A Fixpoint Semantics of Event Systems with and without Fairness Assumptions

Hector Ruiz Barradas, Didier Bert

IMAG

Institut d'Informatique et de Mathématiques Appliquées de Grenoble

LSR
Laboratoire Logiciels, Systèmes, Réseaux

RAPPORT DE RECHERCHE

A Fixpoint Semantics of Event Systems with and without Fairness Assumptions

Héctor Ruíz Barradas[1,2] and Didier Bert[2]

[1] Universidad Autónoma Metropolitana Azcapotzalco, México D. F., México
hrb@correo.azc.uam.mx, Hector.Ruiz@imag.fr
[2] Laboratoire Logiciels, Systèmes, Réseaux - LSR-IMAG - Grenoble, France
Didier.Bert@imag.fr

RR 1081-I LSR 21 Décembre 2005

B.P. 72 - 38402 SAINT MARTIN D'HERES CEDEX - France

Centre National de la Recherche Scientifique
Institut National Polytechnique de Grenoble
Université Joseph Fourier Grenoble I

A Fixpoint Semantics of Event Systems with and without Fairness Assumptions

Abstract

We present a fixpoint semantics of event systems. The semantics is presented in a general framework without concerns of fairness. Soundness and completeness of rules for deriving *leads-to* properties are proved in this general framework. The general framework is instantiated to minimal progress and weak fairness assumptions and similar results are obtained. We show the power of these results by deriving sufficient conditions for *leads-to* under minimal progress proving soundness of proof obligations without reasoning over state-traces.

Keywords

Liveness properties, event systems, action systems, UNITY logic, fairness, weak fairness, minimal progress, set transformer, fixpoints.

Résumé

Dans ce rapport nous présentons une sémantique de point fixe pour les systèmes d'événements. La sémantique est présentée dans un cadre générale sans considérations d'équité. La cohérence et la complétude des règles pour dériver des propriétés *leads-to* est prouvée dans ce cadre général. Le cadre général est instancié avec des hypothèses de progrès minimal et d'équité faible, et des résultats similaires sont prouvés. Nous montrons la puissance de ces résultats par la dérivation de conditions suffisantes pour des propriétés *leads-to* sous l'hypothèse de progrès minimal, et nous prouvons la cohérence de ces règles sans raisonner sur les traces d'états.

Mots-clés

Propriétés de vivacité, système d'événements, systèmes d'actions, logique UNITY, équité, équité faible, progrès minimal, transformateurs d'ensembles, point fixes.

Table of Contents

1 Introduction

Action systems, or event systems, are useful abstractions to model discrete systems. Many formalisms have been proposed to model action systems. In these formalisms, the behavior of a system is described in terms of observations about its state, and they are known as *state based* formalisms. As examples of state based formalisms we can cite Back's action system formalism [3] and UNITY [5]. All of these formalisms have a common aspect: their semantics is founded on state-traces of transition systems.

State traces of transitions systems impose an operational reasoning about the behavior of a system. However this operational behavior can be hidden by using temporal logic to specify safety and liveness properties. Semantics of temporal formulas is given by state-traces of transition systems. A proof system allows us to derive properties from other proved properties without an operational reasoning, only by symbolic calculations. Soundness and completeness of the logic are established by proofs relating logical formulas with assertions about state-traces. So at this point, we come back to operational reasoning about the transition systems.

A more abstract possibility to define the semantics of action systems is to base it on fixpoints of set (or predicates) transformers. Inspired from [2] and [8], we characterize certain liveness properties as fixpoints of set transformers modeling iteration of events, under minimal progress or weak fairness assumptions. We are only interested in properties of type P *leads-to* Q, where P and Q are predicates on the state space of a system, with the informal meaning: "the system *reaches* a state satisfying Q when its execution arrives at any state in P". The fixpoint characterizing this property denotes the largest subset of states, containing all states satisfying P, where *termination* of iteration of events in the system, is guaranteed to terminate in a state satisfying Q. Soundness and completeness of rules allowing derivation of *leads-to* properties is proved by demonstrating that notions of reachability and termination are equals under minimal progress or weak fairness. Moreover, we give two examples of applications of these results: The first one is a proof of sufficient conditions for liveness properties under minimal progress given in [2]. The second one is an original result which gives sufficient conditions to derive a liveness property under minimal progress when the given property holds under weak fairness.

This report is an extended version of the semantics of event systems presented in [11]. In particular all proofs of that paper are given here in an explicit way, and a new section, considering the semantics with the strongest invariant, is presented. Paper [11] presents comparisons with other works dealing with fairness properties. This part is not given here. The report is structured as follows. In Section 2, we present a system as a set transformer and we give syntax and semantics of common set transformers used to model events, or actions, in the system. Moreover we give a brief review of liveness properties in UNITY logic to specify properties of an event system. In Section 3, we develop our semantics of event systems and we prove equality (soundness and completeness) between notions of termination and reachability. In Section 4, we give examples of sufficient conditions to derive liveness properties using the results of the previous section. Finally we give our conclusions and future work in Section 5. Annex A presents the proof of the *leads-to* properties as a relation between predicates or sets. Annex B shows the extension of the semantics to consider the strongest invariant. Annexes C, D and E present the proofs of sections 3 and 4.

2 Set Transformers and UNITY Logic in Event Systems

In this section we introduce the main considerations about event systems and the specification of liveness properties in UNITY logic. This section is divided in two parts. The first part presents an event system as a set transformer and introduces the notion of liberal set transformer, as well as the dovetail operator that is used to model a weak fairness assumption. In the second part we recall the main ideas in the specification and proof of liveness properties under two fairness assumptions in UNITY-like logic.

2.1 Set Transformers

A set transformer is a total function of type $\mathbb{P}(\mathcal{U}) \to \mathbb{P}(\mathcal{U})$ for a certain set $\mathcal{U}$. An event system is made out of a family of events. Any event may be executed in any state where its *guard*, boolean condition on the state, holds. When the guard of an event holds, we say that the event is enabled. As in event-B systems, we considered a system with state variable x and invariant I. The state space u of the system is the set of states where I holds: $u = \{\, z \mid I(z) \,\}$. Therefore events in the system are modeled by conjunctive set transformers E_i of type $\mathbb{P}(u) \to \mathbb{P}(u)$, where i belongs to certain finite index set L. Consequently, the system is modeled by a conjunctive set transformer S which is the bounded choice of events E_i: $S = [\!]_{i \in L}\ E_i$. We denote by $\mathcal{S}$ the set of events in S: $\mathcal{S} = \{E_i \mid i \in L\}$.

For any set transformer T of type $\mathbb{P}(u) \to \mathbb{P}(u)$ and subset r of u, $T(r)$ denotes the largest subset of states where execution of T must begin in order for T to terminate in a state belonging to r [1]. Primitive set transformers considered in this paper are similar to the primitive generalized substitutions in B: skip, bounded choice, sequence, guarded and conditioned set transformer. Following the work reported in [12], for any set transformer T, and subset r of u, we denote by $\mathcal{L}(T)(r)$ the *liberal set transformer* of T, which denotes the largest subset of states where the execution of S must begin in order for T to terminate in a state belonging to r or loop. Common set transformers and liberal set transformers are defined as follows:[1]

$$(\mathcal{L})(\mathit{skip})(r) = r \qquad (\mathcal{L})(F\ ;\ G)(r) = (\mathcal{L})(F)((\mathcal{L})(G)(r))$$
$$(\mathcal{L})(F\ [\!]\ G)(r) = (\mathcal{L})(F)(r) \cap (\mathcal{L})(G)(r) \qquad (\mathcal{L})(p \Longrightarrow F)(r) = \overline{p} \cup (\mathcal{L})(F)(r)$$

In the guarded event, $\overline{p}$ denotes $u - p$. For the preconditioned event we have:

$$(p \mid F)(r) = p \cap F(r)$$
$$\mathcal{L}(p \mid F)(r) = \begin{cases} p \cap \mathcal{L}(F)(r) & \text{if } r \neq u \\ \mathcal{L}(F)(r) & \text{if } r = u \end{cases}$$

Definitions of liberal set transformers presented here are the set counterpart of definitions in [6]. The set transformers $F(r)$ and $\mathcal{L}(F)(r)$ for event F and postcondition r are related by the pairing condition:

$$F(r) = \mathcal{L}(F)(r) \cap \mathsf{pre}(F)$$

where $\mathsf{pre}(F)$, the termination set of F, is equal to $F(u)$. From the pairing condition, we conclude:

$$F(u) = u \Rightarrow F(r) = \mathcal{L}(F)(r)$$

[1] For any set transformer T, $(\mathcal{L})(T)(r)$ denotes definition for the set $T(r)$ or the set $\mathcal{L}(T)(r)$.

We say that a set transformer F is *strict* when it respects the excluded miracle law:

$$F(\varnothing) = \varnothing$$

For any set transformer F, when $F(r)$ or $\mathcal{L}(F)(r)$ are recursively defined:

$$F(r) = \mathcal{F}(F(r)) \quad \text{or} \quad \mathcal{L}(F)(r) = \mathcal{G}(\mathcal{L}(F)(r))$$

for monotonic functions $\mathcal{F}$ and $\mathcal{G}$, according to [7] we take $F(r)$ as the strongest solution of the equation $X = \mathcal{F}(X)$ and $\mathcal{L}(F)(r)$ as the weakest solution of the equation $X = \mathcal{G}(X)$. As these solutions are fixpoints, we take $F(r)$ as the least fixpoint of $\mathcal{F}$ ($\mathsf{fix}(\mathcal{F})$) and $\mathcal{L}(F)(r)$ as the greatest fixpoint of $\mathcal{G}$ ($\mathsf{FIX}(\mathcal{G})$).

The Dovetail Operator To model a weak fairness assumption, we use the dovetail operator $\triangledown$ [4], which is a fair nondeterministic choice operator. The dovetail operator is used to model the notion of fair scheduling of two activities. Let A and B be these activities, then the operational meaning of the construct $A \triangledown B$ denotes the execution of commands A and B fairly in parallel, on separate copies of the state, accepting as an outcome any proper, nonlooping, outcome of either A or B. The fair execution of A and B means that neither computation is permanently neglected if favor of the other.

The semantic definition for dovetail operator in [4] is given by definition of its weakest liberal precondition predicate transformer (*wlp*) and its termination predicate *hlt*. We give an equivalent definition using the weakest liberal set transformer $\mathcal{L}$ and its termination set pre:

$$\mathcal{L}(F \triangledown G)(r) = \mathcal{L}(F)(r) \cap \mathcal{L}(G)(r) \tag{1}$$

$$\mathsf{pre}(F \triangledown G) = (F(u) \cup G(u)) \cap (\overline{F(\varnothing)} \cup G(u)) \cap (\overline{G(\varnothing)} \cup F(u)) \tag{2}$$

We remember that $\mathsf{grd}(F) = \overline{F(\varnothing)}$. From these definitions, in [12] we prove the guard property of the dovetail: $\mathsf{grd}(A \triangledown B) = \mathsf{grd}(A) \cup \mathsf{grd}(B)$.

A motivating example of the use of the dovetail operator is given in [4]. In that example the recursive definition: $X = (n := 0 \triangledown (X \,;\, n := n + 1))$ which has as solution "set n to any natural number", is contrasted with the recursion $Y = (n := 0 \,[\!]\, (Y \,;\, n := n + 1))$ which has as solution "set n to any natural number or loop". The possibility of loop in X is excluded with the dovetail operator because the fair choice of statement $n := 0$ will certainly occur. In Y the execution of that statement is not ensured.

2.2 Liveness Properties in event systems

In this section we give a brief summary of some results in the specification and proof of liveness properties presented in [13], [14] and [12]. In these works, we propose the use of UNITY logic to specify and prove liveness properties in event-B systems.

Liveness properties are divided in two groups: basic and general liveness properties. Each one of these properties are specified by relations on the state of the system. In order to specify and prove these properties we consider a minimal progress or a weak fairness assumption.

Basic Properties under Weak Fairness A weak fairness assumption states that any continuously enabled event is infinitely often executed. For any event G in the set $\mathcal{S}$, we write $G \cdot P \gg_w Q$ (pronounce "by event G, P ensures Q") to specify that by the execution of event G in a state satisfying P the system goes to another state satisfying Q, under a weak

fairness assumption. In [14] we propose sufficient conditions WF0 and WF1, to guarantee the intended meaning of these properties. These conditions were stated in terms of predicates, but we present them as set expression:

$$p \cap \overline{q} \subseteq S(p \cup q) \cap \mathsf{grd}(G) \cap G(q) \Rightarrow G \cdot x \in p \gg_w x \in q \tag{3}$$

where x is the state variable of S, $p = \{z | z \in u \wedge P\}$ and $q = \{z | z \in u \wedge Q\}$ for certain predicates P and Q.

