly guarded, so are ϕ_1 and ϕ_2. By the induction hypothesis, there exist ϕ_i' such that ϕ_i' is strictly guarded, $\phi_i' \Leftrightarrow \phi_i$ and no $+$ occurs in ϕ_i' for $i = 1, 2$. Using the laws of boolean algebra and Lemma 2, we can transfer ϕ_1' and ϕ_2' equivalently as follows:

$$\phi_1' \Leftrightarrow \bigvee_{i=1}^{m_1} \left(\bigwedge_{j=1}^{m_{1,i}} \bigwedge_{h=1}^{m_{1,i,j}} \langle\!\langle \alpha_{1,i,j} \rangle\!\rangle ; \phi_{1,i,j,h} \wedge \bigwedge_{j=1}^{m'_{1,i}} [\![\beta_{1,i,j}]\!] ; \psi_{1,i,j} \wedge q_{1,i} \right) \tag{13}$$

$$\phi_2' \Leftrightarrow \bigvee_{i=1}^{m_2} \left(\bigwedge_{j=1}^{m_{2,i}} \bigwedge_{h=1}^{m_{2,i,j}} \langle\!\langle \alpha_{2,i,j} \rangle\!\rangle ; \phi_{2,i,j,h} \wedge \bigwedge_{j=1}^{m'_{2,i}} [\![\beta_{2,i,j}]\!] ; \psi_{2,i,j} \wedge q_{2,i} \right), \tag{14}$$

where $q_{i,j} \in \{tt, \surd, \tau\}$ for $i = 1, 2$ and $j = 1, \cdots, m_i$, and

$$\begin{aligned} \forall 1 \leqslant i \leqslant 2, \forall 1 \leqslant j \leqslant m_i . (&\forall 1 \leqslant k_1, k_2 \leqslant m_{i,j} . k_1 \neq k_2 \Rightarrow \alpha_{i,j,k_1} \neq \alpha_{i,j,k_2} \wedge \\ &\forall 1 \leqslant k_1, k_2 \leqslant m'_{i,j} . k_1 \neq k_2 \Rightarrow \beta_{i,j,k_1} \neq \beta_{i,j,k_2} \wedge \\ &\forall 1 \leqslant k_1 \leqslant m_{i,j} . \alpha_{i,j,k_1} = \beta_{i,j,k_1}). \end{aligned}$$

By S1, S2, SD and SC, we have

$$\begin{aligned} \phi_1' + \phi_2' \Leftrightarrow \bigvee_{i_1=1}^{m_1} \bigvee_{i_2=1}^{m_2} \Bigg[&\left(\bigwedge_{j=1}^{m_{1,i_1}} \bigwedge_{h=1}^{m_{1,i_1,j}} \langle\!\langle \alpha_{1,i_1,j} \rangle\!\rangle ; \phi_{1,i_1,j,h} \wedge \bigwedge_{j=1}^{m'_{1,i_1}} [\![\beta_{1,i_1,j}]\!] ; \psi_{1,i_1,j} \wedge q_{1,i_1} \right) \\ &+ \left(\bigwedge_{j=1}^{m_{2,i_2}} \bigwedge_{h=1}^{m_{2,i_2,j}} \langle\!\langle \alpha_{2,i_2,j} \rangle\!\rangle ; \phi_{2,i_2,j,h} \wedge \bigwedge_{j=1}^{m'_{2,i_2}} [\![\beta_{2,i_2,j}]\!] ; \psi_{2,i_2,j} \wedge q_{2,i_2} \right) \Bigg] \end{aligned} \tag{15}$$

In the following, for any $1 \leqslant i_1 \leqslant m_1$, $1 \leqslant i_2 \leqslant m_2$, we consider the corresponding disjunct from the following three cases:

(1) $q_{1,i_1} \neq \surd\!\!\surd$ and $q_{2,i_2} \neq \surd\!\!\surd$.
Thus, applying Lemma 2 and Lemma 8, there is a formula φ_{i_1,i_2} in which no $+$ occurs such that

$$\varphi_{i_1,i_2} \Leftrightarrow \left(\bigwedge_{j=1}^{m_{1,i_1}} \bigwedge_{h=1}^{m_{1,i_1,j}} \langle\!\langle \alpha_{1,i_1,j} \rangle\!\rangle ; \phi_{1,i_1,j,h} \wedge \bigwedge_{j=1}^{m'_{1,i_1}} [\![\beta_{1,i_1,j}]\!] ; \psi_{1,i_1,j} \wedge q_{1,i_1}\right)$$
$$+ \left(\bigwedge_{j=1}^{m_{2,i_2}} \bigwedge_{h=1}^{m_{2,i_2,j}} \langle\!\langle \alpha_{2,i_2,j} \rangle\!\rangle ; \phi_{2,i_2,j,h} \wedge \bigwedge_{j=1}^{m'_{2,i_2}} [\![\beta_{2,i_2,j}]\!] ; \psi_{2,i_2,j} \wedge q_{2,i_2}\right).$$

(2) $q_{1,i_1} = \surd\!\!\surd$.
Let

$$Cond_1 = (m_{1,i_1} \neq 0 \wedge \exists j \in \{1, \cdots, m_{1,i_1}\}.m_{1,i_1,j} \neq 0) \vee m'_{1,i_1} \neq 0$$
$$Cond_2 = (m_{2,i_2} \neq 0 \wedge \exists j \in \{1, \cdots, m_{2,i_2}\}.m_{2,i_2,j} \neq 0) \vee m'_{2,i_2} \neq 0$$

Thus, we consider the following three subcases:

(2.1) $Cond_1$ holds.
So let $\varphi_{i_1,i_2} \widehat{=} ff$. By T1 and P2, it follows that φ_{i_1,i_2} is equivalent to the disjunct;

(2.2) $\neg Cond_1 \wedge Cond_2$ holds.
So let $\varphi_{i_1,i_2} \widehat{=} ff$. By T2 and P2, it is easy to see that φ_{i_1,i_2} is equivalent to the disjunct;

(2.3) $\neg Cond_1 \wedge \neg Cond_2$ holds.
For this subcase, we need to consider the following three subsubcases:

(2.3.1) $q_{2,i_2} = \surd\!\!\surd$.
So let $\varphi_{i_1,i_2} \widehat{=} \surd\!\!\surd$. Using P3, it is easy to see φ_{i_1,i_2} is equivalent to the disjunct.

(2.3.2) $q_{2,i_2} = ff$.
So let $\varphi_{i_1,i_2} \widehat{=} ff$. Using P2, it follows that φ_{i_1,i_2} is equivalent to the disjunct.

(2.3.3) $q_{2,i_2} = tt$.
So let $\varphi_{i_1,i_2} \widehat{=} \surd\!\!\surd$. Using T4, it follows that φ_{i_1,i_2} is equivalent to the disjunct.

(3) $q_{2,i_2} = \surd\!\!\surd$.
This is similar to the above case, and we can find a φ_{i_1,i_2} in which no $+$ occurs such that φ_{i_1,i_2} is equivalent to the disjunct.

So let $\phi' \widehat{=} \bigvee_{i=1}^{m_1} \bigvee_{j=1}^{m_2} \varphi_{i,j}$. By Definition 4, it is easy to see that ϕ' is strictly guarded, no $+$ occurs in ϕ' and $\phi \Leftrightarrow \phi'$. □

In the following, we will apply some rewriting techniques to prove that for any closed and guarded formula ϕ of FLC$^+$, there exists ϕ' that is strictly guarded such that $\phi \Leftrightarrow \phi'$.

Lemma 10. For any $\phi \in \mathscr{L}_{\text{FLC}^+}$, there is $\phi' \in \mathscr{L}_{\text{FLC}^+}$ that is strictly guarded such that $\phi \Leftrightarrow \phi'$.

Proof. In order to prove the lemma, we need to show the following equations:

$$\mu X.\phi_1[@;\phi_2[(X \odot \phi_3) + \phi_4]] \Leftrightarrow \mu X.\phi_1[@;\phi_2[\mu Y.(\phi_1[@;\phi_2[Y]] \odot \phi_3) + \phi_4]] \quad (16)$$

$$\nu X.\phi_1[@;\phi_2[(X \odot \phi_3) + \phi_4]] \Leftrightarrow \nu X.\phi_1[@;\phi_2[\nu Y.(\phi_1[@;\phi_2[Y]] \odot \phi_3) + \phi_4]] \quad (17)$$

$$\mu X.\phi_1[@;\phi_2[(X;\phi_3 \odot \phi_4) + \phi_5]] \Leftrightarrow \mu X.\phi_1[@;\phi_2[\mu Y.(\phi_1[@;\phi_2[Y]];\phi_3 \odot \phi_4) + \phi_5]] \quad (18)$$

$$\nu X.\phi_1[@;\phi_2[(X;\phi_3 \odot \phi_4) + \phi_5]] \Leftrightarrow \nu X.\phi_1[@;\phi_2[\nu Y.(\phi_1[@;\phi_2[Y]];\phi_3 \odot \phi_4) + \phi_5]] \quad (19)$$

where $\odot \in \{\wedge, \vee\}$, $\phi_i[\ ]$ stands for a formula with the hole $[\ ]$, and the formula on the left-hand side of each equation is guarded.

We will only prove (18) as an example, the others can be proved similarly. Since

$$\phi_1[@;\phi_2[(X;\phi_3 \odot \phi_4) + \phi_5]]$$

is guarded, by the Tarski–Knaster fixed point theorem (Tarski 1955), it is clear that

$$\mu X.\phi_1[@;\phi_2[(X;\phi_3 \odot \phi_4) + \phi_5]]$$

is the unique least solution of the equation

$$X = \phi_1[@;\phi_2[(X;\phi_3 \odot \phi_4) + \phi_5]]. \quad (20)$$

Let Y be a fresh variable and $Y = (X;\phi_3 \odot \phi_4) + \phi_5$. It is easy to see the least solution of (20) is equivalent to the X-component of the least solution of the following equation system:

$$X = \phi_1[@;\phi_2[(X;\phi_3 \odot \phi_4) + \phi_5]]$$
$$Y = (X;\phi_3 \odot \phi_4) + \phi_5.$$

Then, by exploiting some rewriting techniques, it is easy to transform the problem of finding the least solution of the above equation system into the equivalent problem of finding the least solution of

$$X = \phi_1[@;\phi_2[(X;\phi_3 \odot \phi_4) + \phi_5]]$$
$$Y = (\phi_1[@;\phi_2[Y]];\phi_3 \odot \phi_4) + \phi_5.$$

It is not hard to show the least solution of this equation system is

$$(\mu X.\phi_1[@;\phi_2[\mu Y.(\phi_1[@;\phi_2[Y]];\phi_3 \odot \phi_4) + \phi_5]], \mu Y.(\phi_1[@;\phi_2[Y]];\phi_3 \odot \phi_4) + \phi_5).$$

Therefore, (18) follows.

By repeatedly applying (16)–(19), we can rewrite any given formula $\phi \in \mathscr{L}_{\mathrm{FLC}^+}$ to ϕ', which is strictly guarded such that $\phi \Leftrightarrow \phi'$. □

Remark 1. In the proof of Lemma 10, we only considered the cases where a variable is guarded by a modality @, and ignored the cases where a variable is guarded by a propositional letter p because, from Definition 3, it is easy to show that $p;\phi \Leftrightarrow p$.