Basic Properties under Minimal Progress In a minimal progress assumption, if two or more statements are enabled in a given state, the selection of the statement enabled for execution is non-deterministic. We write $P \gg_m Q$ (pronounce "P ensures Q") to specify that execution of any event of S, in a state satisfying P, terminates into a state establishing Q. In [13] we give sufficient conditions MP0 and MP1 to prove basic properties under minimal progress. We present them as a set expression as follows, for sets p and q defined as above:

$$p \cap \overline{q} \subseteq S(q) \cap \mathsf{grd}(S) \Rightarrow x \in p \gg_m x \in q \tag{4}$$

General Properties General liveness properties are specified by the *leads-to* operator $\rightsquigarrow$. Depending on the fairness assumption considered, we have general liveness properties under minimal progress or weak fairness assumptions. However, the *leads-to* relation is defined in the same way as the closure relation, containing the base relation and it is both transitive and disjunctive. A property $P \rightsquigarrow Q$ holds in an event system, if it is derived by a finite number of applications of the rules defined by the UNITY theory:

	ANTECEDENT	CONSEQUENT
BRL	$P \gg Q$	$P \rightsquigarrow Q$
TRA	$P \rightsquigarrow R$, $R \rightsquigarrow Q$	$P \rightsquigarrow Q$
DSJ	$\forall i \cdot (i \in I \Rightarrow P(i) \rightsquigarrow Q)$	$\exists i \cdot (i \in I \wedge P(i)) \rightsquigarrow Q$

$P \gg Q$, in the BRL rule stands for the basic liveness property $G \cdot P \gg_w Q$ for some G in $\mathcal{S}$ in case where we consider a property under a weak fairness assumption or $P \gg_m Q$, in the case where we consider a minimal progress assumption. In the disjunction rule DSJ, I is any index set.

3 Reachability and Termination

In this section, we prove soundness and (relative) completeness of rules BRL, TRA and DSJ for general liveness properties under minimal progress and weak fairness assumptions in event systems. These rules are sound if for any property $P \rightsquigarrow Q$, iteration of events, under minimal progress or weak fairness assumptions, starting in a state satisfying P, leads to a state in the system where Q holds. Completeness of these rules is proved by showing that $P \rightsquigarrow Q$ can be derived from the fact that any iteration of events, starting in a state where P holds, terminates into a state satisfying Q.

We do not expect that any iteration of events in a system terminates into a state where the guards of every event are disabled. However we can model an iteration of events which *always* terminates in a certain state by supposing, just for the reasoning, that the events

in the system are embedded in a certain guarded event which models the iteration under a fairness assumption. The iteration only proceeds when the guard of that event is enabled. *Termination* of the iteration will be in a state where the guard does not hold. In this way, if the guard of the iteration is $\neg Q$, and the iteration starts in a state where P holds, the system reaches a state where Q holds. *Reachability* from P to Q is then associated to termination of the iteration of events. In the following subsection, we formalize our claims in a general framework without concerns of fairness, and then we particularize these results to minimal progress or weak fairness assumptions in other two subsections.

To simplify matters, the strongest invariant [15] is not considered in definitions of this section. Therefore, instead of implications in proof obligations (3) and (4) used to prove basic liveness properties under weak fairness or minimal progress assumption respectively, we consider them as definitions. In annex B we restate the results given in this section to consider the strongest invariant and we consider again, proof obligations (3) and (4) as implications, as they are stated.

3.1 A General Framework

In this subsection we define a set transformer to model iteration of events and we state its main characteristics. We use this set transformer to define the *termination* relation. Then we give a representation of *leads to* relation in UNITY logic as a relation between subsets of u and we use it to define the *reachability* relation. Finally we prove that the *termination* and the *reachability* relations are equal.

3.1.1 Termination We consider a set transformer W which models a *step* of the iteration of events in a system S. At this time we cannot define the meaning of such a step, however we need two properties of W: it must be *monotonic* and *strict*. When we particularize the iteration under a fairness assumption, the meaning of W will be given in terms of S. For any r in $\mathbb{P}(u)$, $W(r)$ denotes the largest subset of states where the execution of W must begin in order for W to terminate in a state belonging to r.

To model the iteration of events until the system reaches a state in a certain set r in $\mathbb{P}(u)$, we define a guarded event $\mathcal{F}(r)$:

$$\mathcal{F}(r) = (\overline{r} \Longrightarrow W) \tag{5}$$

for any $r \in \mathbb{P}(u)$, which allows iteration of W when the system stays in any state in $\overline{r}$. Iteration of $\mathcal{F}(r)$ is modeled by the $\widehat{\ }$ operator $\mathcal{F}(r)\widehat{\ }$. As this operator has a recursive definition:

$$\mathcal{F}(r)\widehat{\ } = (\mathcal{F}(r)\ ;\ \mathcal{F}(r)\widehat{\ }) \ [\!]\ \mathit{skip}$$

the set where termination of $\mathcal{F}(r)\widehat{\ }$ is guaranteed ($\mathsf{pre}(\mathcal{F}(r)\widehat{\ })$) is given by $\mathsf{fix}(\mathcal{F}(r))$ [1].

As W may model an unbounded non determinist set transformer, we use the *Generalized Limit Theorem* to formally justify that any iteration of $\mathcal{F}(r)$ starting in $\mathsf{pre}(\mathcal{F}(r)\widehat{\ })$ terminates in some state of r. This theorem characterizes the least fixpoint of monotonic functions as an infinite join. We use the version presented in [9], particularizing the theorem to monotonic set transformers. The theorem is as follows:

Theorem 1. (Generalized Limit Theorem)
Let f be a monotonic set transformer, and let f^α, for ordinal α, be defined inductively by

$$f^\alpha = \bigcup \beta \cdot (\beta < \alpha \mid f(f^\beta)) \tag{6}$$

Then $\mathsf{fix}(f) = f^\alpha$ for some ordinal α.

The proof of this theorem is given in [9]. It states that we can choose any ordinal γ, such that $\gamma > \mathsf{card}(\mathsf{dom}(f))$, and then we must have $f^\alpha = f^\beta$ for some $\alpha < \beta < \gamma$. Then it is proved that the common value of f^α and f^β is the least fixpoint of f.

As W is a monotonic function, $\mathcal{F}(r)$ (5) is monotonic, and theorem 1 can be applied to calculate the least fixpoint of $\mathcal{F}(r)$. According to the theorem, we conclude that $\mathcal{F}(r)^0 = \varnothing$ and $\mathcal{F}(r)^1 = r$ *because* W is strict. Moreover, for any ordinal α, $\mathcal{F}(r)^{\alpha+1} = \mathcal{F}(r)(\mathcal{F}(r)^\alpha)$ and $\mathcal{F}(r)^\alpha \subseteq \mathcal{F}(r)^{\alpha+1}$. This fact formally supports our claim that the termination set of $\mathcal{F}(r)^\frown$, contains states where any iteration of $\mathcal{F}(r)$ terminates in a state into r. Now, we can define the *termination* relation $\mathcal{T}$ as follows:

Definition 1. (Termination Relation)

$$\mathcal{T} = \{\, a \mapsto b \mid a \subseteq u \wedge b \subseteq u \wedge a \subseteq \mathit{fix}(\mathcal{F}(b)) \,\} \tag{7}$$

3.1.2 Reachability As presented in section 2.2, *leads-to* relation of UNITY logic is defined as a relation between predicates on the state of programs. In this section we define a similar relation, $\pounds$, but instead of predicates, we define it as a relation between subsets of states in u ($\pounds \subseteq \mathbb{P}(u) \times \mathbb{P}(u)$). Any pair $a \mapsto b$ in $\pounds$ indicates that the system reaches a state in b, when its execution arrives at any state in a. For this reason we name $\pounds$ as the *reachability* relation.

Definition of $\pounds$ is given by induction. The base case needs definition of the basic relation $\mathcal{E}$. At this time $\mathcal{E}$ cannot be defined. As indicated in section 2.2, basic liveness properties depend on fairness assumptions. $\mathcal{E}$ will be defined in the following sections according to minimal progress or weak fairness assumptions. However, these definitions must satisfy two requirements. The first requirement is as follows: If $a \subseteq b$, for any a and b in $\mathbb{P}(u)$, then $a \mapsto b \in \mathcal{E}$ must hold. The second requirement relates $\mathcal{E}$ with the set transformer W: For any ordered pair $a \mapsto b \in \mathcal{E}$, the inclusion $a \cap \overline{b} \subseteq W(b)$ must hold. This inclusion indicates that any execution of W starting in $a \cap \overline{b}$, terminates into a state of b.

Definition 2. (Reachability Relation)
The reachability *relation* $\pounds$, $\pounds \in \mathbb{P}(u) \leftrightarrow \mathbb{P}(u)$, *is defined by the following induction scheme:*
(**SBR**)*:* $\mathcal{E} \subseteq \pounds$
(**STR**)*:* $\pounds \,;\, \pounds \subseteq \pounds$
(**SDR**)*:* $\forall (q, l) \cdot (q \in \mathbb{P}(u) \wedge l \subseteq \mathbb{P}(u) \Rightarrow (l \times \{q\} \subseteq \pounds \Rightarrow \bigcup(l) \mapsto q \in \pounds))$
Closure*:* $\forall l' \cdot (l' \in u \leftrightarrow u \wedge \mathcal{E} \subseteq l' \wedge l' \,;\, l' \subseteq l' \wedge$
$\forall (q, l) \cdot (q \in \mathbb{P}(u) \wedge l \subseteq \mathbb{P}(u) \wedge l \times \{q\} \subseteq l' \Rightarrow \bigcup(l) \mapsto q \in l') \Rightarrow \pounds \subseteq l')$

$\bigcup(l)$ in the SDR rule and the closure clause, denotes the generalized union of subsets in l. Rules SBR, STR and SDR are the set counterpart of the basic rule for *leads-to* BRL, transitivity rule TRA and disjunction rule DSJ respectively, as defined in section 2.2.

In order to connect $\pounds$ with the *leads-to* relation of UNITY logic, we have the following equivalence:

$$P(x) \rightsquigarrow Q(x) \equiv \{\, z \mid z \in u \wedge P(z) \,\} \mapsto \{\, z \mid z \in u \wedge Q(z) \,\} \in \pounds \tag{8}$$

We note that property $P \rightsquigarrow Q$ in UNITY is equivalent to $P \wedge I \rightsquigarrow Q \wedge I$, considering I as an invariant of S, because the *leads-to* relation is defined in states reachable from the initial conditions [15]. The proof of this equivalence is given in annex A.

3.1.3 Soundness and Completeness We are now ready to state our main theorem, formally indicating that *termination* and *reachability* relations are equal:

Theorem 2. (Soundness and Completeness)
Let W be a monotonic and strict set transformer and $\mathcal{F}(r) = (\overline{r} \Longrightarrow W)$ for any r in $\mathbb{P}(u)$. Let relations $\mathcal{T}$ and $\mathcal{L}$ be defined as definitions 1 and 2 respectively. Considering (a) $a \mapsto b \in \mathcal{E} \Rightarrow a \cap \overline{b} \subseteq W(b)$, (b) $a \subseteq b \Rightarrow a \mapsto b \in \mathcal{E}$ and (c) $W(r) \mapsto r \in \mathcal{L}$, for any a, b and r in $\mathbb{P}(u)$, the following equality holds:

$$\mathcal{L} = \mathcal{T}$$

Premise (a) and (b) were commented in the previous section. Premise (c) asserts that any set r is reached from the set $W(r)$ which is the largest subset of states where a step of the iteration terminates in r.

The proof of this theorem is given in two parts: first we prove the inclusion $\mathcal{L} \subseteq \mathcal{T}$ and then $\mathcal{T} \subseteq \mathcal{L}$.

Proof of $\mathcal{L} \subseteq \mathcal{T}$ The proof of this inclusion follows from the closure clause in definition 2, particularizing the quantified variable l' to relation $\mathcal{T}$. Then $\mathcal{L} \subseteq \mathcal{T}$ follows from $\mathcal{E} \subseteq \mathcal{T}$, $\mathcal{T};\mathcal{T} \subseteq \mathcal{T}$ and $l \times \{q\} \subseteq \mathcal{T} \Rightarrow \bigcup(l) \mapsto q \in \mathcal{T}$ for any l in $\mathbb{P}(\mathbb{P}(u))$ and q in $\mathbb{P}(u)$.