From Lemmas 10 and 9, we can get the following theorem.

Theorem 4. $\forall \phi \in \mathscr{L}_{\mathrm{FLC}^+}, \exists \phi' \in \mathscr{L}_{\mathrm{FLC}}. \phi \Leftrightarrow \phi'$.

We use the following example to demonstrate how to translate a closed and guarded formula ϕ of FLC$^+$ into a formula ϕ' of FLC by applying the above procedure.

Example 2. Let $\phi = \mu X.\nu Y.\langle\!\langle\alpha\rangle\!\rangle; (X + Y); X; Y; \langle\!\langle\beta\rangle\!\rangle \vee \langle\!\langle\kappa\rangle\!\rangle$. Applying (16), we have

$$\phi \Leftrightarrow \mu X.\nu Y.\langle\!\langle a\rangle\!\rangle; [\mu Z.(\nu V.\langle\!\langle\alpha\rangle\!\rangle; Z; X; V; \langle\!\langle\beta\rangle\!\rangle \vee \langle\!\langle\kappa\rangle\!\rangle) + Y]; X; Y; \langle\!\langle\beta\rangle\!\rangle \vee \langle\!\langle\kappa\rangle\!\rangle \ \ \widehat{=} \ \ \phi'$$

where

$$\begin{aligned} \phi_1[\,] &\mathrel{\widehat{=}} \nu Y.[\,]; X; Y; \langle\!\langle\beta\rangle\!\rangle \vee \langle\!\langle\kappa\rangle\!\rangle \\ \phi_2[\,] &\mathrel{\widehat{=}} [\,] \\ \phi_3 &\mathrel{\widehat{=}} \begin{cases} tt \text{ if } \odot = \wedge \\ ff \text{ o.w.} \end{cases} \\ \phi_4 &\mathrel{\widehat{=}} Y. \end{aligned}$$

Furthermore, applying (17), we can get

$$\begin{aligned} \phi' \Leftrightarrow\ & \mu X.\nu Y.\langle\!\langle\alpha\rangle\!\rangle; [\mu Z.\nu W.(\langle\!\langle\alpha\rangle\!\rangle; W; X; Y; \langle\!\langle\beta\rangle\!\rangle \vee \langle\!\langle\kappa\rangle\!\rangle) \\ & + (\nu V.\langle\!\langle\alpha\rangle\!\rangle; Z; X; V; \langle\!\langle\beta\rangle\!\rangle \vee \langle\!\langle\kappa\rangle\!\rangle)]; X; Y; \langle\!\langle\beta\rangle\!\rangle \vee \langle\!\langle\kappa\rangle\!\rangle \\ \widehat{=}\ & \phi'' \end{aligned}$$

where

$$\begin{aligned} \phi_1[\,] &\mathrel{\widehat{=}} [\,]; X; Y; \langle\!\langle\beta\rangle\!\rangle \vee \langle\!\langle\kappa\rangle\!\rangle \\ \phi_2[\,] &\mathrel{\widehat{=}} \mu Z.[\,] \\ \phi_3 &\mathrel{\widehat{=}} \begin{cases} tt & \text{if } \odot = \wedge \\ ff & \text{otherwise} \end{cases} \\ \phi_4 &\mathrel{\widehat{=}} \nu V.\langle\!\langle\alpha\rangle\!\rangle; Z; X; V; \langle\!\langle\beta\rangle\!\rangle \vee \langle\!\langle\kappa\rangle\!\rangle. \end{aligned}$$

Thus, using Lemma 9, we can eliminate '+' in ϕ'' as follows:

$$\begin{aligned} \phi'' &\Leftrightarrow \mu X.\nu Y.\langle\!\langle\alpha\rangle\!\rangle; \left[\mu Z.\nu W. \begin{pmatrix} (\langle\!\langle\alpha\rangle\!\rangle; W; X; Y; \langle\!\langle\beta\rangle\!\rangle + \langle\!\langle\kappa\rangle\!\rangle) \vee \\ (\langle\!\langle\alpha\rangle\!\rangle; W; X; Y; \langle\!\langle\beta\rangle\!\rangle + \\ \nu V.\langle\!\langle\alpha\rangle\!\rangle; Z; X; V; \langle\!\langle\beta\rangle\!\rangle) \vee \\ (\nu V.\langle\!\langle\alpha\rangle\!\rangle; Z; X; V; \langle\!\langle\beta\rangle\!\rangle + \langle\!\langle\kappa\rangle\!\rangle) \vee \\ (\langle\!\langle\kappa\rangle\!\rangle + \langle\!\langle\kappa\rangle\!\rangle) \end{pmatrix} \right]; X; Y; \langle\!\langle\beta\rangle\!\rangle \vee \langle\!\langle\kappa\rangle\!\rangle \\ &\Leftrightarrow \mu X.\nu Y.\langle\!\langle\alpha\rangle\!\rangle; [\mu Z.\nu W. \begin{pmatrix} ((\langle\!\langle\alpha\rangle\!\rangle; W; X; Y; \langle\!\langle\beta\rangle\!\rangle \wedge \langle\!\langle\kappa\rangle\!\rangle) \vee \\ (\langle\!\langle\alpha\rangle\!\rangle; W; X; Y; \langle\!\langle\beta\rangle\!\rangle \wedge \\ \nu V.\langle\!\langle\alpha\rangle\!\rangle; Z; X; V; \langle\!\langle\beta\rangle\!\rangle) \vee \\ (\nu V.\langle\!\langle\alpha\rangle\!\rangle; Z; X; V; \langle\!\langle\beta\rangle\!\rangle \wedge \langle\!\langle\kappa\rangle\!\rangle) \vee \\ \langle\!\langle\kappa\rangle\!\rangle \end{pmatrix}; X; Y; \langle\!\langle\beta\rangle\!\rangle \vee \langle\!\langle\kappa\rangle\!\rangle \\ &\mathrel{\widehat{=}} \phi^*. \end{aligned}$$

It is easy to see that $\phi \Leftrightarrow \phi^*$ and no $+$ occurs in ϕ^*.

In the following, we will use *en*(ϕ) to denote the formula resulting from an application of the above procedure to ϕ in which $+$ is eliminated.

4. Connection between $\mathrm{BPA}_{\delta}^{\epsilon,\Omega}$ and FLC^{+} with respect to $\approx^{*}$

In this section, we discuss how to relate the primitives of $\mathrm{BPA}_{\delta}^{\epsilon,\Omega}$ to the connectives of FLC^{+}.

4.1. *Non-determinism*

It is clear that the '+' of $\mathrm{BPA}_{\delta}^{\epsilon,\Omega}$ corresponds to the '+' of FLC^{+}. The connection can be expressed as follows.

Proposition 1.

(i) For any $P, Q \in \mathrm{BPA}_{\delta}^{\epsilon,\Omega}$, if $P \models \phi$ and $Q \models \psi$, then $P + Q \models \phi + \psi$.

(ii) For any $R \in \mathrm{BPA}_{\delta}^{\epsilon,\Omega}$, if $R \models \phi + \psi$, then there exist $P, Q \in \mathrm{BPA}_{\delta}^{\epsilon,\Omega}$ such that $R \approx^{*} P + Q$, $P \models \phi$ and $Q \models \psi$.

4.2. *Sequential composition*

Normally, although $P \models \phi$ and $Q \models \psi$, we have $P;Q \not\models \phi;\psi$ because ϕ may only describe some partial executions of P. For example, let $P = a;\tau;b$, $Q = c;\tau;d$. It is obvious that $P \models \langle\!\langle a\rangle\!\rangle$ and $Q \models \langle\!\langle c\rangle\!\rangle$, but $P;Q \not\models \langle\!\langle a\rangle\!\rangle;\langle\!\langle c\rangle\!\rangle$. Therefore, we require that ϕ specify the full executions of P. This is similar to the premise of the rule Seq-2 that in the process $P;Q$, only after the first segment P has finished its execution, can Q start to run.

Note that a full execution of a process P here means one of its runs, not a trace of the process. For example,

$$\underbrace{aaaa\cdots}_{\text{infinitely many}}$$

is a full execution of the process $recx.a;x$, but a^{n} for any $n \in \mathbb{N}$ is not. Hence, $\nu X.\langle\!\langle a\rangle\!\rangle;X$ specifies the full executions of $recx.a;x$, but $\mu X.[\![a]\!];X$ does not, because $\nu X.\langle\!\langle a\rangle\!\rangle;X$ expresses the fact there is at least one infinite a-run, while $\mu X.[\![a]\!];X$ says that all a-runs are finite. Thus $recx.a;x \models (\nu X.\langle\!\langle a\rangle\!\rangle;X);\surd\!\!\!\surd$, but $recx.a;x \not\models (\mu X.[\![a]\!];X);\surd\!\!\!\surd$.

Another issue is that by the definition of the semantics of $\mathscr{P}^{*}$, we have $nil;P \approx^{*} P$. Therefore, the properties of intermediate terminations should be omitted in the resulting formula, since otherwise the resulting property does not hold in the combined system. For example, let $P = a;\tau;nil$ and $Q = b;\tau;\delta$, $\phi = \langle\!\langle a\rangle\!\rangle;\surd\!\!\!\surd$, and $\psi = \langle\!\langle b\rangle\!\rangle$. It is obvious that $P \models \phi;\surd\!\!\!\surd$ and $Q \models \psi$ but $P;Q \not\models \phi;\psi$. This is because nil is a neutral element of the sequential composition in process algebra, but $\surd$ ($\surd\!\!\!\surd$) is not a neutral element of the corresponding chop ';' in the logic. To solve this problem, we will replace every occurrence of $\surd\!\!\!\surd$ and $\surd$ in ϕ with τ in the resulting formulae, that is, $\phi\{\tau/\surd\!\!\!\surd, \tau/\surd\};\psi$. Because τ is a neutral element of the chop, this is in accordance with nil being a neutral element of the sequential composition (Aceto and Hennessy 1992).

Additionally, $\surd$ ($\surd\!\!\!\surd$) as a sub-formula of ϕ makes the sub-formula following it with ; be discarded during the calculation of the meaning of ϕ according to P1, but the sub-formula will be picked up when interpreting $\phi\{\tau/\surd\!\!\!\surd, \tau/\surd\};\psi$. This will give rise to problems. For example, $nil \models \surd\!\!\!\surd;[\![a]\!];\langle\!\langle b\rangle\!\rangle$ and $a;\tau;\tau;c \models \langle\!\langle a\rangle\!\rangle;\langle\!\langle c\rangle\!\rangle$, but

$$nil;(a;\tau;\tau;c) \not\models (\tau;[\![a]\!];\langle\!\langle b\rangle\!\rangle);(\langle\!\langle a\rangle\!\rangle;\langle\!\langle c\rangle\!\rangle).$$

So, we require ϕ to be a *propositional normal form.* In fact, Lemma 3 guarantees that this requirement is reasonable.

Summarising, we have the following connection between the chop of FLC$^+$ and the sequential composition of process algebra.

Theorem 5. Assume $\phi, \psi \in \mathscr{L}_{\mathrm{FLC}^+}$ are PNF. If $P \models \phi;\surd\!\!\!\surd$ and $Q \models \psi$, then $P;Q \models \phi\{\tau/\surd\!\!\!\surd, \tau/\surd\};\psi$.

Proof. The proof is by induction on $<$:

Base cases:

— $\phi = \tau$
Since $P \models \tau;\surd\!\!\!\surd$, it follows that $P \models \surd\!\!\!\surd$ by N. Hence, $\mathbb{T}(P)$. Thus,

$$P;Q \models \phi\{\tau/\surd\!\!\!\surd, \tau/\surd\};\psi$$

by Seq-2, N and the assumption $Q \models \psi$.

— $\phi = tt$ or ff
This case is easy.

— $\phi = \surd$ or $\phi = \surd\!\!\!\surd$
From $P \models \phi;\surd\!\!\!\surd$, we have $P \models \surd\!\!\!\surd$ by P1. Thus, $\mathbb{T}(P)$. Hence,

$$P;Q \models \phi\{\tau/\surd\!\!\!\surd, \tau/\surd\};\psi$$

by Seq-2, N and the assumption $Q \models \psi$.

— $\phi = \langle\!\langle\alpha\rangle\!\rangle$
Since $P \models \langle\!\langle\alpha\rangle\!\rangle;\surd\!\!\!\surd$, there exists P' such that $P \overset{\alpha}{\Rightarrow} P'$ and $\mathbb{T}(P')$. Thus, $P;Q \overset{\alpha}{\rightarrow} Q$ by Seq-2. Furthermore, because $Q \models \psi$, we obtain that $P;Q \models \phi\{\tau/\surd\!\!\!\surd, \tau/\surd\};\psi$.

— $\phi = [\![\alpha]\!]$
It is easy to show that $\neg\mathbb{T}(P)$ and $\forall P'.P \overset{\alpha}{\Rightarrow} P'$ implies $\mathbb{T}(P')$ because $P \models [\![\alpha]\!];\surd\!\!\!\surd$. On the other hand, by Seq-2, it can be shown that $\forall R.P;Q \overset{\alpha}{\Rightarrow} R$ only if $\exists P'.P \overset{\alpha}{\Rightarrow} P' \wedge R \approx^* Q$. Hence, by Theorem 3, $P;Q \models [\![\alpha]\!];\psi$.

Induction hypothesis (IH): For any closed PNF formulae φ and χ, and $P_1, P_1', P_2 \in \mathscr{P}^*$, if $P_1 \models \varphi$ and $P_2 \models \chi$, then for any PNF formula γ, if $\gamma < \varphi$ and $P_1' \models \gamma;\surd\!\!\!\surd$, then $P_1';P_2 \models \gamma\{\tau/\surd\!\!\!\surd, \tau/\surd\};\chi$.

Induction steps:

— $\phi = \bigwedge_{i\in I}\phi_i$
Since $P \models (\bigwedge_{i\in I}\phi_i;);\surd\!\!\!\surd$, it follows that $P \models \phi_i;\surd\!\!\!\surd$ for any $i \in I$ by the generalised IC. Besides, it is clear that ϕ_i is PNF since ϕ is PNF. Whence, we have that $P;Q \models \phi_i\{\tau/\surd\!\!\!\surd, \tau/\surd\};\psi$ by (IH) for each $i \in I$. Thus, we have $P;Q \models (\bigwedge \phi_i\{\tau/\surd\!\!\!\surd, \tau/\surd\});\psi$ from the generalised IC.

— $\phi = \bigvee_{i\in I}\phi_i$
This is similar to the above case.

— $\phi = \phi_1 ; \phi_2$ (without loss of generality, we assume $\phi_2 \not\Leftrightarrow \tau$ by N)
This case is carried out by induction on ϕ_1 with respect to $<$ as follows:

- $\phi_1 = tt$ or ff
  This case is easy to show by P1.
- $\phi_1 = \surd$ or $\psi_1 = \surd\!\!\!\surd$
  This violates the assumption that ϕ is PNF, so we do not need to consider it.
- $\phi_1 = \tau$
  For $P \models (\phi_1 ; \phi_2) ; \surd\!\!\!\surd$, we have $P \models \phi_2 ; \surd\!\!\!\surd$ by N. Since ϕ_2 is a proper sub-formula of ϕ, we get $P ; Q \models \phi_2\{\tau/\surd\!\!\!\surd, \tau/\surd\} ; \psi$ by (IH). Therefore,

  $$P ; Q \models (\phi_1 ; \phi_2)\{\tau/\surd\!\!\!\surd, \tau/\surd\} ; \psi$$

  by N.
- $\psi_1 = \langle\!\langle \alpha \rangle\!\rangle$
  As $P \models \langle\!\langle \alpha \rangle\!\rangle ; \phi_2 ; \surd\!\!\!\surd$, there exists P' such that $P \overset{\alpha}{\Rightarrow} P'$ and $P' \models \phi_2 ; \surd\!\!\!\surd$. Because $\phi_2 < \phi$, we have $P' ; Q \models \phi_2\{\tau/\surd\!\!\!\surd, \tau/\surd\} ; \psi$ by (IH). Thus, by Seq-1, $P ; Q \models (\langle\!\langle \alpha \rangle\!\rangle ; \phi_2)\{\tau/\surd\!\!\!\surd, \tau/\surd\} ; \psi$.
- $\psi_1 = [\![\alpha]\!]$
  It is easy to see that $\neg\mathbb{T}(P)$ and for all P', $P \overset{\alpha}{\Rightarrow} P'$ implies $P' \models \phi_2 ; \surd\!\!\!\surd$, since $P \models [\![\alpha]\!] ; \phi_2 ; \surd\!\!\!\surd$. Moreover, since $\phi_2 < \phi$, we get $P' ; Q \models \phi_2\{\tau/\surd\!\!\!\surd, \tau/\surd\} ; \psi$ by (IH). On the other hand, by Seq-1, for any R, we have $P ; Q \overset{\alpha}{\Rightarrow} R$ only if there exists P' such that $P \overset{\alpha}{\Rightarrow} P'$ and $R \approx^{*} P' ; Q$. Hence, $P ; Q \models ([\![\alpha]\!] ; \psi_2)\{\tau/\surd\!\!\!\surd, \tau/\surd\} ; \psi$ by Theorem 3.
- $\phi_1 = \bigwedge_{i \in I} \phi'_i$
  Since $P \models (\bigwedge_{i \in I} \phi'_i) ; \psi_2 ; \surd\!\!\!\surd$, we have $P \models (\bigwedge_{i \in I} \phi'_i ; \psi_2) ; \surd\!\!\!\surd$ from the generalised IC, therefore $P \models (\phi'_i ; \psi_2) ; \surd\!\!\!\surd$ for each $i \in I$. It is obvious that $\phi'_i ; \phi_2 < \bigwedge_{i \in I} \phi'_i ; \psi_2$. It then follows that $P ; Q \models (\phi'_i ; \phi_2)\{\tau/\surd\!\!\!\surd, \tau/\surd\} ; \psi$ for any $i \in I$ from (IH). Thus, $P ; Q \models ((\bigwedge_{i \in I} \phi'_i) ; \phi_2)\{\tau/\surd\!\!\!\surd, \tau/\surd\} ; \psi$ by the generalised IC.
- $\phi_1 = \bigvee_{i \in I} \phi'$
  This is similar to the above case.
- $\phi_1 = \phi' ; \phi''$
  By C, $(\phi' ; \phi'') ; \phi_2 \Leftrightarrow \phi' ; (\phi'' ; \phi_2)$. Thus, it follows that $P \models \phi' ; (\phi'' ; \phi_2) ; \surd\!\!\!\surd$ because $P \models (\phi' ; \phi'') ; \psi_2 ; \surd\!\!\!\surd$. On the other hand, it is easy to see that $\phi' ; (\phi'' ; \phi_2) < (\phi' ; \phi'') ; \phi_2$ by the definition of $<$. So, we have $P ; Q \models (\phi' ; (\phi'' ; \phi_2))\{\tau/\surd\!\!\!\surd, \tau/\surd\} ; \psi$ by (IH), and, therefore, $P ; Q \models ((\phi' ; \phi'') ; \phi_2)\{\tau/\surd\!\!\!\surd, \tau/\surd\} ; \psi$ by applying C.
- $\phi_1 = \nu^{\alpha} X . \phi'$
  We will use the following property under (IH) to justify this case.

  Property 1. If $P' \models (\nu^{\alpha} X . \sigma_1^{\beta_1 + 1} X_1 . \cdots . \sigma_n^{\beta_n + 1} X_n . \varphi) ; \psi_2 ; \surd\!\!\!\surd$ and $Q' \models \chi$, then

  $$P' ; Q' \models [(\nu^{\alpha} X . \sigma_1^{\beta_1 + 1} X_1 . \cdots . \sigma_n^{\beta_n + 1} X_n . \varphi) ; \psi_2]\{\tau/\surd\!\!\!\surd, \tau/\surd\} ; \chi,$$

  where φ is a PNF with one of the forms $Y, p, \tau @, \phi'_1 \vee \phi'_2, \phi'_1 \wedge \phi'_2, \phi'_1 ; \phi'_2, \sigma Y . \phi'_1$ or $\sigma^{\lambda'} Y . \phi'_1$, where λ' is a limit ordinal.

Proof. We use induction on $\alpha + (\beta_1 + 1) + \cdots + (\beta_n + 1)$.

(1) $\alpha = 0$
This case is trivial.

(2) $\alpha = \lambda$, where λ is a limit ordinal
Thus,

$$P' \models (\nu^{\lambda} X.\sigma_1^{\beta_1+1} X_1.\cdots.\sigma_n^{\beta_n+1} X_n.\varphi); \psi_2; \surd\!\!\surd$$

if and only if

$$\forall \beta < \lambda . P' \models (\nu^{\beta} X.\sigma_1^{\beta_1+1} X_1.\cdots.\sigma_n^{\beta_n+1} X_n.\varphi); \psi_2; \surd\!\!\surd.$$

By the local induction hypothesis, we have

$$\forall \beta < \lambda . P'; Q' \models ((\nu^{\beta} X.\sigma_1^{\beta_1+1} X_1.\cdots.\sigma_n^{\beta_n+1} X_n.\varphi); \psi_2)\{\tau/\surd\!\!\surd, \tau/\surd\}; \chi.$$

Therefore, $P'; Q' \models ((\nu^{\lambda} X.\sigma_1^{\beta_1+1} X_1.\cdots.\sigma_n^{\beta_n+1} X_n.\varphi); \psi_2)\{\tau/\surd\!\!\surd, \tau/\surd\}; \chi$.