The proof of $\mathcal{E} \subseteq \mathcal{T}$ uses the following property for monotonic function f and iteration defined in (6):

$$\forall \alpha \cdot (f^{\alpha} \subseteq \mathsf{fix}(f)) \tag{9}$$

which is easily proved by transfinite induction; the proof is given in appendix C. The proof of $\mathcal{E} \subseteq \mathcal{T}$ is given by the proof of $a \mapsto b \in \mathcal{E} \Rightarrow a \mapsto b \in \mathcal{T}$:

1. $a \mapsto b \in \mathcal{E}$	; premise
2. $a \cap \overline{b} \subseteq W(b)$	; 1 and hyp. (a)
3. $a \subseteq \mathcal{F}(b)(b)$	; 2 and def. (5)
4. $a \subseteq \mathcal{F}(b)^2$	; 3 and iterate (6)
5. $a \subseteq \mathsf{fix}(\mathcal{F}(b))$	; 4 and (9)
6. $a \mapsto b \in \mathcal{T}$	; 5 and def. (7)

In order to prove the transitivity of $\mathcal{T}$, we need the following property:

$$a \mapsto b \in \mathcal{T} \Rightarrow \mathsf{fix}(\mathcal{F}(a)) \subseteq \mathsf{fix}(\mathcal{F}(b)) \tag{10}$$

for any a and b in $\mathbb{P}(u)$. Taking $a \mapsto b \in \mathcal{T}$ as a premise, and considering $\mathsf{fix}(\mathcal{F}(a))$ as the least fixpoint of $\mathcal{F}(a)$, in order to prove property (10) it suffices to prove $\mathcal{F}(a)(\mathsf{fix}(\mathcal{F}(b))) \subseteq \mathsf{fix}(\mathcal{F}(b))$, which follows directly from $a \mapsto b \in \mathcal{T}$ and $\mathcal{F}(b)(\mathsf{fix}(\mathcal{F}(b))) = \mathsf{fix}(\mathcal{F}(b))$. Now the proof of $\mathcal{T}\ ;\ \mathcal{T} \subseteq \mathcal{T}$ is equivalent to prove $a \mapsto b \in \mathcal{T}\ ;\ \mathcal{T} \Rightarrow a \mapsto b \in \mathcal{T}$ for any a and b in $\mathbb{P}(u)$:

1. $\exists c \cdot (a \mapsto c \in \mathcal{T} \wedge c \mapsto b \in \mathcal{T})$	; from $a \mapsto b \in \mathcal{T};\mathcal{T}$
2. $\exists c \cdot (a \subseteq \mathsf{fix}(\mathcal{F}(c)) \wedge c \mapsto b \in \mathcal{T})$	; 1 and def. $\mathcal{T}$
3. $\exists c \cdot (a \subseteq \mathsf{fix}(\mathcal{F}(c)) \wedge \mathsf{fix}(\mathcal{F}(c)) \subseteq \mathsf{fix}(\mathcal{F}(b)))$	; 2 and (10)
4. $a \subseteq \mathsf{fix}(\mathcal{F}(b))$	; 3
5. $a \mapsto b \in \mathcal{T}$	; 6 and def. $\mathcal{T}$

Finally, the proof of $l \times \{q\} \subseteq \mathcal{T} \Rightarrow \bigcup(l) \mapsto q \in \mathcal{T}$ is as follows:

1. $l \times \{q\} \subseteq \mathcal{T}$	; premise
2. $\forall p \cdot (p \in l \Rightarrow p \mapsto q \in \mathcal{T})$	; 1
3. $\forall p \cdot (p \in l \Rightarrow p \subseteq \mathsf{fix}(\mathcal{F}(q)))$	; 2 and def. $\mathcal{T}$
4. $\bigcup(l) \subseteq \mathsf{fix}(\mathcal{F}(q))$	; 3
5. $\bigcup(l) \mapsto q \in \mathcal{T}$	; 4 and def. $\mathcal{T}$

This last deduction concludes the proof of $\mathcal{L} \subseteq \mathcal{T}$.

Proof of $\mathcal{T} \subseteq \mathcal{L}$ The proof of this inclusion requires the following property:

$$\forall r \cdot (r \in \mathbb{P}(u) \Rightarrow \mathcal{F}(r)^\alpha \mapsto r \in \mathcal{L}) \quad \text{for any ordinal } \alpha \tag{11}$$

The proof of (11) is done by transfinite induction. For a successor ordinal we need to prove $\mathcal{F}(r)^\alpha \mapsto r \in \mathcal{L} \Rightarrow \mathcal{F}(r)^{\alpha+1} \mapsto r \in \mathcal{L}$; this proof is given in appendix C. For a limit ordinal we prove $\forall \beta \cdot (\beta < \alpha \Rightarrow \mathcal{F}(r)^\beta \mapsto r \in \mathcal{L}) \Rightarrow \mathcal{F}(r)^\alpha \mapsto r \in \mathcal{L}$:

1. $\forall \beta \cdot (\beta < \alpha \Rightarrow \mathcal{F}(r)^\beta \mapsto r \in \mathcal{L})$	; ind. hyp.
2. $\forall \beta \cdot (\beta < \alpha \Rightarrow W(\mathcal{F}(r)^\beta) \mapsto \mathcal{F}(r)^\beta \in \mathcal{L})$	; from hyp. (c)
3. $\forall \beta \cdot (\beta < \alpha \Rightarrow W(\mathcal{F}(r)^\beta) \mapsto r \in \mathcal{L})$	; 2, 1 and STR
4. $r \mapsto r \in \mathcal{L}$	; hyp. (b) and SBR
5. $\forall \beta \cdot (\beta < \alpha \Rightarrow r \cup W(\mathcal{F}(r)^\beta) \mapsto r \in \mathcal{L})$	; 4, 3 and SDR
6. $\forall \beta \cdot (\beta < \alpha \Rightarrow \mathcal{F}(r)(\mathcal{F}(r)^\beta) \mapsto r \in \mathcal{L})$	; def. $\mathcal{F}(r)$ and 5
7. $\bigcup \beta \cdot (\beta < \alpha \mid \mathcal{F}(r)(\mathcal{F}(r)^\beta)) \mapsto r \in \mathcal{L}$	; 6 and SDR
8. $\mathcal{F}(r)^\alpha \mapsto r \in \mathcal{L}$	; 7 and def. iterate

Using (11), we prove $\mathcal{T} \subseteq \mathcal{L}$ by the proof of $a \mapsto b \in \mathcal{T} \Rightarrow a \mapsto b \in \mathcal{L}$ for any a and b in $\mathbb{P}(u)$ as follows:

1. $a \subseteq \mathsf{fix}(\mathcal{F}(b))$	; from $a \mapsto b \in \mathcal{T}$
2. $\exists \alpha \cdot (a \subseteq \mathcal{F}(b)^\alpha)$	; 1 and theorem 1
3. $\exists \alpha \cdot (a \mapsto \mathcal{F}(b)^\alpha \in \mathcal{L})$	; 2, (b) and SBR
4. $\exists \alpha \cdot (a \mapsto \mathcal{F}(b)^\alpha \in \mathcal{L} \wedge \mathcal{F}(b)^\alpha \mapsto b \in \mathcal{L})$	; 3 and (11)
5. $a \mapsto b \in \mathcal{L}$	; 4 and STR

This deduction concludes the proof of theorem 2.

3.2 Minimal Progress

In this paragraph we define the *termination* and *reachability* relations under minimal progress and we prove that they satisfy the premises of theorem 2. Therefore we claim that relations $\mathcal{T}$ and $\mathcal{L}$ are equal in the case of minimal progress.

3.2.1 Termination under MP To model a step of the iteration of events of system S under minimal progress assumptions, we note that if we need to establish a certain postcondition when this step is achieved, any event in S must be able to establish the postcondition. Moreover, as we are interested in the execution of any event, we need to start the execution step in a state satisfying the guard of at least one event. Therefore, taking into account these considerations, we propose the following preconditioned set transformer:

$$W_m = \mathsf{grd}(S) \mid S \tag{12}$$

From definition of preconditioned set transformer in Section 2.1 we actually have that $W_m(r) = \mathsf{grd}(S) \cap S(r)$. From monotonicity of S , we derive the monotonicity of W_m and $W_m(\varnothing) = (\mathsf{grd}(S) \cap S(\varnothing)) = \varnothing$ which proves the strictness of W_m.

The body of the iteration of events under minimal progress is the guarded event $\mathcal{F}_m(r)$ defined as follows:

$$\mathcal{F}_m(r) = \overline{r} \Longrightarrow W_m \tag{13}$$

Definition of the *termination* relation under minimal progress is given by all ordered pairs $a \mapsto b$ satisfying $a \subseteq \mathsf{pre}(\mathcal{F}_m(b)^\frown)$:

$$\mathcal{T}_m = \{\, a \mapsto b \,|\, a \subseteq u \wedge b \subseteq u \wedge a \subseteq \mathsf{fix}(\mathcal{F}_m(b)) \,\} \tag{14}$$

3.2.2 Reachability under MP The basic relation under minimal progress contains all ordered pairs $a \mapsto b$ from which we can derive a property $x \in a \gg_m x \in b$ (4):

$$\mathcal{E}_m = \{\, a \mapsto b \,|\, a \subseteq u \wedge b \subseteq u \wedge a \cap \overline{b} \subseteq S(b) \cap \mathsf{grd}(S) \,\} \tag{15}$$

From definitions of $\mathcal{E}_m$ and W_m, the proof of premise (a) of theorem 2 follows for the case of minimal progress $a \mapsto b \in \mathcal{E}_m \Rightarrow a \cap \overline{b} \subseteq W_m(b)$:

1. $a \mapsto b \in \mathcal{E}_m$	; premise
2. $a \cap \overline{b} \subseteq \mathsf{grd}(S) \cap S(b)$	; 1 and def. (15)
3. $a \cap \overline{b} \subseteq (\mathsf{grd}(S) \mid S)(b)$	; 2 and set transf.
4. $a \cap \overline{b} \subseteq W_m(b)$	; 3 and def. (12)

From definition of $\mathcal{E}_m$, the implication $a \subseteq b \Rightarrow a \mapsto b \in \mathcal{E}_m$ follows immediately because $a \cap \overline{b} = \varnothing$. It proves premise (b) of theorem 2 for the case of minimal progress.

Now, we use an induction scheme to define the *reachability* relation under minimal progress $\mathcal{L}_m$ similar to definition 2. Therefore $\mathcal{L}_m$ is the smallest relation containing the base relation $\mathcal{E}_m$ and it is both, transitive and disjunctive.

Finally we prove that the weakest precondition $W_m(r)$, for any $r \in \mathbb{P}(u)$ leads to r: $W_m(r) \mapsto r \in \mathcal{L}_m$

1. $\mathsf{grd}(S) \cap S(r) \cap \overline{r} \subseteq \mathsf{grd}(S) \cap S(r)$	; trivial
2. $\mathsf{grd}(S) \cap S(r) \mapsto r \in \mathcal{E}_m$	; 1 and def. $\mathcal{E}_m$
3. $W_m(r) \mapsto r \in \mathcal{E}_m$	; 2 and (12)
4. $W_m(r) \mapsto r \in \mathcal{L}_m$	; 3 and def. $\mathcal{L}_m$

This proves premise (c) of theorem 2 for the case of minimal progress.

At this time, monotonicity and strictness of W_m and premises (a), (b) and (c) of theorem 2 instantiated to the case of minimal progress have been proved. Therefore the equality between *termination* and *reachability* relations is stated:

$$\mathcal{T}_m = \mathcal{L}_m \tag{16}$$

3.3 Weak Fairness

In this subsection, we define the *termination* and *reachability* relations for weak fairness assumptions. We prove that premises of theorem 2, instantiated to the case of weak fairness, are satisfied with these definitions. Therefore we claim the equality between these relations.

3.3.1 Termination under WF We use the dovetail operator presented in section 2.1 to model a *fair loop* for a certain event G in $\mathcal{S}$:

$$Y(q)(G) = \overline{q} \Longrightarrow ((S \;;\; Y(q)(G)) \;\triangledown\; (\mathsf{grd}(G) \mid G)) \tag{17}$$

The guard $\overline{q}$ of this loop prevents iteration of the fair choice in any state belonging to q. Informally, we expect that any execution of $Y(G)(q)$ in any state in $q \cup \mathsf{grd}(G)$ terminates. Execution of $Y(q)(G)$ in $\overline{q} \cap \mathsf{grd}(G)$ cannot loops forever because the dovetail operator prevents unlimited execution of the branch $S \;;\; Y(q)(G)$. Moreover the set transformer $\mathsf{grd}(G) \mid G$ is always enabled ($\mathsf{grd}(\mathsf{grd}(G) \mid G) = u$) and therefore it will be eventually executed. All our claims are formally justified by the calculi of termination set and the liberal weakest precondition of $Y(q)(G)$, for any q and r, $r \neq u$ in $\mathbb{P}(u)$:

$$\mathsf{pre}(Y(q)(G)) = \mathsf{fix}(\overline{q} \cap G(\varnothing) \Longrightarrow \overline{S(q)} \mid S) \tag{18}$$

$$\mathcal{L}(Y(q)(G))(r) = \mathsf{FIX}(\overline{q} \Longrightarrow (\mathsf{grd}(G) \cap G(r) \mid S)) \tag{19}$$

These calculi follow from definitions of set transformers given in section 2.1 and the extreme solutions of the recursive equations generated. The proof of (18) and (19) is given in appendix D. Moreover, in appendix D appears the proof of the following inclusion, for any q and r in $\mathbb{P}(u)$:

$$\mathcal{L}(Y(q)(G))(r) \subseteq \mathsf{pre}(Y(q)(G)) \tag{20}$$

(20), and the pairing condition, give us the set transformer associated with the fair loop:

$$Y(q)(G)(r) = \mathsf{FIX}(\overline{q} \Longrightarrow (\mathsf{grd}(G) \cap G(r) \mid S)) \tag{21}$$

From this definition follows the monotonicity of $Y(q)(G)$, which is proved in appendix D.