(3) $\alpha = \beta + 1$
By the Tarski–Knaster fixed point theorem (Tarski 1955),

$$\nu^{\beta+1} \sigma_1^{\beta_1+1} X_1.\cdots.\sigma_n^{\beta_n+1} X_n.\varphi \Leftrightarrow \varphi\{\varphi'/X\}\{\varphi_1'/X_1\}\cdots\{\varphi_n'/X_n\},$$

where

$$\begin{aligned}
\varphi' &= \nu^{\beta} X.\sigma_1^{\beta_1+1} X_1.\cdots.\sigma_n^{\beta_n+1} X_n.\varphi,\\
\varphi_1' &= \sigma_1^{\beta_1} X_1.\sigma_2^{\beta_2+1} X_2.\cdots.\sigma_n^{\beta_n+1} X_n.\varphi\{\varphi'/X\},\\
&\ \vdots\\
\varphi_i' &= \sigma_i^{\beta_i} X_i.\sigma_{i+1}^{\beta_{i+1}+1} X_{i+1}.\cdots.\sigma_n^{\beta_n+1}.\varphi\{\varphi'/X\}\{\varphi_1'/X_1\}\cdots\{\varphi_{i-1}'/X_{i-1}\},\\
&\ \vdots\\
\varphi_n' &= \sigma_n^{\beta_n} X_n.\varphi\{\varphi'/X\}\{\varphi_1'/X_1\}\cdots\{\varphi_{n-1}'/X_{n-1}\}.
\end{aligned}$$

For brevity, we use $\{\overrightarrow{\varphi^*}\}$ to denote the vector $\{\varphi'/X\}\{\varphi_1'/X_1\}\cdots\{\varphi_n'/X_n\}$. Now we show this subcase by a case analysis on the structure of φ:

(a) $\varphi = p$
This case is straightforward.

(b) $\varphi = \tau$
It is easy to show this case using (IH).

(c) $\varphi = X$ or X_i where $i = 1, \cdots, n$
This is trivial by the local induction hypothesis.

(d) $\varphi = @$
This is similar to the subcases where $\psi_1 = @$.

(e) $\varphi = \phi_1' \wedge \phi_2'$
Thus, $P' \models (\phi_i'\{\overrightarrow{\varphi^*}\}; \phi_2); \surd\!\!\surd$ for $i = 1, 2$ as $P' \models (\varphi'; \phi_2); \surd\!\!\surd$. Applying (IH), we get

$$P'; Q' \models ((\phi_i'\{\overrightarrow{\varphi^*}\}); \phi_2))\{\tau/\surd\!\!\surd, \tau/\surd\}; \chi$$

for $i = 1, 2$. Hence,

$$P'; Q' \models ((\nu^{\beta+1}.\sigma_1^{\beta_1+1}X_1.\cdots.\sigma_n^{\beta_n+1}X_n.\varphi); \phi_2)\{\tau/\surd\!\!\surd, \tau/\surd\}; \chi.$$

(f) $\varphi = \phi_1' \vee \phi_2'$
This is similar to the above subcase.

(g) $\varphi = \phi_1'; \phi_2'$
It is obvious that $\phi_1'\{\overrightarrow{\varphi^*}\}; (\phi_2'\{\overrightarrow{\varphi^*}\}; \phi_2) < (\phi_1'\{\overrightarrow{\varphi^*}\}; \phi_2'\{\overrightarrow{\varphi^*}\}); \phi_2)$ from the definition of $<$. Therefore,

$$P'; Q' \models (\phi_1'\{\overrightarrow{\varphi^*}\}; (\phi_2'\{\overrightarrow{\varphi^*}\}; \phi_2))\{\tau/\surd\!\!\surd, \tau/\surd\}; \chi$$

by applying (IH). By C, we have

$$P'; Q' \models (\nu^{\alpha}X.\sigma_1^{\beta_1+1}X_1.\cdots.\sigma_n^{\beta_n+1}X_n.\varphi; \phi_2)\{\tau/\surd\!\!\surd, \tau/\surd\}; \chi.$$

(h) $\phi' = \sigma Y.\phi''$ or $\sigma^{\lambda'}Y.\phi'$ where λ' is a limit ordinal

From the Tarski–Knaster fixed point theorem (Tarski 1955), these subcases can be readily reduced to case (2) earlier in the proof of Property 1. This completes the proof of Property 1. □

- $\phi_2 = \mu^{\alpha}X.\phi'$
  This is similar to the above subcase.
- $\phi_1 = \sigma X.\phi'$
  Applying the Tarski–Knaster fixed point theorem (Tarski 1955) again, this case can be reduced to the previous two subcases.

— $\phi = \sigma^{\alpha}X.\phi_1$ or $\sigma X.\phi_1$
This is similar to the subcase where we had $\psi_1 = \nu^{\alpha}X.\phi'$ in the proof for the case $\phi = \phi_1; \phi_2$. □

Remark 2. In Theorem 5, if P cannot be evolved to a terminated process and $P \models \phi; \surd\!\!\surd$, where ϕ is PNF, we can prove that

$$\phi\{\tau/\surd\!\!\surd, \tau/\surd\}; \psi \Leftrightarrow \phi\{\tau/\surd\!\!\surd, \tau/\surd\}.$$

This is in accordance with $P; Q \approx^* P$ in the model level. For example,

$$\begin{aligned} P &\mathrel{\widehat{=}} rec\, x.a; \tau; x \\ Q &\mathrel{\widehat{=}} c; \tau; \tau; d \\ \phi &\mathrel{\widehat{=}} \nu X.\langle\!\langle a\rangle\!\rangle; X \\ \psi &\mathrel{\widehat{=}} \langle\!\langle c\rangle\!\rangle; \langle\!\langle d\rangle\!\rangle. \end{aligned}$$

It is obvious that $P \models \phi; \surd\!\!\surd$ and $Q \models \psi$, thus

$$P; Q \models \phi\{\tau/\surd\!\!\surd, \tau/\surd\}; \psi.$$

On the other hand, it is easy to see that $P; Q \approx^* P$ and

$$\phi\{\tau/\surd\!\!\surd, \tau/\surd\}; \psi \Leftrightarrow \phi\{\tau/\surd\!\!\surd, \tau/\surd\}.$$

Remark 3. The above remark implies that the converse of Theorem 5 is not valid in general, that is, it is possible that $P\,;Q \models \phi\{\tau/\surd\!\!\surd, \tau/\surd\}\,;\psi$ and $P \models \phi;\surd\!\!\surd$, where ϕ is PNF, but $Q \not\models \psi$. For example, in the previous example, let $\psi' \widehat{=} \langle\!\langle d\rangle\!\rangle;\langle\!\langle c\rangle\!\rangle$. Since $P\,;Q \approx^{*} P$ and

$$\phi\{\tau/\surd\!\!\surd, \tau/\surd\}\,;\psi' \Leftrightarrow \phi\{\tau/\surd\!\!\surd, \tau/\surd\},$$

it is easy to see that

$$P\,;Q \models \phi\{\tau/\surd\!\!\surd, \tau/\surd\}\,;\psi'$$

from $P \models \phi;\surd\!\!\surd$, but $Q \not\models \psi'$.

4.3. *Recursion*

Here, we show how to relate *rec x* to νX and μX. To this end, we first employ a relation called *weak syntactical confirmation* between processes and formulae, with the type $\mathscr{P}^s \times w\mathrm{FLC}^{+} \mapsto \{\mathrm{tt}, \mathrm{ff}\}$, and denoted by $\models_{wsc}$.

Definition 7. Given a formula ϕ, we associate a map from $2^{\mathscr{P}^s}$ to $2^{\mathscr{P}^s}$ with it, which is denoted by $\widetilde{\phi}$ and constructed by the following rules:

$$\begin{aligned}
\widetilde{\surd\!\!\surd}(\mathscr{E}) &\widehat{=} \{E \in \mathscr{P}^s \mid \mathbb{T}(E)\}\\
\widetilde{tt}(\mathscr{E}) &\widehat{=} \mathscr{P}^s\\
\widetilde{ff}(\mathscr{E}) &\widehat{=} \varnothing\\
\widetilde{\tau}(\mathscr{E}) &\widehat{=} \mathscr{E}\\
\widetilde{X}(\mathscr{E}) &\widehat{=} \{x;\tau^n;E \mid E \in \mathscr{E}, 0 \leqslant n\}\\
\widetilde{\langle\!\langle\alpha\rangle\!\rangle}(\mathscr{E}) &\widehat{=} \{E \mid \exists E' \in \mathscr{E}.E \overset{\alpha}{\Rightarrow} E'\}\\
\widetilde{[\![\alpha]\!]}(\mathscr{E}) &\widehat{=} \{E \mid \neg\mathbb{T}(E) \wedge E \text{ is guarded } \wedge \forall E'.E \overset{\alpha}{\Rightarrow} E' \Rightarrow E' \in \mathscr{E}\}\\
\phi_1 \widetilde{\wedge} \phi_2(\mathscr{E}) &\widehat{=} \widetilde{\phi_1}(\mathscr{E}) \cap \widetilde{\phi_2}(\mathscr{E})\\
\phi_1 \widetilde{\vee} \phi_2(\mathscr{E}) &\widehat{=} \widetilde{\phi_1}(\mathscr{E}) \cup \widetilde{\phi_2}(\mathscr{E})\\
\phi_1 \widetilde{+} \phi_2(\mathscr{E}) &\widehat{=} \{E \mid \exists E_1, E_2.E = E_1 + E_2 \wedge E_1 \in \widetilde{\phi_1}(\mathscr{E}) \wedge E_2 \in \widetilde{\phi_2}(\mathscr{E})\}\\
\widetilde{\phi_1;\phi_2}(\mathscr{E}) &\widehat{=} \widetilde{\phi_1} \cdot \widetilde{\phi_2}(\mathscr{E})\\
\widetilde{\sigma X.\phi}(\mathscr{E}) &\widehat{=} \{(rec\ x.E_1);E_2 \mid E_1 \in \widetilde{\phi}(\{\epsilon\}) \wedge E_2 \in \mathscr{E}\}
\end{aligned}$$

where $\alpha \in Act_\tau, \mathscr{E} \subseteq \mathscr{P}^s$.

$\models_{wsc}(E,\phi) = \mathrm{tt}$ if and only if $E \in \widetilde{\phi}(\{\epsilon\})$; otherwise, $\models_{wsc}(E,\phi) = \mathrm{ff}$. In the following, we use $E \models_{wsc} \phi$ to denote $\models_{wsc}(E,\phi) = \mathrm{tt}$ and $E \not\models_{wsc} \phi$ to denote $\models_{wsc}(E,\phi) = \mathrm{ff}$.

Informally, $P \models_{wsc} \phi$ means that P and ϕ have a similar syntax in the sense that all occurrences of the τ action in P that are not at the head of P are abstracted away. However, in comparison with the notion of *syntactical confirmation* in Zhan and Wu (2005), the clauses for $\surd\!\!\surd$, x, $\langle\!\langle\alpha\rangle\!\rangle$ and $[\![\alpha]\!]$ are very different.

Example 3. Let

$$\begin{aligned}
E_0 &\mathrel{\widehat{=}} rec\, x.\tau;x+\tau\\
E_1 &\mathrel{\widehat{=}} (\tau;\tau;a;x;x)+d;\tau\\
E_2 &\mathrel{\widehat{=}} x;(b;\tau+c);\tau;y;\tau\\
E_3 &\mathrel{\widehat{=}} E_0;a;b;c
\end{aligned}$$

and

$$\begin{aligned}
\phi_0 &\mathrel{\widehat{=}} \surd\\
\phi_1 &\mathrel{\widehat{=}} \langle\!\langle\alpha\rangle\!\rangle;X;X\\
\phi_2 &\mathrel{\widehat{=}} X;\langle\!\langle\beta\rangle\!\rangle;Y\\
\phi_3 &\mathrel{\widehat{=}} [\![\alpha]\!];\langle\!\langle\beta\rangle\!\rangle;\langle\!\langle\kappa\rangle\!\rangle.
\end{aligned}$$

Then, according to the above definition, we have

$$\begin{aligned}
E_0 &\models_{wsc} \phi_0\\
E_1 &\models_{wsc} \phi_1\\
E_2 &\models_{wsc} \phi_2\\
E_3 &\models_{wsc} \phi_3.
\end{aligned}$$

The following Theorem shows that $\models_{wsc}$ itself is also compositional.