The fair loop $Y(q)(G)$ models a *fair G-step* in the iteration of events under weak fairness assumptions. We say that G is the helpful event in this G-step. A *fair step* in the iteration of events is modeled by the following set transformer:

$$W_w = \lambda r \cdot (r \subseteq u \mid \bigcup G \cdot (G \in \mathcal{S} \mid Y(r)(G)(r))) \tag{22}$$

From (21) follows $\mathsf{grd}(Y(q)(G)) = \overline{q}$ for any G in $\mathcal{S}$ and $q \in \mathbb{P}(u)$, therefore the strictness of W_w follows. On the other hand, from monotonicity of $Y(q)(G)$ follows the monotonicity of W_w. These three proofs are given in appendix D.

The body of the iteration of events under weak fairness is the guarded event $\mathcal{F}_w(r)$ defined as follows:

$$\mathcal{F}_w(r) = \overline{r} \Longrightarrow W_w \tag{23}$$

Definition of the *termination* relation under weak fairness is:

$$\mathcal{T}_w = \{\, a \mapsto b \mid a \subseteq u \wedge b \subseteq u \wedge a \subseteq \mathsf{fix}(\mathcal{F}_w(b)) \,\} \tag{24}$$

3.3.2 Reachability under WF We define the basic relation $\mathcal{E}(G)$ for a helpful event G, as the set of pairs $a \mapsto b$ from which we can derive a property $G \cdot x \in a \gg_w x \in b$ (3):

$$\mathcal{E}_w(G) = \{\, a \mapsto b \mid a \subseteq u \wedge b \subseteq u \wedge a \cap \overline{b} \subseteq S(a \cup b) \cap \overline{G(\varnothing)} \cap G(b) \,\} \tag{25}$$

Now, the basic relation for weak fairness is:

$$\mathcal{E}_w = \bigcup G \cdot (G \in \mathcal{S} \mid \mathcal{E}'_w(G)) \tag{26}$$

The proof of premise (a) of theorem 2 instantiated to weak fairness requires the following property which is proved in appendix D:

$$\forall G \cdot (G \in \mathcal{S} \wedge a \mapsto b \in \mathcal{E}'_w(G) \Rightarrow a \subseteq Y(b)(G)(b)) \tag{27}$$

Using (27), the proof of $a \mapsto b \in \mathcal{E}_w \Rightarrow a \cap \overline{b} \subseteq W_w(b)$ is:

1. $\forall G \cdot (G \in \mathcal{S} \Rightarrow (a \mapsto b \in \mathcal{E}'_w(G) \Rightarrow a \subseteq Y(b)(G)(b)))$	; (27)
2. $\exists G \cdot (G \in \mathcal{S} \wedge a \mapsto b \in \mathcal{E}'_w(G)) \Rightarrow a \subseteq W_w(b)$	; 1 and (22).
3. $a \mapsto b \in \bigcup G \cdot (G \in \mathcal{S} \mid \mathcal{E}'_w(G)) \Rightarrow a \subseteq W_w(b)$	; 2
4. $a \mapsto b \in \mathcal{E}_w \Rightarrow a \subseteq W_w(b)$	; 3 and (26)
5. $a \mapsto b \in \mathcal{E}_w \Rightarrow a \cap \overline{b} \subseteq W_w(b)$	; 4 and $b \subseteq W_w(b)$

From (25) immediately follows $a \mapsto b \in \mathcal{E}'_w(G)$, for any G in $\mathcal{S}$ if $a \subseteq b$ holds, and from (26) follows $a \subseteq b \Rightarrow a \mapsto b \in \mathcal{E}_w$. This proves premise (b) of theorem 2.

We use an induction scheme to define the *reachability* relation under weak fairness $\mathcal{L}_w$ similar to definition 2. Therefore $\mathcal{L}_w$ is the smallest relation containing the base relation $\mathcal{E}_w$ and it is both, transitive and disjunctive.

From (21) and (25) follows the property:

$$\forall (G, r) \cdot (G \in \mathcal{S} \wedge r \subseteq u \Rightarrow Y(r)(G)(r) \mapsto r \in \mathcal{E}'_w(G)) \tag{28}$$

We use this property to prove the premise (c) of theorem 2: $W_w(r) \mapsto r \in \mathcal{L}_w$ as follows:

1. $\forall G \cdot (G \in \mathcal{S} \Rightarrow Y(r)(G)(r) \mapsto r \in \mathcal{E}'_w(G))$	; from (28)
2. $\forall G \cdot (G \in \mathcal{S} \Rightarrow \mathcal{E}'_w(G) \subseteq \mathcal{E}_w)$	; def. $\mathcal{E}_w$
3. $\forall G \cdot (G \in \mathcal{S} \Rightarrow Y(r)(G)(r) \mapsto r \in \mathcal{E}_w)$	; 2 and 1
4. $\forall G \cdot (G \in \mathcal{S} \Rightarrow Y(r)(G)(r) \mapsto r \in \mathcal{L}_w)$	; def. $\mathcal{L}_w$
5. $\{ Y(r)(G)(r) \mid G \in \mathcal{S} \} \times \{r\} \subseteq \mathcal{L}_w$	; 4
6. $\bigcup(\{ Y(r)(G)(r) \mid G \in \mathcal{S} \}) \mapsto r \in \mathcal{L}_w$	; 5 and SDR
7. $\bigcup G \cdot (G \in \mathcal{S} \mid Y(r)(G)(r)) \mapsto r \in \mathcal{L}_w$	; 6
8. $W_w(r) \mapsto r \in \mathcal{L}_w$	; 7 and def. F

At this time *termination* ($\mathcal{T}_w$), basic relation ($\mathcal{E}_w$) and *reachability* ($\mathcal{L}_m$) relations for weak fairness assumptions have been defined. Monotonicity and strictness of the set transformer W_w, and premises (a), (b) and (c) of theorem 2 instantiated to the case of weak fairness have been proved. Therefore, the equality between *termination* and *reachability* relations under weak fairness is stated:

$$\mathcal{T}_w = \mathcal{L}_w \tag{29}$$

4 Deriving Liveness Properties

In this section we present two examples where we show practical usefulness of equalities between *termination* and *reachability* relations under minimal progress and weak fairness assumptions. This section is divided in three parts. In the first part we state and prove the *Variant Theorem*, which allows us to prove termination of iterations over a set transformer if a variant decreases. In the second part we use this theorem to prove a sufficient condition allowing derivation of liveness properties under minimal progress. Finally, we give another sufficient condition to derive a liveness property under minimal progress when a similar property holds in weak fairness assumptions

4.1 The Variant Theorem

The variant theorem allows us to prove termination of iteration of conjunctive set transformers. This theorem considers a total function which maps each element of the state space to an element of a well founded order and a set which is invariant at each iteration of the set transformer. The theorem states that if any execution of the set transformer starting in a state in the invariant set and a certain value of the variant function, terminates in a state where the value of the variant is decremented, then the invariant set is contained in the termination set of the iteration of the set transformer. Formally, the theorem is stated as follows:

Theorem 3. (Variant Theorem)
Let $V \in u \rightarrow \mathbb{N}$, $v = \lambda n \cdot (n \in \mathbb{N} \mid \{\, z \mid z \in u \wedge V(z) = n \,\})$ *and* $v' = \lambda n \cdot (n \in \mathbb{N} \mid \{\, z \mid z \in u \wedge V(z) < n \,\})$. *For any conjunctive set transformer* f *in* $\mathbb{P}(u) \rightarrow \mathbb{P}(u)$ *and* p *in* $\mathbb{P}(u)$, *such that* $v(n) \cap p \subseteq f(v'(n))$ *and* $p \subseteq f(p)$ *, for any* n *in* $\mathbb{N}$, *the following inclusion holds:*

$$p \subseteq \mathit{fix}(f)$$

The proof of this theorem uses the following equalities:

$$\forall n \cdot (n \in \mathbb{N} \Rightarrow v'(n) = \bigcup i \cdot (i \in \mathbb{N} \wedge i < n \mid v(i))) \tag{30}$$

$$\bigcup i \cdot (i \in \mathbb{N} \mid v'(i+1)) = \bigcup i \cdot (i \in \mathbb{N} \mid v(i)) \tag{31}$$

$$\bigcup i \cdot (i \in \mathbb{N} \mid v(i)) = u \tag{32}$$

and the following property:

$$\forall n \cdot (n \in \mathbb{N} \Rightarrow \bigcup i \cdot (i \in \mathbb{N} \wedge i \leq n \mid v(i)) \cap p \subseteq f^{n+1}) \tag{33}$$

which are proved, under the assumptions of the theorem 3, in appendix E. The proof of theorem 3 is as follows:

1. $\forall n \cdot (n \in \mathbb{N} \Rightarrow \bigcup i \cdot (i \in \mathbb{N} \wedge i \leq n \mid v(i)) \cap p \subseteq \mathsf{fix}(f))$; (33) and (9)
2. $\forall n \cdot (n \in \mathbb{N} \Rightarrow v'(n+1) \cap p \subseteq \mathsf{fix}(f))$; from (30) and 1
3. $\bigcup i \cdot (i \in \mathbb{N} \mid v'(i+1)) \cap p \subseteq \mathsf{fix}(f)$; 2
4. $\bigcup i \cdot (i \in \mathbb{N} \mid v(i)) \cap p \subseteq \mathsf{fix}(f)$; 3 and (31)
5. $u \cap p \subseteq \mathsf{fix}(f)$; 4 and (32)
6. $p \subseteq \mathsf{fix}(p)$; 5 and $p \subseteq u$

4.2 A Sufficient Condition for Minimal Progress

A system reaches a certain set from any set of starting states under minimal progress, if the set of depart is invariant in the system, it is contained in the guard of the system and each execution of the system decrements a variant. Formally, these conditions are stated as follows:

ANTECEDENT	CONSEQUENT
$\forall n \cdot (n \in \mathbb{N} \Rightarrow a \cap \overline{b} \cap v(n) \subseteq S(v'(n)))$ $a \cap \overline{b} \subseteq \mathsf{grd}(S) \cap S(a)$	$a \mapsto b \in \mathcal{L}_m$

We remark from definition (13), that $\mathcal{F}_m(b)$ is a conjunctive set transformer. From this remark the proof of the rule is as follows:

1. $\forall n \cdot (n \in \mathbb{N} \Rightarrow a \cap \overline{b} \cap v(n) \subseteq S(v'(n)) \cap \mathsf{grd}(S))$	; from premises
2. $\forall n \cdot (n \in \mathbb{N} \Rightarrow a \cap v(n) \subseteq \mathcal{F}_m(b)(v'(n)))$	; 1 and (13)
3. $a \subseteq \mathcal{F}_m(b)(a)$	; premise and (13)
4. $a \subseteq \mathsf{fix}(\mathcal{F}_m(b))$	; 3, 2, theorem 3
5. $a \mapsto b \in \mathcal{T}_m$	; 4 and (14)
6. $a \mapsto b \in \mathcal{L}_m$	; 5, equality (16)

Antecedent of this rule corresponds to sufficient conditions in [2] to prove liveness properties and it is the only rule concerning the proof of liveness properties. Soundness of this rule is proved here in a more direct way.

Soundness of this rule is given without reasoning over state-traces, taking advantage of the fixpoint semantics approach.

4.3 From Weak Fairness to Minimal Progress

Using the variant theorem, we prove a sufficient condition to establish that a liveness property under minimal progress, follows from a corresponding property proved under weak fairness and from the decrement of a variant:

ANTECEDENT	CONSEQUENT
$\forall n \cdot (n \in \mathbb{N} \Rightarrow \overline{b} \cap v(n) \subseteq S(v'(n)))$ $a \mapsto b \in \mathcal{L}_w$	$a \mapsto b \in \mathcal{L}_m$

The proof of these conditions is given by the *Variant Theorem*. In order to apply the theorem, we need to identify an invariant set under $\mathcal{F}_m(b)$. However, as the sets a and b cannot be proved as invariants, we prove that the least fixpoint of $\mathcal{F}_w(b)$ is invariant under $\mathcal{F}_m(b)$, that is $\mathsf{fix}(\mathcal{F}_w(b)) \subseteq \mathcal{F}_m(b)(\mathsf{fix}(\mathcal{F}_w(b)))$. This proof requires the following lemma:

$$\forall \alpha \cdot (\mathcal{F}_w(b)^\alpha \subseteq b \cup (\mathsf{grd}(S) \cap S(\mathsf{fix}(\mathcal{F}_w(b))))) \tag{34}$$

The proof of (34) is done by transfinite induction; it is presented in appendix E. Using (34), the proof of sufficient conditions are as follows:

1. $\mathsf{fix}(\mathcal{F}_w(b)) \subseteq b \cup (\mathsf{grd}(S) \cap S(\mathsf{fix}(\mathcal{F}_w(b))))$	; Theorem 1, (34)
2. $\mathsf{fix}(\mathcal{F}_w(b)) \subseteq \mathcal{F}_m(b)(\mathsf{fix}(\mathcal{F}_w(b)))$	; 1 and (13)
3. $\forall n \cdot (n \in \mathbb{N} \Rightarrow \mathsf{fix}(\mathcal{F}_w(b)) \cap v(n) \subseteq b \cup \mathsf{grd}(S) \cap S(v'(n)))$	; 2 and premise
4. $\forall n \cdot (n \in \mathbb{N} \Rightarrow \mathsf{fix}(\mathcal{F}_w(b)) \cap v(n) \subseteq \mathcal{F}_m(b)(v'(n)))$	; 3 and (13)
5. $\mathsf{fix}(\mathcal{F}_w(b)) \subseteq \mathsf{fix}(\mathcal{F}_m(b))$	; 4,2 and th. 3
6. $a \mapsto b \in \mathcal{T}_w$	; premise, eq. (29)
7. $a \subseteq \mathsf{fix}(\mathcal{F}_w(b))$	; 6 and def. $\mathcal{T}_w$
8. $a \subseteq \mathsf{fix}(\mathcal{F}_m(b))$	; 7 and 5
9. $a \mapsto b \in \mathcal{L}_m$	; 8, def. $\mathcal{T}_m$, eq. (16)

5 Conclusions

We have presented a fixpoint semantics of event systems under minimal progress and weak fairness assumptions. Then we have proved soundness and completeness of rules for deriving *leads-to* properties under weak fairness and minimal progress assumptions. Finally we have proved sufficient conditions to guarantee a liveness property under minimal progress in two cases of hypothesis: every event decrements a variant under an invariant, or every event decrements a variant and the property holds under weak fairness.

The development of our semantics is structured. First a general framework is established without concerns of fairness, and our notions of termination and reachability are elaborated. Soundness and completeness of rules for *leads-to* are proved in this framework. The general framework is then instantiated to the cases of minimal progress and weak fairness assumptions and the corresponding results are proved. Each element in our models has a concrete representation as a set transformer. In particular, we stress how the weak fairness assumption is modeled by the dovetail operator.

We have stated a simple form of the variant theorem and given a simple proof of it. We remark the usefulness of this theorem in the proofs of liveness properties. Particularly we note the importance of conditions which guarantee the derivation of a certain liveness property $\mathcal{P}$ under minimal progress if $\mathcal{P}$ holds under weak fairness, and every element of the system decrements a variant. This is a new result which gives the possibility to *implement* fairness in a system.

As a future work we investigate how our approach can be managed to deal with refinement of event systems. Another line will be to consider how to instantiate the general framework for strong fairness.

References

1. J.-R. Abrial. *The B-Book, Assigning Programs to Meanings*. Cambridge University Press, 1996.
2. J.-R. Abrial and L. Mussat. Introducing Dynamic Constraints in B. In *B'98: Recent Advances in the Development and Use of the B Method, LNCS 1393*, pages 83–128. Springer-Verlag, april 1998.
3. R.J.R Back and R. Kurki-Suonio. Decentralization of Process Nets with Centralized Control. In *2nd ACM SIGACT-SIGOPS Symp. on Principles of Distributed Computing*, pages 131–143, 1983.
4. Manfred Broy and Greg Nelson. Adding Fair Choice to Dijkstra's Calculus. *ACM Transactions on Programming Languages and Systems*, 16(3):924–938, May 1994.
5. K. Mani Chandy and Jayadev Misra. *Parallel Program Design A Foundation*. Addison-Wesley, 1988.
6. Steve Dune. Introducing Backward Refinement into B . In *ZB 2003: Formal Specification and Development in Z an B, LNCS 2651*, pages 178–196. Springer-Verlag, June 2003.
7. Eric C.R. Hehner. do Considere od: A Contribution to the Programming Calculus. *Acta Informatica*, 11:287–304, 1979.
8. Charanjit S. Jutla and Josyula R. Rao. A Methodology for Designing Proof Rules for Fair Parallel Programs. *Formal Aspects of Computing*, 9:359–378, 1997.
9. Greg Nelson. A Generalization of Dijkstra's Calculus. *ACM Transactions on Programming Languages and Systems*, 11(4):517–561, October 1989.
10. I. S. W. B. Prasetya. Error in the UNITY Substitution Rule for Subscripted Operators. *Formal Aspects of Computing*, 6:466–470, 1994.
11. Héctor Ruíz Barradas and Didier Bert. A Fixpoint Semantics of Event Systems with and without Fairness Assumptions. In *Fifth International Conference on Integrated Formal Methods IFM 2005, LNCS 3771*. Springer-Verlag, 2005.
12. Héctor Ruiz Barradas and Didier Bert. Proof Obligations for Specification and Refinement of Liveness Prope rties under Weak Fairness. Technical Report 1071-I LSR 20, LSR-IMAG, Grenoble, 2005.

13. Héctor Ruíz Barradas and Didier Bert. Specification and Proof of Liveness Properties under Fairness Assumptions in B Event Systems . In *Integrated Formal Methods , Third International Conference IFM 2002, LNCS 2335*, pages 360–379. Springer-Verlag, May 2002.
14. Héctor Ruíz Barradas and Didier Bert. Propriétés dynamiques avec hypothèses d'équité en B événementiel. In *Approches Formelles dans l'Assitance au Développement de Logiciels, AFADL'2004*, pages 299–313. Besançon, France, june 2004.
15. Beverly A. Sanders. Eliminating the Substitution Axion from UNITY Logic. *Acta Informatica*, 3:189–205, 1991.

ANNEXES

A *leads-to* as Relation Between Predicates or Sets

In order to guarantee that *leads-to* ($\leadsto$), as a relation between predicates on the system state, and the relation $\pounds$ between subsets of u are equivalent, we supposed the following equivalence:

$$P(x) \leadsto Q(x) \equiv \{\, z \mid z \in u \wedge P(z) \,\} \mapsto \{\, z \mid z \in u \wedge Q(z) \,\} \in \pounds \tag{8}$$

In the following paragraphs we give the proof of this equivalence. It is founded in the fact that *leads-to* relation of UNITY logic, as pointed in [8], can be defined by an induction scheme, similar to definition 2. That is, $\leadsto$ as a relation between predicates, $\leadsto \subseteq \mathsf{Pred} \times \mathsf{Pred}$, where Pred is the set of predicates on the space of the state variable x, is the smallest relation satisfying rules BRL, TRA and DSJ given in section 2.2[2]:

BRL: $E \subseteq \leadsto$
TRA: $\leadsto^2 \subseteq \leadsto$
DSJ: $\forall m \cdot (m \in M \Rightarrow P(m) \leadsto Q) \Rightarrow \exists m \cdot (m \in M \wedge P(m)) \leadsto Q$

where E is the set of couples of predicates satisfying the *ensures* relation:

$$E = \{\, P \mapsto Q \mid P \gg Q \,\} \tag{35}$$

We recall that $\gg$ relation must be instantiated to $\gg_m$ relation under minimal progress hypothesis or $\gg_w$ relation under weak fairness assumptions, in similar way to the instantiation of the basic relation $\mathcal{E}$. In order to give the proof of equivalence (8), at this time we suppose that E and $\mathcal{E}$ satisfy the following properties:

$$\forall (P, Q) \cdot (P \in \mathsf{Pred} \wedge Q \in \mathsf{Pred} \Rightarrow P(x) \gg Q(x) \equiv \{\, z \mid z \in u \wedge P(z) \,\} \mapsto \{\, z \mid z \in u \wedge Q(z) \,\} \in \mathcal{E}) \tag{36}$$

$$\forall (p, q) \cdot (p \subseteq u \wedge q \subseteq u \Rightarrow p \mapsto q \in \mathcal{E} \equiv x \in p \gg x \in q) \tag{37}$$

We give below the proof of these properties, instantiated to weak fairness or minimal progress assumptions.

The proof of (8) is given in two parts:

$$P(x) \leadsto Q(x) \Rightarrow \{\, z \mid z \in u \wedge P(z) \,\} \mapsto \{\, z \mid z \in u \wedge Q(z) \,\} \in \pounds \tag{38}$$

$$\{\, z \mid z \in u \wedge P(z) \,\} \mapsto \{\, z \mid z \in u \wedge Q(z) \,\} \in \pounds \Rightarrow P(x) \leadsto Q(x) \tag{39}$$

Proof of (38)
Let $\mathcal{P}$ be the following set:

$$\mathcal{P} = \{\, P \mapsto Q \mid (P \leadsto Q) \wedge \{\, z \mid z \in u \wedge P(z) \,\} \mapsto \{\, z \mid z \in u \wedge Q(z) \,\} \in \pounds \,\}$$

From this definition follows $\mathcal{P} \subseteq \leadsto$. Inclusion $\leadsto \subseteq \mathcal{P}$ is proved below by structural induction. From these inclusions, follows the equality $\mathcal{P} = \leadsto$. Finally, from this equality follows (38):

$$\begin{array}{ll} & \mathcal{P} = \leadsto \\ \equiv & \{\ \mathcal{P} = \leadsto \cap \{\, P \mapsto Q \mid \{\, z \mid z \in u \wedge P(z) \,\} \mapsto \{\, z \mid z \in u \wedge Q(z) \,\} \in \pounds \,\}\ \} \\ & \leadsto \subseteq \{\, P \mapsto Q \mid \{\, z \mid z \in u \wedge P(z) \,\} \mapsto \{\, z \mid z \in u \wedge Q(z) \,\} \in \pounds \,\} \\ \equiv & \\ & \forall (P, Q) \cdot (P \leadsto Q \Rightarrow \{\, z \mid z \in u \wedge P(z) \,\} \mapsto \{\, z \mid z \in u \wedge Q(z) \,\} \in \pounds) \end{array}$$

□

In order to proof $\leadsto \subseteq \mathcal{P}$, the following proofs are required:

[2] The infix notation $P \leadsto Q$ is used to state that $P \mapsto Q \in \leadsto$, for any predicate P and Q in Pred.

– $E \subseteq \mathcal{P}$.
– $\mathcal{P}^2 \subseteq \mathcal{P}$.
– $\forall i \cdot (i \in I \Rightarrow P(i) \mapsto Q \in \mathcal{P}) \Rightarrow \exists i \cdot (i \in I \wedge P(i)) \mapsto Q \in \mathcal{P}$

Proof of Base Case

1. $P \gg Q \Rightarrow \{\, z \mid z \in u \wedge P(z) \,\} \mapsto \{\, z \mid z \in u \wedge Q(z) \,\} \in \mathcal{E}$	; from (36)
2. $P \gg Q \Rightarrow \{\, z \mid z \in u \wedge P(z) \,\} \mapsto \{\, z \mid z \in u \wedge Q(z) \,\} \in \mathcal{L}$	; 1 and def. 2
3. $P \gg Q \Rightarrow P \rightsquigarrow Q$	; BRA
4. $P \mapsto Q \in E \Rightarrow P \mapsto Q \in \mathcal{P}$	; 3, 2 and (35)
5. $E \subseteq \mathcal{P}$	; 4

□

Proof of Transitivity
It follows from $P \mapsto Q \in \mathcal{P} \wedge Q \mapsto R \in \mathcal{P} \Rightarrow P \mapsto R \in \mathcal{P}$:

1. $P \mapsto Q \in \mathcal{P} \wedge Q \mapsto r \in \mathcal{P}$	; premise
2. $P \rightsquigarrow R$	; 1, def. $\mathcal{P}$, TRA
3. $\{\, z \mid z \in u \wedge P(z) \,\} \mapsto \{\, z \mid z \in u \wedge R(z) \,\} \in \mathcal{L}$	; 1, def. $\mathcal{P}$, STR
4. $P \mapsto R \in \mathcal{P}$	; 3, 2 and def. $\mathcal{P}$