Theorem 6. Let ϕ_1, ϕ_2 and ϕ be PNF. Then,

(i) If $E_1 \models_{wsc} \phi_1$ and $E_2 \models_{wsc} \phi_2$, then $E_1+E_2 \models_{wsc} \phi_1+\phi_2$.
(ii) If $E_1 \models_{wsc} \phi_1$ and $E_2 \models_{wsc} \phi_2$, then $E_1;E_2 \models_{wsc} \phi_1\{\tau/\surd\!\surd\};\phi_2$.
(iii) If $E \models_{wsc} \phi$, then *rec x.E* $\models_{wsc} \sigma X.\phi\{\tau/\surd\!\surd\}$.

Example 4. In Example 3, according to Theorem 6, we obtain

$$\begin{aligned}
E_1+E_2 &\models_{wsc} \phi_1+\phi_2\\
E_3;(E_1+E_2) &\models_{wsc} \phi_3;(\phi_1+\phi_2)\\
rec\ x.\ rec\ y.E_3;(E_1+E_3) &\models_{wsc} \nu X.\nu Y.(\phi_3;(\phi_1+\phi_2)).
\end{aligned}$$

In order to prove Theorem 6, we need the following lemma.

Lemma 11. If ϕ_1, ϕ_2 and ϕ_3 are PNFs and there is no $\surd\!\surd$ occurring in ϕ_1, then

$$(\widetilde{\phi_1}\cdot\widetilde{\phi_2}(\mathscr{E}));\widetilde{\phi_3}(\mathscr{E}) \subseteq \widetilde{\phi_1}(\widetilde{\phi_2}(\mathscr{E});\widetilde{\phi_3}(\mathscr{E})),$$

where $\mathscr{A}\,;\,\mathscr{B}$ stands for

$$\{E_1\ ;\ E_2 \mid E_1 \in \mathscr{A} \text{ and } E_2 \in \mathscr{B}\}.$$

Proof. We use case analysis on the structure of ϕ_1:

— $\phi_1 = \tau, X, tt$ or ff
These cases are trivial from Definition 7.

— $\phi_1 = \surd$

This case violates the assumption so we do not need to consider it.

— $\phi_1 = \langle\!\langle \alpha \rangle\!\rangle$

$$\begin{array}{rcl}
\text{LHS} & = & \{E \mid \exists E'.E \overset{\alpha}{\Rightarrow} E' \wedge E' \in \widetilde{\phi_2(\mathscr{E})}\};\widetilde{\phi_3(\mathscr{E})} \\
& \subseteq & \{E \mid \exists E'.E \overset{\alpha}{\Rightarrow} E' \wedge E' \in \widetilde{\phi_2(\mathscr{E})};\widetilde{\phi_3(\mathscr{E})}\} \\
& = & \langle\!\langle \alpha \rangle\!\rangle(\{\widetilde{\phi_2(\mathscr{E})};\widetilde{\phi_3(\mathscr{E})}\}) \\
& = & \text{RHS.}
\end{array}$$

— $\phi_1 = [\![\alpha]\!]$

$$\begin{array}{rcl}
\text{LHS} & = & \{E \mid \neg\mathbb{T}(E) \text{ and } E \text{ is guarded and } \forall E'.E \overset{\alpha}{\Rightarrow} E' \Rightarrow E' \in \widetilde{\phi_2(\mathscr{E})}\};\widetilde{\phi_3(\mathscr{E})} \\
& \subseteq & \{E \mid \neg\mathbb{T}(E) \text{ and } E \text{ is guarded and } \forall E'.E \overset{\alpha}{\Rightarrow} E' \Rightarrow E' \in \widetilde{\phi_2(\mathscr{E})};\widetilde{\phi_3(\mathscr{E})}\} \\
& = & [\![\alpha]\!] \cdot (\widetilde{\phi_2(\mathscr{E})};\widetilde{\phi_3(\mathscr{E})}) \\
& = & \text{RHS.}
\end{array}$$

— $\phi_1 = \phi' \wedge \phi''$

$$\begin{array}{rcll}
\text{LHS} & = & \widetilde{\phi' \wedge \phi''} \cdot \widetilde{\phi_2(\mathscr{E})};\widetilde{\phi_3(\mathscr{E})} & \\
& = & (\widetilde{\phi'} \cdot \widetilde{\phi_2(\mathscr{E})} \cap \widetilde{\phi''} \cdot \widetilde{\phi_2(\mathscr{E})});\widetilde{\phi_3(\mathscr{E})} & \text{(Definition 7)} \\
& = & (\widetilde{\phi'} \cdot \widetilde{\phi_2(\mathscr{E})};\widetilde{\phi_3(\mathscr{E})}) \cap (\widetilde{\phi''} \cdot \widetilde{\phi_2(\mathscr{E})};\widetilde{\phi_3(\mathscr{E})}) & \\
& \subseteq & \widetilde{\phi'}(\widetilde{\phi_2(\mathscr{E})};\widetilde{\phi_3(\mathscr{E})}) \cap \widetilde{\phi''}(\widetilde{\phi_2(\mathscr{E})};\widetilde{\phi_3(\mathscr{E})}) & \text{(induction hypothesis)} \\
& = & \widetilde{\phi' \wedge \phi''} \cdot (\widetilde{\phi_2(\mathscr{E})};\widetilde{\phi_3(\mathscr{E})}) & \\
& = & \text{RHS.} &
\end{array}$$

— $\phi_1 = \phi' \vee \phi''$

This is similar to the above case.

— $\phi_1 = \phi';\phi''$

$$\begin{array}{rcll}
\text{LHS} & = & (\widetilde{\phi';\phi''} \cdot \widetilde{\phi_2(\mathscr{E})});\widetilde{\phi_3(\mathscr{E})} & \\
& = & (\widetilde{\phi'} \cdot (\widetilde{\phi''} \cdot \widetilde{\phi_2(\mathscr{E})}));\widetilde{\phi_3(\mathscr{E})} & \\
& \subseteq & \widetilde{\phi'} \cdot (\widetilde{\phi''} \cdot \widetilde{\phi_2(\mathscr{E})};\widetilde{\phi_3(\mathscr{E})}) & \text{(induction hypothesis)} \\
& \subseteq & \widetilde{\phi'} \cdot \widetilde{\phi''} \cdot (\widetilde{\phi_2(\mathscr{E})};\widetilde{\phi_3(\mathscr{E})}) & \text{(induction hypothesis)} \\
& = & (\widetilde{\phi';\phi''}) \cdot (\widetilde{\phi_2(\mathscr{E})};\widetilde{\phi_3(\mathscr{E})}) & \\
& = & \text{RHS.} &
\end{array}$$

— $\phi_1 = \phi_1 + \phi_2$

$$\begin{array}{rcll}
\text{LHS} & = & (\widetilde{\phi' + \phi''} \cdot \widetilde{\phi_2(\mathscr{E})});\widetilde{\phi_3(\mathscr{E})} & \\
& = & \{E \mid E \approx^* E_1 + E_2 \wedge & \\
& & \quad E_1 \in \widetilde{\phi'} \cdot \widetilde{\phi_2(\mathscr{E})} \wedge & \\
& & \quad E_2 \in \widetilde{\phi''} \cdot \widetilde{\phi_2(\mathscr{E})}\};\widetilde{\phi_3(\mathscr{E})} & \text{(Definition 7)} \\
& = & \{E;E' \mid E = E_1 + E_2 \wedge E_1 \in \widetilde{\phi'} \cdot \widetilde{\phi_2(\mathscr{E})} \wedge & \\
& & \qquad E_2 \in \widetilde{\phi''} \cdot \widetilde{\phi_2(\mathscr{E})} \wedge E' \in \widetilde{\phi_3(\mathscr{E})}\} & \text{(Definition of ;)} \\
& \subseteq & \{E \mid E \approx^* E_1;E' + E_2;E' \wedge & \\
& & \quad E_1;E' \in (\widetilde{\phi'} \cdot \widetilde{\phi_2(\mathscr{E})});\widetilde{\phi_3(\mathscr{E})} \wedge & \\
& & \quad E_2;E' \in (\widetilde{\phi''} \cdot \widetilde{\phi_2(\mathscr{E})});\widetilde{\phi_3(\mathscr{E})}\} & \text{(distribution of ; over +)} \\
& \subseteq & \{E \mid E = E_1;E' + E_2;E' \wedge & \\
& & \quad E_1;E' \in \widetilde{\phi'} \cdot (\widetilde{\phi_2(\mathscr{E})};\widetilde{\phi_3(\mathscr{E})}) \wedge & \\
& & \quad E_2;E' \in \widetilde{\phi''} \cdot (\widetilde{\phi_2(\mathscr{E})};\widetilde{\phi_3(\mathscr{E})})\} & \text{(induction hypothesis)} \\
& \subseteq & \widetilde{\phi' + \phi''}(\widetilde{\phi_2(\mathscr{E})};\widetilde{\phi_3(\mathscr{E})}) & \text{(Definition 7)} \\
& = & \text{RHS.} &
\end{array}$$

— $\phi_1 = \nu X.\phi'$

$$\begin{array}{rcll}
\text{LHS} & = & \{(rec\ x.E_1);E_2 \mid E_1 \in \widetilde{\phi'}(\{\epsilon\})\wedge & \\
 & & \qquad E_2 \in \widetilde{\phi_2}(\mathscr{E})\};\widetilde{\phi_3}(\mathscr{E}) & \text{(Definition 7)} \\
 & = & \{((rec\ x.E_1);E_2);E_3 \mid E_1 \in \widetilde{\phi'}(\{\epsilon\})\wedge & \\
 & & \qquad E_2 \in \widetilde{\phi_2}(\mathscr{E}) \wedge E_3 \in \widetilde{\phi_3}(\mathscr{E})\} & \text{(Definition of ;)} \\
 & = & \{(rec\ x.E_1);(E_2;E_3) \mid E_1 \in \widetilde{\phi'}(\{\epsilon\})\wedge & \\
 & & \qquad E_2 \in \widetilde{\phi_2}(\mathscr{E}) \wedge E_3 \in \widetilde{\phi_3}(\mathscr{E})\} & \text{(association of ;)} \\
 & \subseteq & \widetilde{\nu X.\phi'} \cdot (\widetilde{\phi_2}(\mathscr{E});\widetilde{\phi_3}(\mathscr{E})) & \text{(Definition 7)} \\
 & = & \text{RHS.} &
\end{array}$$

— $\phi_1 = \mu X.\phi'$

This is similar to the above case. □

We can now give the proof for Theorem 6.