□

Proof of Disjunction

1. $\forall i \cdot (i \in I \Rightarrow P(i) \mapsto Q \in \mathcal{P})$	; premise
2. $\exists i \cdot (i \in I \wedge P(i)) \rightsquigarrow Q$	; 1, def. $\mathcal{P}$, DSJ
3. $\forall i \cdot (i \in I \Rightarrow \{\, z \mid z \in u \wedge P(i)(z) \,\} \mapsto \{\, z \mid z \in u \wedge Q(z) \,\} \in \mathcal{L})$	; 1, def. $\mathcal{P}$
4. $\{\, \{\, z \mid z \in u \wedge P(i)(z) \,\} \mid i \in I \,\} \times \{\, z \mid z \in u \wedge Q(z) \,\} \subseteq \mathcal{L}$	; 3
5. $\bigcup(\{\, \{\, z \mid z \in u \wedge P(i)(z) \,\} \mid i \in I \,\}) \mapsto \{\, z \mid z \in u \wedge Q(z) \,\} \in \mathcal{L}$	; 4, SDJ
6. $\{\, z \mid z \in u \wedge \exists i \cdot (i \in I \wedge P(i)(z)) \,\} \mapsto \{\, z \mid z \in u \wedge Q(z) \,\} \in \mathcal{L}$	; 5
7. $\exists i \cdot (i \in I \wedge P(i)) \mapsto Q \in \mathcal{P}$	; 6, 2 and def. $\mathcal{P}$

□

Proof of (39)
This proof is similar to the proof of (38). Let $\mathcal{Q}$ be the following set:

$$\mathcal{Q} = \{\, p \mapsto q \mid p \mapsto q \in \mathcal{L} \wedge x \in p \rightsquigarrow x \in q \,\}$$

From this definition follows $\mathcal{Q} \subseteq \mathcal{L}$. Inclusion $\mathcal{L} \subseteq \mathcal{Q}$ is proved below by structural induction. From these inclusions follows equality $\mathcal{Q} = \mathcal{L}$. Now, from this equality follows inclusion $\mathcal{L} \subseteq \{\, p \mapsto q \mid p \mapsto q \in \mathcal{L} \wedge x \in p \rightsquigarrow x \in q \,\}$:

$$\begin{array}{ll} & \mathcal{Q} = \mathcal{L} \\ \equiv & \{\ \ Q = \mathcal{L} \cap \{\, p \mapsto q \mid p \subseteq u \wedge q \subseteq u \wedge x \in p \rightsquigarrow x \in q \,\}\ \ \} \\ & \mathcal{L} \subseteq \{\, p \mapsto q \mid p \subseteq u \wedge q \subseteq u \wedge x \in p \rightsquigarrow x \in q \,\} \end{array}$$

Finally, from this inclusion, and taking $\{\, z \mid z \in u \wedge P(z) \,\} \mapsto \{\, z \mid z \in u \wedge Q(z) \,\} \in \mathcal{L}$ as a premise, the conclusion $P \rightsquigarrow Q$ of (39) follows.

□

In order to prove $\mathcal{L} \subseteq \mathcal{Q}$ the following proofs are required:

– $\mathcal{E} \subseteq \mathcal{Q}$.

– $\mathcal{Q}^2 \subseteq \mathcal{Q}$.
– $l \times \{q\} \subseteq \mathcal{Q} \Rightarrow \bigcup(l) \mapsto q \in \mathcal{Q}$

Proof of Base Case

1. $p \mapsto q \in \mathcal{E} \Rightarrow x \in p \gg x \in q$	; from (37)
2. $p \mapsto q \in \mathcal{E} \Rightarrow x \in p \rightsquigarrow x \in q$	; 1 and BRL
3. $p \mapsto q \in \mathcal{E} \Rightarrow p \mapsto q \in \pounds$	; SBR
4. $p \mapsto q \in \mathcal{E} \Rightarrow p \mapsto q \in \mathcal{Q}$	; 3, 2, def. $\mathcal{Q}$
5. $\mathcal{E} \subseteq \mathcal{Q}$	; 4

□

Proof of Transitivity

1. $p \mapsto q \in \mathcal{Q} \wedge q \mapsto r \in \mathcal{Q}$	; premise
2. $p \mapsto q \in \pounds \wedge q \mapsto r \in \pounds$	; 1, def $\mathcal{Q}$
3. $(x \in p \rightsquigarrow x \in q) \wedge (x \in q \rightsquigarrow x \in r)$	; 1, def Q
4. $p \mapsto r \in \pounds \wedge x \in p \rightsquigarrow x \in r$	; 2, 3, TRA,STR
5. $p \mapsto r \in \mathcal{Q}$	; 4, def. $\mathcal{Q}$

□

Proof of Disjunction

1. $l \times \{q\} \subseteq \mathcal{Q}$	; premise
2. $l \times \{q\} \subseteq \pounds$	; 1, def. $\mathcal{Q}$
3. $\bigcup(l) \mapsto q \in \pounds$	; 2, SDR
4. $l \times \{q\} \subseteq \{\, a \mapsto b \mid a \subseteq u \wedge b \subseteq u \wedge x \in a \rightsquigarrow x \in b \,\}$	; 1, def. $\mathcal{Q}$
5. $\forall s \cdot (s \in l \Rightarrow x \in s \rightsquigarrow x \in q)$	; $l \subseteq \mathbb{P}(u)$, 4
6. $\exists s \cdot (s \in l \wedge x \in s) \rightsquigarrow x \in q$	; 5, DSJ
7. $x \in \bigcup(l) \rightsquigarrow x \in q$	; 6
8. $\bigcup(l) \mapsto q \in \mathcal{Q}$	; 7, 3, def. $\mathcal{Q}$

□

A.1 Instantiation of *ensures* to Minimal Progress

In this section, properties (36) and (37) are proved when the *ensures* relation is instantiated to a minimal progress assumption.

Definition of *ensures* relation under minimal progress assumptions ($\gg_m$), without considering the strongest invariant, is given by the following definition:

$$\forall (P, Q) \cdot (P \in \mathsf{Pred} \wedge Q \in \mathsf{Pred} \Rightarrow P(x) \gg_m Q(x) \equiv$$
$$\forall x \cdot (I(x) \wedge P(x) \wedge \neg Q(x) \Rightarrow \mathit{grd}(\mathsf{sub}(S)) \wedge [\mathsf{sub}(S)]\, Q(x)))$$

where $\mathsf{sub}(S)$ denotes the *generalized substitution* associated with set transformer S, and for any generalized substitution T, the predicate $\mathit{grd}(T)$ is equivalent to $\neg[T]\, \mathit{false}$.

Proof of (36)

$$
\begin{array}{ll}
& P(x) \gg_m Q(x) \\
\equiv & \{\ \text{def. } \gg_m\ \} \\
& \forall x \cdot (I(x) \wedge P(x) \wedge \neg Q(x) \Rightarrow grd(\mathsf{sub}(S)) \wedge [\mathsf{sub}(S)]\, Q(x)) \\
\equiv & \{\ \text{set theory}\ \} \\
& \forall x \cdot (x \in \{\, z \mid I(z) \wedge P(z) \,\} \cap \{\, z \mid I(z) \wedge \neg Q(x) \,\} \Rightarrow I(x) \wedge grd(\mathsf{sub}(S)) \wedge \\
& [\mathsf{sub}(S)]\, Q(x)) \\
\equiv & \{\ I(x) \Rightarrow [\mathsf{sub}(S)]\, I(x), \text{ conjunctive } S\ \} \\
& \forall x \cdot (x \in \{\, z \mid I(z) \wedge P(z) \,\} \cap \{\, z \mid I(z) \wedge \neg Q(x) \,\} \Rightarrow I(x) \wedge grd(\mathsf{sub}(S)) \wedge [\mathsf{sub}(S)]\, I(x) \wedge Q(x)) \\
\equiv & \{\ \text{set transformers}\ \} \\
& \forall x \cdot (x \in \{\, z \mid I(z) \wedge P(z) \,\} \cap \{\, z \mid I(z) \wedge \neg Q(x) \,\} \Rightarrow x \in \mathsf{grd}(S) \cap S(\{\, z \mid I(z) \wedge Q(z) \,\})) \\
\equiv & \{\ \text{set theory, } u = \{\, z \mid I(z) \,\}\ \} \\
& \{\, z \mid z \in u \wedge P(z) \,\} \cap \overline{\{\, z \mid z \in u \wedge Q(x) \,\}} \subseteq \mathsf{grd}(S) \cap S(\{\, z \mid z \in u \wedge Q(z) \,\}) \\
\equiv & \{\ \text{def. } \mathcal{E}_m\ \} \\
& \{\, z \mid z \in u \wedge P(z) \,\} \mapsto \{\, z \mid z \in u \wedge Q(x) \,\} \in \mathcal{E}_m
\end{array}
$$

□

Proof of (37)

$$
\begin{array}{ll}
& p \mapsto q \in \mathcal{E}_m \\
\equiv & \{\ \text{def. } \mathcal{E}_m\ \} \\
& p \cap \overline{q} \subseteq S(q) \cap \mathsf{grd}(S) \\
\equiv & \\
& \forall x \cdot (x \in p \cap \overline{q} \Rightarrow x \in S(q) \cap \mathsf{grd}(S)) \\
\equiv & \{\ x \in p \Rightarrow I(x)\ \} \\
& \forall x \cdot (I(x) \wedge x \in p \wedge \neg x \in q \Rightarrow x \in S(q) \cap \mathsf{grd}(S)) \\
\equiv & \{\ \text{set transformers}\ \} \\
& \forall x \cdot (I(x) \wedge x \in p \wedge \neg x \in q \Rightarrow [\mathsf{sub}(S)]\, x \in q \wedge grd(S)) \\
\equiv & \{\ \text{def. } \gg_m\ \} \\
& x \in p \gg_m x \in q
\end{array}
$$

□

A.2 Instantiation of *ensures* to Weak Fairness

In this section, properties (36) and (37) are proved when the *ensures* relation ($\gg$) is instantiated to a weak fairness assumption relation ($\gg_w$). The instantiation under this condition is given by the following equivalence:

$$P(x) \gg Q(x) \equiv \exists G \cdot (G \in \mathcal{S} \wedge G \cdot P(x) \gg_w Q(x))$$

Definition of *ensures* relation under weak fairness assumptions ($\gg_m$), without considering the strongest invariant, is given by the following definition:

$$
\begin{array}{l}
\forall (P, Q) \cdot (P \in \mathsf{Pred} \wedge Q \in \mathsf{Pred} \Rightarrow G \cdot P(x) \gg_w Q(x) \equiv \\
\quad \forall x \cdot (I(x) \wedge P(x) \wedge \neg Q(x) \Rightarrow ([\mathsf{sub}(S)]\, (P(x) \vee Q(x))) \wedge grd(\mathsf{sub}(G)) \wedge [\mathsf{sub}(G)]\, Q(x)))
\end{array}
$$

where $\mathsf{sub}(S)$ and $\mathsf{sub}(G)$ denote the *generalized substitutions* associated with set transformers S and G.

The proof follows from the following equivalences which are proved below:

$$G \cdot P(x) \gg_w Q(x) \equiv \{\, z \mid z \in u \wedge P(z) \,\} \mapsto \{\, z \mid z \in u \wedge Q(x) \,\} \in \mathcal{E}(G) \tag{40}$$

$$p \mapsto q \in \mathcal{E}(G) \equiv G \cdot x \in p \gg_w x \in q \tag{41}$$

Proof of (36)
Implication from left to right follows from (40)

$$\begin{array}{ll} & G \cdot P(x) \gg_w Q(x) \equiv \{\, z \mid z \in u \wedge P(z) \,\} \mapsto \{\, z \mid z \in u \wedge Q(x) \,\} \in \mathcal{E}(G) \\ \Rightarrow & \qquad \{\ \mathcal{E}_w = \bigcup G \cdot (G \in \mathcal{S} \mid \mathcal{E}(G))\ \} \\ & G \cdot P(x) \gg_w Q(x) \Rightarrow \{\, z \mid z \in u \wedge P(z) \,\} \mapsto \{\, z \mid z \in u \wedge Q(x) \,\} \in \mathcal{E}_w \\ \Rightarrow & \\ & \exists G \cdot (G \in \mathcal{S} \wedge G \cdot P(x) \gg_w Q(x)) \Rightarrow \{\, z \mid z \in u \wedge P(z) \,\} \mapsto \{\, z \mid z \in u \wedge Q(x) \,\} \in \mathcal{E}_w \end{array}$$