Proof. The proofs for parts (i) and (iii) are obvious by Definition 7. The proof for (ii) can be done by induction on the structure of ϕ_1. We will only consider the interesting case $\phi_1 = \phi';\phi''$:

$$\begin{array}{rll}
E_1;E_2 & \in \{E \mid E \models_{wsc} \phi';\phi''\};\widetilde{\phi_2}(\{\epsilon\}) & \\
 & \subseteq \{E \mid E \models_{wsc} (\phi'\{(\llbracket\,\rrbracket;\langle\!\langle\rangle\!\rangle)/\surd\!\!\surd\};\phi'')\};\widetilde{\phi_2}(\{\epsilon\}) & \text{(assumption)} \\
 & \subseteq \widetilde{\phi'}\{(\llbracket\,\rrbracket;\langle\!\langle\rangle\!\rangle)/\surd\!\!\surd\} \cdot (\{E \mid E \models_{sc} \phi''\};\widetilde{\phi_2}(\{\epsilon\})) & \text{(Lemma 11)} \\
 & \subseteq \widetilde{\phi'}\{(\llbracket\,\rrbracket;\langle\!\langle\rangle\!\rangle)/\surd\!\!\surd\} \cdot (\widetilde{\phi''\{\tau/\surd\}} \cdot \widetilde{\phi_2}(\{\epsilon\})) & \text{(induction hypothesis)} \\
 & = (\widetilde{\phi';\phi''}\{(\llbracket\,\rrbracket;\langle\!\langle\rangle\!\rangle)/\surd\!\!\surd\} \cdot \widetilde{\phi_2}(\{\epsilon\}). &
\end{array}$$

Hence, $E_1;E_2 \models_{wsc} (\phi';\phi'')\{(\llbracket\,\rrbracket;\langle\!\langle\rangle\!\rangle)/\surd\!\!\surd\};\phi_2$. □

In order to establish a correlation between $\models_{wsc}$ and $\models$, we need the following results.

Lemma 12. Let

$$fn(E) \subseteq \{x_1,\cdots,x_n\}$$
$$fn(\psi) \subseteq \{X_1,\cdots,X_n\}.$$

If $E \models_{wsc} \psi$ and $P_i \models \phi_i;\surd\!\!\surd$, then

$$E\{P_1/x_1,\cdots,P_n/x_n\} \models \psi\{\phi_1/X_1,\cdots,\phi_n/X_n\};\surd\!\!\surd,$$

provided $\surd\!\!\surd$ does not occur in ϕ_i for $i \in \{1,\cdots,n\}$ or in ψ.

Proof. The proof is similar to the proof of Theorem 5, using induction on ψ with respect to $<$. □

The following theorem establishes a connection between $\models_{wsc}$ and $\models$, to relate *rec x* to νX. For instance, in Example 4, we get

$$rec\ x.\ rec\ y.E_3;(E_1+E_3) \models \nu X.\nu Y.(\varphi;(\phi+\psi)).$$

Theorem 7. For any given $P \in \mathrm{BPA}_{\delta}^{\epsilon,\Omega}$ and formula ϕ that is PNF, if $P \models_{wsc} \phi$, then $P \models \phi; \surd\!\!\surd$.

Proof. This proof is by induction on the structure of ϕ. The only interesting cases are the ones when $\phi = \sigma X.\phi'$. We will only give the proof for the case when $\phi = \nu X.\phi'$; the proof for the case when $\phi = \mu X.\phi'$ is similar.

By the Tarski–Knaster fixed point theorem (Tarski 1955),

$$P \models (\nu X.\phi'); \surd\!\!\surd \text{ if and only if } P \models \left(\bigwedge_{\alpha<\kappa} \nu^{\alpha} X.\phi' \right); \surd\!\!\surd,$$

where κ is some limit ordinal. Thus, we show this case by induction on α:

— $\alpha = 0$
This case is trivial.

— $\alpha = \lambda$, where λ is a limit ordinal
Since $P \models (\nu^{\lambda} X.\phi'); \surd$ if and only if $\forall \alpha < \lambda . P \models (\nu^{\alpha} X.\phi'); \surd\!\!\surd$, this case is true by the induction hypothesis.

— $\alpha = \beta + 1$
Since $P \models_{wsc} \nu X.\phi'$, there exists E^* such that $P = \mathit{rec}\ x.E^*$ and $E^* \models_{wsc} \phi'$. By the induction hypothesis, we have $P \models (\nu^{\beta} X.\phi'); \surd\!\!\surd$. Therefore, by Lemma 12, we have $E^*\{P/x\} \models \phi'\{(\nu^{\beta} X.\phi')/Y\}; \surd\!\!\surd$. That is, $P \models (\nu^{\beta+1} X.\phi')/Y\}; \surd\!\!\surd$. □

5. Case study: a production line

As a consequence of the compositionality of FLC derived in the previous section, we can use FLC to give a compositional specification for a system. Typically, this may allow much more concise descriptions of concurrent systems and for easier composition/decomposition of the verification of a large system from/to some similar and simpler verifications of the subsystems. For example, using '+' as an auxiliary operator could be useful in practice because:

(i) It enables a precise and compact specification of certain non-deterministic systems.
(ii) It is very easy to modify the specification of a system when additional alternatives for the behaviour of the system should be allowed.
(iii) It enhances the possibility of modularity in model checking, which is useful when redesigning systems.

These advantages are illustrated by the following example. Consider a car factory that wants to establish the assembly line shown in Figure 2, which we denote by the process P, for one step in the production. If there is a car available for P, then P will either get the car, adjust the motor, mount the windscreen, control the car, and then put the car back on the conveyer belt or P will get the car, mount the windscreen, adjust the motor, control the car, and then put it back. Afterwards, P may start again. Before or after each action, some internal actions could be done.

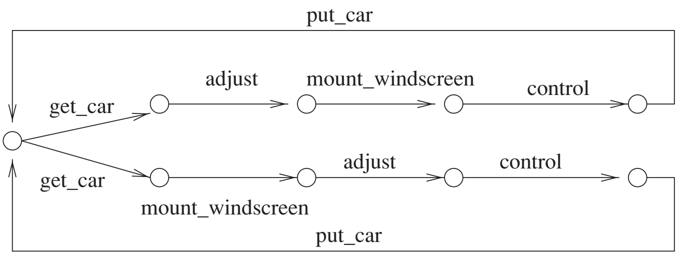

Fig. 2. The Process P

The first option can be specified by

$$\text{Spec}_1 \mathrel{\widehat{=}} [\![\text{get\_car}]\!]\,;\langle\!\langle\text{adjust}\rangle\!\rangle;\langle\!\langle\text{mount\_windscreen}\rangle\!\rangle;\langle\!\langle\text{control}\rangle\!\rangle;\langle\!\langle\text{put\_car}\rangle\!\rangle \wedge \langle\!\langle\text{get\_car}\rangle\!\rangle;\text{tt},$$

while the second is described by

$$\text{Spec}_2 \mathrel{\widehat{=}} [\![\text{get\_car}]\!]\,;\langle\!\langle\text{mount\_windscreen}\rangle\!\rangle;\langle\!\langle\text{adjust}\rangle\!\rangle;\langle\!\langle\text{control}\rangle\!\rangle;\langle\!\langle\text{put\_car}\rangle\!\rangle \wedge \langle\!\langle\text{get\_car}\rangle\!\rangle;\text{tt}.$$

We are now looking for a specification that admits only such systems that offer both alternatives and can be easily constructed from Spec_1 and Spec_2. Obviously, $\text{Spec}_1 \wedge \text{Spec}_2$ is not suitable, and neither is $\text{Spec}_1 \vee \text{Spec}_2$ since it allows for implementations that exhibit only one of the behaviours. However, $\text{Spec}_1 + \text{Spec}_2$ does describe the behaviour we have in mind, and a system that offers this behaviour repeatedly is described by $\text{Spec} \mathrel{\widehat{=}} \nu X.(\text{Spec}_1 + \text{Spec}_2);X$.

It is easy to show that $rec\ x.(P_1 + P_2);x \models \text{Spec}$, where

$$\text{P}_1 \mathrel{\widehat{=}} \tau^*;\text{get\_car};\tau^*;\text{adjust};\tau^*;\text{mount\_windscreen};\tau^*;\text{control};\tau^*;\text{put\_car}$$
$$\text{P}_2 \mathrel{\widehat{=}} \tau^*;\text{get\_car};\tau^*;\text{mount\_windscreen};\tau^*;\text{adjust};\tau^*;\text{control};\tau^*;\text{put\_car}.$$

We now assume that the system specification needs modification to allow for a third alternative behaviour Spec_3. This specification may simply be ‘added’ to form

$$\text{Spec}' \mathrel{\widehat{=}} \nu X.(\text{Spec}_1 + \text{Spec}_2 + \text{Spec}_3);X.$$

If we establish $P_3 \models \text{Spec}_3$, we immediately have

$$rec\ x.(P_1 + P_2 + P_3);x \models \text{Spec}'.$$

In addition, if we have to modify Spec_1 to Spec_1' such that $P_1' \models \text{Spec}_1'$, we can obtain

$$rec\ x.(P_1' + P_2 + P_3);x \models \nu X.(\text{Spec}_1' + \text{Spec}_2 + \text{Spec}_3);X.$$

6. Constructing characteristic formulae for context-free processes up to $\preceq$ and $\preceq^*$ compositionally

In this section, we will first discuss how to define the characteristic formula of a process in $\text{BPA}_\delta^{\epsilon,\Omega}$ up to $\preceq$, then consider how to define its characteristic formula up to $\preceq^*$.

We will use the following notation:

$$[\![\downarrow]\!] = \mu X.[\tau];X$$
$$\langle\!\langle\uparrow\rangle\!\rangle = \nu X.\langle\tau\rangle;X.$$

The first formula says that any process that satisfies the formula must be convergent, that is, the process cannot perform an infinite sequence of unobservable actions; the second says that any process with the property may potentially perform an infinite sequence of unobservable actions, that is, be divergent. It is clear that a divergent process has the property $\langle\!\langle\uparrow\rangle\!\rangle$, but cannot satisfy $[\![\downarrow]\!]$.

For simplicity, $\bigwedge_{\alpha\in Act_\tau - A}[\![\alpha]\!];ff$ will be abbreviated to Φ_{-A} from now on.

In the following, we discuss how to characterise the primitives of $\mathrm{BPA}_\delta^{\epsilon,\Omega}$ up to the preorder $\preceq$ so that the characteristic formula of a composite process may be built from those of the primitives according to its syntactical structure:

— We will first consider the characteristic formulae of δ. It is obvious that for any process Q, if $\delta \preceq^* Q$, then Q should have the following properties:

- Q cannot do any action after a finite sequence of τ according to Definition 2;
- Q cannot terminate and must be convergent.

So the characteristic formula of δ up to $\preceq$ can be defined as $\Phi_{-\{\,\}}$ ($\Phi_\delta^{\preceq}$ for short). Notice that if we view δ as an abbreviation for $rec\,x.x$, then $\delta \models_{wsc} \Phi_\delta^{\preceq}$ according to Definition 7.

— Any process Q with $\epsilon \preceq^* Q$, must terminate after executing a finite sequence of τ actions. Moreover, it cannot execute any action other than τ. Therefore, ϵ can be characterised by $\Phi_{-\{\tau\}} \wedge \surd\!\!\!\surd$, written as $\Phi_\epsilon^{\preceq}$. Note that $\Phi_\epsilon^{\preceq}$ guarantees that the process is weak terminated, and $\epsilon \models_{wsc} \Phi_\epsilon^{\preceq}$.

— Intuitively, the characteristic formula of Ω should be $\langle\!\langle\uparrow\rangle\!\rangle$ up to $\preceq$. But according to the observational preorder, all internal actions will be abstracted away, so $\langle\!\langle\uparrow\rangle\!\rangle$ will become *tt*, that is, the characteristic formula of Ω is *tt*. This is in accordance with $\Omega \preceq Q$ for any $Q \in \mathrm{BPA}_\delta^{\epsilon,\Omega}$.

— For an action $a \in Act_\tau \setminus \{\tau\}$, for any process Q for which $a \preceq^* Q$, the process Q should have the following properties:

- Q performs a and then evolves to ϵ;
- Q may perform any finitely many unobservable actions before and after executing a, but cannot diverge.

Let

$$\Phi_a^{\preceq} = \Phi_{-\{a,\tau\}} \wedge ([\![\bar{a}]\!] \wedge \langle\!\langle\bar{a}\rangle\!\rangle).$$

So we can define the characteristic formula of a up to $\preceq$ as $\Phi_a^{\preceq};\surd\!\!\!\surd$. It also follows that $a \models_{wsc} \Phi_a^{\preceq}$ by Definition 7.

— The τ action will be abstracted away, so it can be characterised by the formula τ.

— Since the recursive operator may introduce divergence, we define the characteristic formula according to whether it gives rise to divergence that can be determined by checking whether the process satisfies $\langle\!\langle\uparrow\rangle\!\rangle$. Therefore, unlike in Zhan and Wu (2005) the characteristic formula of a context-free process up to $\sim$ can be constructed syntactically. It is obvious that the characteristic formula for a divergent process Ω up to $\preceq^*$ is tt because $\Omega \preceq^* Q$ for any $Q \in \mathrm{BPA}_\delta^{\epsilon,\Omega}$. Moreover, it is well known that if a process E is divergent, then so are $E + F$ and $F + E$. Therefore, the characteristic formulae of $E + F$ and $F + E$ up to $\preceq$ are tt also if either of them diverges.

Summarising, given a process term $E \in \mathscr{P}^s$, we can use the following algorithm to associate a formula of wFLC$^+$ with E according to its syntax.

Definition 8. Given a process term $E \in \mathscr{P}^s$, we associate with it a formula of wFLC$^+$, denoted by $\Psi_E^{\preceq}$, constructed by the following rules:

$$\begin{aligned}
\Psi_\delta^{\preceq} &\mathrel{\widehat{=}} \Phi_\delta^{\preceq}\\
\Psi_\varepsilon^{\preceq} &\mathrel{\widehat{=}} \Phi_\epsilon^{\preceq}\\
\Psi_\Omega^{\preceq} &\mathrel{\widehat{=}} tt\\
\Psi_x^{\preceq} &\mathrel{\widehat{=}} X\\
\Psi_a^{\preceq} &\mathrel{\widehat{=}} \Phi_a^{\preceq} \text{ for } a \in Act_\tau \setminus \{\tau\}\\
\Psi_\tau^{\preceq} &\mathrel{\widehat{=}} \tau\\
\Psi_{E_1;E_2}^{\preceq} &\mathrel{\widehat{=}} \Psi_{E_1}^{\preceq}\{\tau/\surd\!\!\surd\}; \Psi_{E_2}^{\preceq},\\
\Psi_{E_1+E_2}^{\preceq} &\mathrel{\widehat{=}} \begin{cases} tt & \text{if } \Psi_{E_1}^{\preceq} \Leftrightarrow tt \text{ or } \Psi_{E_2}^{\preceq} \Leftrightarrow tt\\ \Psi_{E_1}^{\preceq} + \Psi_{E_2}^{\preceq} & \text{otherwise}\end{cases}\\
\Psi_{rec\ x.E}^{\preceq} &\mathrel{\widehat{=}} \begin{cases} tt & \text{if } rec\, x.E \models \langle\!\langle \uparrow \rangle\!\rangle\\ \nu X.\Psi_E\{\tau/\surd\!\!\surd\} & \text{otherwise.}\end{cases}
\end{aligned}$$

Definition 8 gives rise to the following lemma.

Lemma 13.

(1) For any $E \in \mathscr{P}^s$, we have $E \models_{wsc} \Psi_E^{\preceq}$ and $E \models_{wsc} \Psi_E^{\preceq}; \surd\!\!\surd$.
(2) For any $P \in \mathrm{BPA}_\delta^{\epsilon,\Omega}$, we have $\Psi_P^{\preceq}; \surd\!\!\surd \in w\mathscr{L}_{\mathrm{FLC}^+}$.

In the following, we will show that $en(\Psi_P^{\preceq}); \surd\!\!\surd$ is the characteristic formula of P up to $\preceq$ for each $P \in \mathrm{BPA}_\delta^{\epsilon,\Omega}$.

Theorem 8. For any $P \in \mathrm{BPA}_\delta^{\epsilon,\Omega}$, we have $Q \models en(\Psi_P^{\preceq}); \surd\!\!\surd$ if and only if $P \preceq Q$.

Proof.

Only if: By Lemma 13, we have $P \models_{wsc} \Psi_P^{\preceq}$ and therefore $P \models \Psi_P^{\preceq}; \surd\!\!\surd$ according to Theorem 7. So it follows that $Q \models \Psi_P^{\preceq}; \surd\!\!\surd$ by Theorem 2. This completes the proof for the only if part.

If: Let $R = \{(P_1, P_2) \mid P_2 \models \Psi_{P_1}\Psi_P^{\preceq}; \surd\!\!\surd\}$. Suppose $(Q_1, Q_2) \in R$. By induction on (Q_1, Q_2), we have:

(i) It is obvious that if $(Q_1, Q_2) \in R$ and $\downarrow (Q_1)$, then $\mathbb{T}(Q_1)$ if and only if $\mathbb{T}(Q_2)$.

(ii) Suppose $Q_1 \xrightarrow{\alpha} Q_1'$. According to the definition of $\Psi^{\preceq}_{Q_1};\surd\!\!\surd$, we have $(\Psi^{\preceq}_{Q_1};\surd\!\!\surd) \Rightarrow (\langle\!\langle\bar{\alpha}\rangle\!\rangle;\Psi^{\preceq}_{Q_1'};\surd\!\!\surd)$. Therefore, $Q_2 \models \langle\!\langle\bar{\alpha}\rangle\!\rangle;\Psi^{\preceq}_{Q_1'};\surd\!\!\surd$. Thus, there exists Q_2' such that $Q_2 \overset{\bar{\alpha}}{\Rightarrow} Q_2'$ and $Q_2' \models \Psi^{\preceq}_{Q_1'};\surd\!\!\surd$. So, $(Q_1', Q_2') \in R$ by the definition.

(iii) Suppose $\downarrow_\alpha (Q_1)$.
On the one hand, it is easy to prove

$$Q_1 \approx \sum_{j=1}^{i_\alpha} \tau^{\ell_0};\bar{\alpha};\tau^{\ell_1};Q_j' + \sum_{\beta\in Act_\tau}\sum_{j=1}^{i_\beta} \tau^{\ell_{j0}}\bar{\beta};\tau^{\ell_{j1}};Q_{\beta,j} + (\delta) + (\Omega)\widehat{=}Q_1^*,$$

in which δ and Ω are optional. Thus, it follows that $\downarrow (Q_j)$ for $j = 1,\ldots,i_\alpha$.
On the other hand, from $Q_1 \approx Q_1^*$ and Theorems 2, 1 and 9 (the last of these will be proved below), we have $\Psi_{Q_1};\surd\!\!\surd \Leftrightarrow \Psi_{Q_1^*};\surd\!\!\surd$. So $Q_2 \models \Psi_{Q_1^*}$. Thus, we have $Q_2 \models [\![\bar{\alpha}]\!];\bigvee_{j=1}^{i_\alpha}\Psi_{Q_j'};\surd\!\!\surd$ from Definition 8. So, for any Q_2', if $Q_2 \overset{\bar{\alpha}}{\Rightarrow} Q_2'$, we have $Q_2' \models \bigvee_{j=1}^{i_\alpha}\Psi_{Q_j'};\surd\!\!\surd$. That is, $Q_2' \models \Psi_{Q_j'};\surd\!\!\surd$ for some $j \in \{1,\ldots,i_\alpha\}$. By the induction hypothesis, we have $(Q_j', Q_2') \in R$ and $\downarrow (Q_2')$. Thus, $\downarrow_\alpha (Q_2)$.

So we can conclude that $Q_1 \preceq Q_2$ from Definition 1. □

Remark 4. In Theorem 8, the condition that P is guarded is essential – the theorem fails without this condition. For instance,

$$\nu X.(X + (\langle\!\langle\alpha\rangle\!\rangle \wedge [\![\alpha]\!][\![\downarrow]\!] \wedge \Phi_{-\{a\}}))$$

is equivalent to $\Psi_{rec\ x.(x+a)}$, but

$$(\nu X.(X + (\langle\!\langle\alpha\rangle\!\rangle \wedge [\![\alpha]\!] \wedge \Phi_{-\{a\}})));\surd\!\!\surd$$

is not the characteristic formula of *rec* $x.(x+a)$ since *rex* $x.(x+b+a)$ satisfies the formula, but *rec* $x.(x+a) \not\preceq$ *rex* $x.(x+b+a)$.

In order to define the characteristic formula of P up to $\preceq^*$, we need to allow $[\![\tau]\!]$ and $\langle\!\langle\tau\rangle\!\rangle$ to be formulae of wFLC.

The characteristic formula of P up to $\preceq^*$, denoted $\Psi^{\preceq^*}_P$, can be constructed similarly to its characteristic formula up to $\preceq$, except that

$$\Psi^{\preceq^*}_\tau = \Phi_{\{\tau\}} \wedge ([\![\tau]\!] \wedge \langle\!\langle\tau\rangle\!\rangle);\surd\!\!\surd$$

and

$$\Psi^{\preceq^*}_{E_1;E_2}\widehat{=}\begin{cases}\Psi^{\preceq^*}_{E_1}\{\tau/\surd\!\!\surd\};\Psi^{\preceq^*}_{E_2} & \text{if } E_2 \neq \tau\\ \Psi^{\preceq^*}_{E_1} & \text{otherwise.}\end{cases}$$

The following lemma says that the proof system for $\preceq^*$ (See Section 2) will be valid in FLC$^+$ if P is substituted by $\Psi^{\preceq^*}_P;\surd\!\!\surd$, and $=$ by $\Leftrightarrow$. That is, we have the following lemma.