Implication from right to left follows from (40)

$$\begin{array}{ll} & G \cdot P(x) \gg_w Q(x) \equiv \{\, z \mid z \in u \wedge P(z) \,\} \mapsto \{\, z \mid z \in u \wedge Q(x) \,\} \in \mathcal{E}(G) \\ \Rightarrow & \\ & \{\, z \mid z \in u \wedge P(z) \,\} \mapsto \{\, z \mid z \in u \wedge Q(x) \,\} \in \mathcal{E}(G) \Rightarrow \exists G \cdot (G \in \mathcal{S} \wedge G \cdot P(x) \gg_w Q(x)) \\ \Rightarrow & \\ & \exists G \cdot (G \in \mathcal{S} \wedge \{\, z \mid z \in u \wedge P(z) \,\} \mapsto \{\, z \mid z \in u \wedge Q(x) \,\} \in \mathcal{E}(G)) \Rightarrow \exists G \cdot (G \in \mathcal{S} \wedge G \cdot P(x) \gg_w Q(x)) \\ \Rightarrow & \\ & \{\, z \mid z \in u \wedge P(z) \,\} \mapsto \{\, z \mid z \in u \wedge Q(x) \,\} \in \bigcup G \cdot (G \in \mathcal{S} \mid \mathcal{E}(G)) \Rightarrow \exists G \cdot (G \in \mathcal{S} \wedge G \cdot P(x) \gg_w Q(x)) \\ \equiv & \qquad \{\ \text{def. } \mathcal{E}\ \} \\ & \{\, z \mid z \in u \wedge P(z) \,\} \mapsto \{\, z \mid z \in u \wedge Q(x) \,\} \in \mathcal{E}_w \Rightarrow \exists G \cdot (G \in \mathcal{S} \wedge G \cdot P(x) \gg_w Q(x)) \end{array}$$

□

Proof of (37)
Implication from left to right follows from (41)

$$\begin{array}{ll} & p \mapsto q \in \mathcal{E}(G) \equiv G \cdot x \in p \gg_w x \in q \\ \Rightarrow & \qquad \{\ \mathcal{E}_w = \bigcup G \cdot (G \in \mathcal{S} \mid \mathcal{E}(G))\ \} \\ & p \mapsto q \in \mathcal{E}(G) \Rightarrow \exists G \cdot (G \in \mathcal{S} \wedge G \cdot x \in p \gg_w x \in q) \\ \Rightarrow & \\ & \exists G \cdot (G \in \mathcal{S} \wedge p \mapsto q \in \mathcal{E}(G)) \Rightarrow \exists G \cdot (G \in \mathcal{S} \wedge G \cdot x \in p \gg_w x \in q) \end{array}$$

Implication from right to left follows from (41)

$$\begin{array}{ll} & p \mapsto q \in \mathcal{E}(G) \equiv G \cdot x \in p \gg_w x \in q \\ \Rightarrow & \\ & p \mapsto q \in \mathcal{E}(G) \Rightarrow \exists G \cdot (G \in \mathcal{S} \wedge G \cdot x \in p \gg_w x \in q) \\ \Rightarrow & \\ & \exists G \cdot (p \mapsto q \in \mathcal{E}(G)) \Rightarrow \exists G \cdot (G \in \mathcal{S} \wedge G \cdot x \in p \gg_w x \in q) \\ \Rightarrow & \\ & p \mapsto q \in \mathcal{E}_w \Rightarrow \exists G \cdot (G \in \mathcal{S} \wedge G \cdot x \in p \gg_w x \in q) \end{array}$$

□

Proof of (40)

$$
\begin{array}{ll}
& G \cdot P(x) \gg_w Q(x) \\
\equiv & \{\ \text{def. } \gg_w\ \} \\
& \forall x \cdot (I(x) \ \wedge\ P(x) \ \wedge\ \neg Q(x) \ \Rightarrow\ ([\mathsf{sub}(S)]\,(P(x) \ \vee\ Q(x))) \ \wedge\ \mathit{grd}(\mathsf{sub}(G)) \ \wedge\ [\mathsf{sub}(G)]\,Q(x)) \\
\equiv & \{\ \text{set theory}\ \} \\
& \forall x \cdot (x \in \{\, z \mid I(z) \ \wedge\ P(z) \,\} \cap \{\, z \mid I(z) \ \wedge\ \neg Q(x) \,\} \ \Rightarrow\ ([\mathsf{sub}(S)]\,(P(x) \ \vee\ Q(x))) \ \wedge\ \mathit{grd}(\mathsf{sub}(G)) \wedge [\mathsf{sub}(G)]\,Q(x)) \\
\equiv & \{\ I(x) \Rightarrow [\mathsf{sub}(S)]\,I(x), \text{ conjunctive } S \text{ and } G\ \} \\
& \forall x \cdot (x \in \{\, z \mid I(z) \wedge P(z) \,\} \cap \{\, z \mid I(z) \wedge \neg Q(x) \,\} \Rightarrow ([\mathsf{sub}(S)]\,(I(x) \wedge P(x) \vee I(x) \wedge Q(x))) \wedge \mathit{grd}(\mathsf{sub}(G)) \wedge [\mathsf{sub}(G)]\,I(x) \wedge Q(x)) \\
\equiv & \{\ \text{set transformers}\ \} \\
& \forall x \cdot (x \in \{\, z \mid I(z) \ \wedge\ P(z) \,\} \cap \{\, z \mid I(z) \ \wedge\ \neg Q(x) \,\} \ \Rightarrow\ x \in S(\{\, z \mid z \in u \ \wedge\ P(z) \,\} \cup \{\, z \mid z \in u \wedge Q(x) \,\}) \wedge x \in \mathsf{grd}(G) \wedge x \in G(\{\, z \mid z \in u \wedge Q(x) \,\})) \\
\equiv & \{\ \text{set theory, } u = \{\, z \mid I(z) \,\}\ \} \\
& \{\, z \mid z \in u \ \wedge\ P(z) \,\} \cap \overline{\{\, z \mid z \in u \wedge Q(x) \,\}} \subseteq S(\{\, z \mid z \in u \ \wedge\ P(z) \,\} \cup \{\, z \mid z \in u \ \wedge\ Q(x) \,\}) \cap \mathsf{grd}(G) \cap G(\{\, z \mid z \in u \wedge Q(x) \,\}) \\
\equiv & \{\ \text{def. } \mathcal{E}(G)\ \} \\
& \{\, z \mid z \in u \wedge P(z) \,\} \mapsto \{\, z \mid z \in u \wedge Q(x) \,\} \in \mathcal{E}(G)
\end{array}
$$

□

Proof of (41)

$$
\begin{array}{ll}
& p \mapsto q \in \mathcal{E}(G) \\
\equiv & \{\ \text{def. } \mathcal{E}_w\ \} \\
& p \cap \overline{q} \subseteq S(p \cup q) \cap \mathsf{grd}(G) \cap G(q) \\
\equiv & \\
& \forall x \cdot (x \in p \cap \overline{q} \Rightarrow x \in S(p \cup q) \cap \mathsf{grd}(G) \cap G(q)) \\
\equiv & \{\ x \in p \Rightarrow I(x)\ \} \\
& \forall x \cdot (I(x) \wedge x \in p \wedge \neg x \in q \Rightarrow x \in S(p \cup q) \cap \mathsf{grd}(G) \cap G(q)) \\
\equiv & \{\ \text{set transformers}\ \} \\
& \forall x \cdot (I(x) \wedge x \in p \wedge \neg x \in q \Rightarrow ([\mathsf{sub}(S)]\,(x \in p \vee x \in q)) \wedge \mathit{grd}(G) \wedge [\mathsf{sub}(G)]\,x \in q) \\
\equiv & \{\ \text{def. } \gg_w\ \} \\
& G \cdot x \in p \gg_w x \in q
\end{array}
$$

□

B Extension of Semantics to Consider the Strongest Invariant

In this annex, the strongest invariant is considered in definitions of *termination* and *reachability* relations. It allows us to preserve soundness of UNITY logic. Certain definitions and proofs are independent of the strongest invariant and they remain unchanged. New definitions and proofs are only considered in this annex. It is structured in four parts. In section B.1, the strongest invariant is presented. In section B.2, the general theorem about soundness and completeness is restated and proved. In section B.4, *termination* and basic relation for *leads-to* are redefined to consider a minimal progress assumption, and the hypothesis of the theorem of soundness and completeness are proved. In section B.5 an similar treatment is considered to the case of a weak fairness assumption.

B.1 Strongest Invariant

Original definitions of the fundamental relations *unless* and *ensures* in UNITY logic [5], do not consider initial conditions. On another hand, in order to give the possibility to prove valid properties (completeness), in [5] the *Substitution Axiom* is proposed. Basically, this axiom states that any invariant predicate may be replaced by *true* and vice versa.

Original definitions of the fundamental relations in [5], along with the substitution axiom, give an unsound proof system as it is reported in [15]. To fix this problem, the relation *unless* and *ensures* are redefined to consider initial conditions. The new definitions in [15] consider the *strongest invariant*, which holds in the reachable states. Moreover, the substitution axiom is replaced by a substitution rule, which becomes a theorem in the new logic. However, in [10], a problem with the new rule is reported and another substitution rule is proposed. In this report we are not concerned by this last issue.

Following the proposal in [15], and adapting the definition to our framework, the strongest invariant is defined as follows:

Definition 3. Strongest Invariant

Let $\mathfrak{S}$ be a B *event system with state variable x, initialization U and choice of events S. The strongest invariant SI of $\mathfrak{S}$ is the strongest predicate X satisfying:*

$$\forall x \cdot ((X \Rightarrow [S]\, X) \wedge (([x' := x]\, \mathsf{prd}(U)) \Rightarrow X))$$

where $\mathsf{prd}(U)$ denotes the before-after relation associated with the initilization U [1]. Using the strongest invariant, the definition of the *ensures* relation, to specify basic liveness properties, under our two fairness assumptions is as follows:

Definition 4. Ensures under Minimal Progress

Let $\mathfrak{S}$ be a B *event system with state variable x, initialization U and choice of events S. For any predicate P and Q over x, the basic liveness relation $\gg_m$ is defined as follows:*

$$P \gg_m Q \equiv SI \wedge P \wedge \neg Q \Rightarrow (([S]\, Q) \wedge grd(S))$$

Definition 5. Ensures under Weak Fairness

Let $\mathfrak{S}$ be a B *event system with state variable x, initialization U, choice of events S and G an event of $\mathfrak{S}$. For any predicate P and Q over x, the basic liveness relation $\gg_w$ is defined as follows:*

$$G \cdot P \gg_w Q \equiv SI \wedge P \wedge \neg Q \Rightarrow (([S]\ P \vee Q) \wedge ([G]\ Q) \wedge grd(S))$$

Finally si, the set counterpart of the strongest invariant, is given by the following definition

$$si = \{z \mid SI(z)\}$$

B.2 General Framework

The body of iteration in the general framework does not change:

$$\mathcal{F}(r) = (\overline{r} \Longrightarrow W) \tag{5}$$

The *termination* relation is redefined to consider the strongest invariant as follows:

Definition 6. (Termination Relation)

$$\mathcal{T} = \{\, a \mapsto b \,|\, a \subseteq u \wedge b \subseteq u \wedge si \cap a \subseteq \mathit{fix}(\mathcal{F}(si \cap b)) \,\} \tag{42}$$

The *reachability* relation is not modified directly:

Definition 7. (Reachability Relation)
The reachability *relation $\mathcal{L}$, $\mathcal{L} \in \mathbb{P}(u) \leftrightarrow \mathbb{P}(u)$, is defined by the following induction scheme:*
(**SBR**)*: $\mathcal{E} \subseteq \mathcal{L}$*
(**STR**)*: $\mathcal{L}$; $\mathcal{L} \subseteq \mathcal{L}$*
(**SDR**)*: $\forall (q,l) \cdot (q \in \mathbb{P}(u) \wedge l \subseteq \mathbb{P}(u) \Rightarrow (l \times \{q\} \subseteq \mathcal{L} \Rightarrow \bigcup(l) \mapsto q \in \mathcal{L}))$*
Closure*: $\forall l' \cdot (l' \in u \leftrightarrow u \wedge \mathcal{E} \subseteq l' \wedge l'$; $l' \subseteq l' \wedge$*
$\forall (q,l) \cdot (q \in \mathbb{P}(u) \wedge l \subseteq \mathbb{P}(u) \wedge l \times \{q\} \subseteq l' \Rightarrow \bigcup(l) \mapsto q \in l') \Rightarrow \mathcal{L} \subseteq l')$*

However, when $\mathcal{L}$ is instantiated to minimal or weak fairness assumptions, the strongest invariant is considered in the definition of the base relation.

The theorem of soundness and completeness, taking into account new definitions of $\mathcal{T}$ and $\mathcal{L}$ remains basically unchanged. Only hypothesis concerning the strongest invariant and the basic relation, are modified with respect to the precedent version.

Theorem 4. (Soundness and Completeness)
Let W be a monotonic and strict set transformer and $\mathcal{F}(r) = (\overline{r} \Longrightarrow W)$ for any r in $\mathbb{P}(u)$. Let relations $\mathcal{T}$ and $\mathcal{L}$ be defined as definitions 6 and 7 respectively. Considering (a) $a \mapsto b \in \mathcal{E} \Rightarrow si \cap a \cap \overline{b} \subseteq W(si \cap b)$, (b) $a \subseteq b \Rightarrow a \mapsto b \in \mathcal{E}$, (c) $si \cap a \subseteq b \Rightarrow a \mapsto b \in \mathcal{E}$ and (d) $W(r) \mapsto r \in \mathcal{L}$, for any a, b and r in $\mathbb{P}(u)$, the following equality holds:

$$\mathcal{L} = \mathcal{T}$$

The proof is given in the following section.