Lemma 14.

$$
\begin{array}{llll}
\text{A0} & \Psi^{\leq^*}_{E_1+E_2};\surd\!\!\surd \Leftrightarrow \Psi^{\leq^*}_{E_2+E_1};\surd\!\!\surd & \text{A1} & \Psi^{\leq^*}_{(E_1+E_2)+E_3};\surd\!\!\surd \Leftrightarrow \Psi^{\leq^*}_{E_1+(E_2+E_3)};\surd\!\!\surd \\
\text{A2} & \Psi^{\leq^*}_{E+E};\surd\!\!\surd \Leftrightarrow \Psi^{\leq^*}_{E};\surd\!\!\surd & \text{A3} & \Psi^{\leq^*}_{(E_1+E_2);E_3};\surd\!\!\surd \Leftrightarrow \Psi^{\leq^*}_{(E_1;E_3)+(E_2;E_3)};\surd\!\!\surd \\
\text{A4} & \Psi^{\leq^*}_{(E_1;E_2);E_3};\surd\!\!\surd \Leftrightarrow \Psi^{\leq^*}_{E_1;(E_2;E_3)};\surd\!\!\surd & \text{A5} & \Psi^{\leq^*}_{rec\ x.E};\surd\!\!\surd \Leftrightarrow \Psi^{\leq^*}_{E\{rec\ x.E/x\}};\surd\!\!\surd \\
\text{A6} & \Psi^{\leq^*}_{E+\delta};\surd\!\!\surd \Leftrightarrow \Psi^{\leq^*}_{E};\surd\!\!\surd & \text{A7} & \Psi^{\leq^*}_{\delta;E};\surd\!\!\surd \Leftrightarrow \Psi^{\leq^*}_{\delta};\surd\!\!\surd \\
\text{A8} & \Psi^{\leq^*}_{E;\epsilon};\surd\!\!\surd \Leftrightarrow \Psi^{\leq^*}_{E};\surd\!\!\surd & \text{A9} & \Psi^{\leq^*}_{\epsilon;E};\surd\!\!\surd \Leftrightarrow \Psi^{\leq^*}_{E};\surd\!\!\surd \\
\text{A10} & \Psi^{\leq^*}_{P};\surd\!\!\surd \Rightarrow \Psi^{\leq^*}_{\Omega};\surd\!\!\surd & \text{A11} & \Psi^{\leq^*}_{P+\Omega};\surd\!\!\surd \Rightarrow \Psi^{\leq^*}_{\tau;(P+\Omega)};\surd\!\!\surd \\
\text{A12} & \Psi^{\leq^*}_{\Omega};\surd\!\!\surd \Rightarrow \Psi^{\leq^*}_{\Omega;P};\surd\!\!\surd & \text{A13} & \Psi^{\leq^*}_{\mu;\tau};\surd\!\!\surd \Leftrightarrow \Psi^{\leq^*}_{\mu};\surd\!\!\surd \\
\text{A14} & \Psi^{\leq^*}_{\tau;E+E};\surd\!\!\surd \Leftrightarrow \Psi^{\leq^*}_{E};\surd\!\!\surd & \text{A15} & \Psi^{\leq^*}_{\mu;(P+\tau;Q)};\surd\!\!\surd \Leftrightarrow \Psi^{\leq^*}_{\mu;(P+\tau;Q)+\mu;Q}\surd\!\!\surd.
\end{array}
$$

The following theorem is immediate from Lemma 14 and the result shown in Aceto and Hennessy (1992) that the proof system for $\leq^*$ is complete with respect to $\mathrm{BPA}_\delta^{\epsilon,\Omega}$.

Theorem 9 (Completeness). If $E_1 \approx E_2$, then $\Psi^{\leq^*}_{E_1};\surd\!\!\surd \Leftrightarrow \Psi^{\leq^*}_{E_2};\surd\!\!\surd$.

For any process $P \in \mathrm{BPA}_\delta^{\epsilon,\Omega}$, we can prove the following result in a similar way to the proof of Theorem 8.

Theorem 10. For any $P \in \mathrm{BPA}_\delta^{\epsilon,\Omega}$, $Q \models en(\Psi^{\leq^*}_{P});\surd\!\!\surd$ if and only if $P \leq^* Q$.

7. Concluding remarks

In this paper, we first proved the definability of the non-deterministic choice '+' in FLC with respect to the observational semantics, and then established a connection between FLC and $\mathrm{BPA}_\delta^{\epsilon,\Omega}$. We also gave algorithms for constructing characteristic formulae of a context-free process up to $\leq$ and $\leq^*$ compositionally.

The significance of this work for the development of highly reliable software is obvious. The work of the current paper and that of Zhan and Wu (2005) has established some connections between the algebraic and logical approaches – in particular, connections with respect to the strong bisimulation semantics and the observational semantics, which are the most important semantics used in process algebra community.

By relating the constructs of $\mathrm{BPA}_\delta^{\epsilon,\Omega}$ to the connectives of FLC, we can obtain the compositionality of modal logics. So a complex system may be developed using modal logics but in a process algebra-like compositional manner. The advantages of compositionality can be seen from the example in Section 5. On the other hand, by constructing the characteristic formulae up to different semantics, we can reduce many verification problems arising in an algebraic setting to the corresponding logical setting.

As future work, we believe it will be worth investigating the parallel operator and establishing a proof system for FLC.

References

Abramsky, S. (1987) Observation equivalence as a testing equivalence. *Theoretical Computer Science* **53** 225–241.

Abramsky, S. (1991) A domain equation for bisimulation. *Information and Computation* **92** 161–218.

Aceto, L. and Hennessy, M. (1992) Termination, deadlock, and divergence. *Journal of ACM* **39** (1) 147–187.

Andersen, H. R., Stirling, C. and Winskel, G. (1994) A compositional proof system for the modal μ-calculus. *Proceedings of the 9th Annual IEEE Symposium on Logic in Computer Science*, IEEE Computer Society Press 144–153.

Barringer, H., Kuiper, R. and Pnueli, R. (1984) Now you may compose temporal logic specifications. *STOC '84: Proceedings of the sixteenth annual ACM symposium on theory of computing*, ACM 51–63.

Barringer, H., Kuiper, R. and Pnueli, R. (1985) A compositional temporal approach to a CSP-like language. In: Neuhold, E. J. and Chroust, G. (eds.) *Formal Models of Programming* (Proceedings of IFIP conference, The Role of Abstract Models in Information Processing), North Holland 207–227.

Bergstra, J. A. and Klop, J. W. (1985) Algebra of communication processes with abstraction. *Theoretical Computer Science* **37** 77–121.

Dutertre, B. (1995) Complete Proof Systems for First Order Interval Temporal Logic. In: *Proceedings 10th Annual IEEE Symposium on Logic in Computer Science (LICS'95)*, IEEE Computer Society 36–43.

Emerson, E. A. and Jutla, C. S. (1991) Tree automata, μ-calculus, and determinacy. In: *Proceedings 32nd Annual Symposium on Foundations of Computer Science (FOCS)*, IEEE Computer Society 368–377.

Gorrieri, R. and Rensink, A. (2001) Action refinement. *Handbook of Process Algebra*, Elsevier Science 1047–1147.

Graf, S. and Sifakis, J. (1986a) A modal characterization of observational congruence on finite terms of CCS. *Information and Control* **68** 125–145.

Graf, S. and Sifakis, J. (1986b) A logic for the description of non-deterministic programs and their properties. *Information and Control* **68** 254–270.

Hennessy, M. and Plotkin, G. (1980) Full abstraction for a simple parallel programming language. In: Proceedings of MFCS'80. *Springer-Verlag Lecture Notes in Computer Science* **74**.

Hoare, C. A. R. (1985) *Communicating Sequential Processes*, Prentice Hall.

Janin, D. and Walukiewicz, I. (1996) On the expressive completeness of the propositional μ-calculus with respect to monadic second order logic. In: Proceedings of CONCUR'96. *Springer-Verlag Lecture Notes in Computer Science* **1119** 263–277.

Kozen, D. (1983) Results on the propositional mu-calculus. *Theoretical Computer Science* **27** 333–354.

Lange, M. (2002) Local model checking games for fixed point logic with chop. In: Proceedings of CONCUR'02. *Springer-Verlag Lecture Notes in Computer Science* **2421** 240–254.

Lange, M. and Stirling, C. (2002) Model checking fixed point logic with chop. In: Proceedings of FOSSACS'02. *Springer-Verlag Lecture Notes in Computer Science* **2303** 250–263.

Larsen, K. G. and Liu, X. X. (1990) Equation solving using modal transition systems. In: *Proceedings of the Fifth Annual IEEE Symposium on Logic in Computer Science (LICS 1990)*, IEEE Computer Society 108–107.

Larsen, K. G. and Thomsen, B. (1988) A modal process logic. In: *Proceedings of the Third Annual Symposium on Logic in Computer Science, LICS '88*, IEEE Computer Society 203–210.

Majster-Cederbaum, M. and Salger, F. (2004) Towards the hierarchical verification of reactive systems. *Theoretical Computer Science* **318** (3) 243–296.

Milner, R. (1981) A modal characterization of observable machine-behavior. In: Proceedings of CAAD'81. *Springer-Verlag Lecture Notes in Computer Science* **112** 23–34.

Milner, R. (1989) *Communication and Concurrency*, Prentice Hall.

Moszkowski, B. (1986) *Executing Temporal Logic Programms*, Cambridge University Press.

Müller-Olm, M. (1999) A modal fixpoint logic with chop. In: Proceedings of STACS'99. *Springer-Verlag Lecture Notes in Computer Science* **1563** 510–520.

Paige, R. and Tarjan, R. (1987) Three partition refinement algorithms. *SIAM Journal on Computing* **16** (6) 973–989.

Pnueli, A. (1977) The temporal logic of programs. In: *Proceedings 18th Annual Symposium on Foundations of Computer Science (FOCS 1977)*, IEEE Computer Science Society 46–57.

Roscoe, A. W. (1997) *The Theory and Practice of Concurrency*, Prentice Hall.

Rosner, R. and Pnueli, A. (1986) A choppy logic. In: *Proceedings of LICS'86*, IEEE Computer Science Society 306–313.

Steffen, B. and Ingólfsdóttir, A. (1994) Characteristic formulae for processes with divergence. *Information and Computation* **110** 149–163.

Stirling, C. (2001) *Modal and Temporal Logics for Processes*, Springer-Verlag.

Tarski, A. (1955) A lattice-theoretical fixpoint theorem and its application. *Pacific J. Math.* **5** 285–309.

van Glabbeek, R. (2001) The linear time vs branching time spectrum I: The semantics of concrete, sequential processes. In: Bergstra, J. A., Ponse, A. and Smolka, S. A. (eds.) *Handbook of Process Algebra*, Elsevier 3–99.

Zhan, N. (2006) Connecting algebraic and logical descriptions of concurrent systems. In: Margaria, T., Phillipou, A. and Steffen, B (eds.) *Proceedings of the Second International Symposium on Leveraging Applications of Formal Methods, Verification and Validation (ISOLA '06)*, IEEE Computer Society Press 383–391.

Zhan, N. and Majster-Cederbaum, M. (2005) Deriving nondeterminism from conjunction and disjunction. In: proceedings of FORTE'05. *Springer-Verlag Lecture Notes in Computer Science* **3731** 351–365.

Zhan, N. and Wu, J. (2005) Compositionality of fixpoint logic with chop. In: proceedings of ICTAC'05. *Springer-Verlag Lecture Notes in Computer Science* **3722** 136–150.

Zhou, C., Hoare, C. A. R. and Ravn, A. (1991) A calculus of durations. *Information Processing Letters* **40** (5) 269–276.