In appendix A, the equivalence between the reachability relation $\mathcal{L}$ and the definition of the *leads-to* relation $\rightsquigarrow$ is proved. That proof does not consider the strongest invariant in the given definitions. In order to connect the definition of the reachability relation, considering

the strongest invariant, a demonstration similar to the proof of (8), can be given to prove the following equivalence:

$$P(x) \rightsquigarrow Q(x) \equiv \{\, z \mid z \in si \wedge P(z) \,\} \mapsto \{\, z \mid z \in si \wedge Q(z) \,\} \in \pounds$$

which relates the definition of the *leads-to* relation with the reachability relation considering the strongest invariant.

B.3 Proof of Soundness and Completeness

As before, the proof is divided in $\pounds \subseteq \mathcal{T}$ and $\mathcal{T} \subseteq \pounds$.

B.3.1 Proof of $\pounds \subseteq \mathcal{T}$

The proof of $\pounds \subseteq \mathcal{T}$ follows from the closure clause in definition of $\pounds$. According to this clause, $\mathcal{T}$ must contain the base relation $\mathcal{E}$, and it must be transitive and disjunctive. The following paragraphs present the proof of these cases.

Base Case

$$a \mapsto b \in \mathcal{E} \Rightarrow a \mapsto b \in \mathcal{T} \tag{43}$$

1. $a \mapsto b \in \mathcal{E}$	; premise
2. $si \cap a \cap \overline{b} \subseteq W(b \cap si)$	; 1 and hyp. (a)
3. $si \cap a \subseteq b \cup W(b \cap si)$	; 2
4. $si \cap a \subseteq si \cap b \cup W(b \cap si)$	; 3
5. $si \cap a \subseteq \mathcal{F}(si \cap b)(b \cap si)$	; 4 and def. (5)
6. $si \cap a \subseteq \mathcal{F}(si \cap b)^2$	; 5 and iterate (6)
7. $si \cap a \subseteq \mathsf{fix}(\mathcal{F}(si \cap b))$	; 6 and (9)
8. $a \mapsto b \in \mathcal{T}$	; 7 and def. (42)

□

Transitivity

$$\forall (a, b) \cdot (a \mapsto b \in (\mathcal{T} \,;\, \mathcal{T}) \Rightarrow a \mapsto b \in \mathcal{T}) \tag{44}$$

The proof of (44) requires the following property:

$$\forall (a, b) \cdot (a \mapsto b \in \mathcal{T} \Rightarrow \mathsf{fix}(\mathcal{F}(si \cap a)) \subseteq \mathsf{fix}(\mathcal{F}(si \cap b))) \tag{45}$$

Taking $a \mapsto b \in \mathcal{T}$ as a premise, and considering $\mathsf{fix}(\mathcal{F}(si \cap a))$ as the least fixpoint of $\mathcal{F}(si \cap a)$, (45) follows from $\mathcal{F}(si \cap a)(\mathsf{fix}(\mathcal{F}(si \cap b))) \subseteq \mathsf{fix}(\mathcal{F}(si \cap b))$ as follows:

1. $si \cap a \subseteq \mathsf{fix}(\mathcal{F}(si \cap b))$	; from $a \mapsto b \in \mathcal{T}$
2. $\mathcal{F}(si \cap b)(\mathsf{fix}(\mathcal{F}(si \cap b))) = \mathsf{fix}(\mathcal{F}(si \cap b))$	; fixpoint definition
3. $W(\mathsf{fix}(\mathcal{F}(si \cap b))) \subseteq \mathsf{fix}(\mathcal{F}(si \cap b))$	; 2 and (5)
4. $\mathcal{F}(si \cap a)(\mathsf{fix}(\mathcal{F}(si \cap b))) \subseteq \mathsf{fix}(\mathcal{F}(si \cap b))$	; 3, 1 and (5)

□

Proof of (44)

1. $\exists c \cdot (a \mapsto c \in \mathcal{T} \land c \mapsto b \in \mathcal{T})$; from $a \mapsto b \in \mathcal{T}; \mathcal{T}$
2. $\exists c \cdot (si \cap a \subseteq \mathsf{fix}(\mathcal{F}(si \cap c)) \land c \mapsto b \in \mathcal{T})$; 3 and def. $\mathcal{T}$
3. $\exists c \cdot (si \cap a \subseteq \mathsf{fix}(\mathcal{F}(si \cap c)) \land \mathsf{fix}(\mathcal{F}(si \cap c)) \subseteq \mathsf{fix}(\mathcal{F}(si \cap b)))$; 2 and (45)
4. $si \cap a \subseteq \mathsf{fix}(\mathcal{F}(si \cap b))$; 3
5. $a \mapsto b \in \mathcal{T}$; 6 and def. $\mathcal{T}$

□

Disjunction

$$\forall (l, q) \cdot (l \times \{q\} \subseteq \mathcal{T} \Rightarrow \bigcup(l) \mapsto q \in \mathcal{T}) \tag{46}$$

1. $l \times \{q\} \subseteq \mathcal{T}$; premise
2. $\forall p \cdot (p \in l \Rightarrow p \mapsto q \in \mathcal{T})$; 1
3. $\forall p \cdot (p \in l \Rightarrow si \cap p \subseteq \mathsf{fix}(\mathcal{F}(si \cap q)))$; 2 and def. $\mathcal{T}_m$
4. $\bigcup p \cdot (p \in l \mid si \cap p) \subseteq \mathsf{fix}(\mathcal{F}(si \cap q))$; 3
5. $si \cap \bigcup p \cdot (p \in l \mid p) \subseteq \mathsf{fix}(\mathcal{F}(si \cap q))$; 4
6. $si \cap \bigcup(l) \subseteq \mathsf{fix}(\mathcal{F}(si \cap q))$; 5
7. $\bigcup(l) \mapsto q \in \mathcal{T}$; 4 and def. $\mathcal{T}_m$

□

B.3.2 Proof of $\mathcal{T} \subseteq \mathcal{L}$

The proof of this inclusion requires the following property which is already proved:

$$\forall r \cdot (r \in \mathbb{P}(u) \Rightarrow \mathcal{F}(r)^\alpha \mapsto r \in \mathcal{L}) \tag{11}$$

Proof of $\mathcal{T} \subseteq \mathcal{L}$

1. $si \cap a \subseteq \mathsf{fix}(\mathcal{F}(si \cap b))$; from $a \mapsto b \in \mathcal{T}$
2. $\exists \alpha \cdot (si \cap a \subseteq \mathcal{F}(si \cap b)^\alpha)$; 1 and theorem 1
3. $\exists \alpha \cdot (a \mapsto \mathcal{F}(si \cap b)^\alpha \in \mathcal{E})$; 2 and hyp. (c)
4. $\exists \alpha \cdot (a \mapsto \mathcal{F}(si \cap b)^\alpha \in \mathcal{L})$; 3 and STR
5. $a \mapsto si \cap b \in \mathcal{L}$; 4 and (11)
6. $a \mapsto b \in \mathcal{L}$; 5, $si \cap b \mapsto b \in \mathcal{L}$, STR

□

B.4 Minimal Progress

The body of iteration under a minimal progress assumption does not change:

$$\mathcal{F}_m(r) = (\overline{r} \Longrightarrow W_m)$$

where W_m remains defined as before:

$$W_m = \mathsf{grd}(S) \mid S \tag{12}$$

termination relation under weak fairness assumption is defined as follows:

$$\mathcal{T}_m = \{\, a \mapsto b \,|\, a \subseteq u \land b \subseteq u \land si \cap a \subseteq \mathsf{fix}(\mathcal{F}_m(si \cap b)) \,\} \tag{47}$$

Basic relation $\mathcal{E}_m$ for *reachability* relation $\mathcal{L}_m$ under minimal progress assumptions is defined as follows:

$$\mathcal{E}_m = \{\, a \mapsto b \,|\, a \subseteq u \wedge b \subseteq u \wedge si \cap a \cap \overline{b} \subseteq S(b) \cap \mathsf{grd}(S) \,\} \tag{48}$$

Relation $\mathcal{L}_m$ is defined by an induction scheme, according to definition 2.

The following proofs of hypothesis in theorem 4 allow us to conclude the equality between *reachability* and *termination* relations under a minimal progress assumption:

$$\mathcal{T}_m = \mathcal{L}_m$$

B.4.1 Proof of Premise (a)

$$a \mapsto b \in \mathcal{E}_m \Rightarrow si \cap a \cap \overline{b} \subseteq W_m(si \cap b) \tag{49}$$

$$\begin{array}{ll}
& a \mapsto b \in \mathcal{E}_m \\
\equiv & \qquad \{\ (48)\ \} \\
& si \cap a \cap \overline{b} \subseteq S(b) \cap \mathsf{grd}(S) \\
\Rightarrow & \qquad \{\ si \subseteq S(si), \text{ conjunctive } S\ \} \\
& si \cap a \cap \overline{b} \subseteq S(si \cap b) \cap \mathsf{grd}(S) \\
\equiv & \qquad \{\ (12)\ \} \\
& si \cap a \cap \overline{b} \subseteq W_m(si \cap b)
\end{array}$$

□

B.4.2 Proof of Premise (b)

$$a \subseteq b \Rightarrow a \mapsto b \in \mathcal{E}_m \tag{50}$$

1. $a \subseteq b$; premise
2. $si \cap a \cap \overline{b} = \varnothing$; 1
3. $si \cap a \cap \overline{b} \subseteq \mathsf{grd}(S) \cap S(b)$; 2
4. $a \mapsto b \in \mathcal{E}_m$; 3 and (48)

□

B.4.3 Proof of Premise (c)

$$si \cap a \subseteq b \Rightarrow a \mapsto b \in \mathcal{E}_m \tag{51}$$

1. $si \cap a \subseteq b$; premise
2. $si \cap b \cap \overline{b} = \varnothing$; 1
3. $si \cap a \cap \overline{b} \subseteq \mathsf{grd}(S) \cap S(b)$; 2
4. $a \mapsto b \in \mathcal{E}_m$; 3 and (48)

□

B.4.4 Proof of Premise (d)

$$W_m(r) \mapsto r \in \mathcal{L}_m \tag{52}$$

1. $si \cap \mathsf{grd}(S) \cap S(r) \cap \overline{r} \subseteq \mathsf{grd}(S) \cap S(r)$; trivial
2. $\mathsf{grd}(S) \cap S(r) \mapsto r \in \mathcal{E}_m$; 1 and def. $\mathcal{E}_m$
3. $W_m(r) \mapsto r \in \mathcal{E}_m$; 2 and (12)
4. $W_m(r) \mapsto r \in \mathcal{L}_m$; 3 and def. $\mathcal{L}_m$

□

B.5 Weak Fairness

The body of iteration under weak fairness assumption does not change:

$$\mathcal{F}_w(r) = \overline{r} \Longrightarrow W_w \tag{23}$$

where W_w is defined as follows:

$$W_w = \lambda r \cdot (r \subseteq u \mid \bigcup G \cdot (G \in \mathcal{S} \mid Y(r)(G)(r))) \tag{22}$$

and $Y(r)(G)(r)$ is defined by:

$$Y(q)(G)(r) = \mathsf{FIX}(\overline{q} \Longrightarrow (\mathsf{grd}(G) \cap G(r) \mid S)) \tag{21}$$

termination relation under weak fairness assumption is defined as follows:

$$\mathcal{T}_w = \{\, a \mapsto b \,|\, a \subseteq u \wedge b \subseteq u \wedge si \cap a \subseteq \mathsf{fix}(\mathcal{F}_w(si \cap b)) \,\} \tag{53}$$

Basic relation $\mathcal{E}_w$ for *reachability* relation $\mathcal{L}_w$ under weak fairness assumption is not changed directly:

$$\mathcal{E}_w = \bigcup G \cdot (G \in \mathcal{S} \mid \mathcal{E}(G)) \tag{26}$$

However, $\mathcal{E}(G)$ is redefined to consider the strongest invariant:

$$\mathcal{E}(G) = \{\, a \mapsto b \,|\, a \subseteq u \wedge b \subseteq u \wedge si \cap a \cap \overline{b} \subseteq S(a \cup b) \cap \overline{G(\varnothing)} \cap G(b) \,\} \tag{54}$$

Relation $\mathcal{L}_w$ is defined by an induction scheme, according to definition 2.

The following proofs of hypothesis in theorem 4 allow us to conclude the equality between *reachability* and *termination* relations under a weak fairness assumption:

$$\mathcal{T}_w = \mathcal{L}_w$$

B.5.1 Proof of Premise (a)

$$a \mapsto b \in \mathcal{E}_w \Rightarrow si \cap a \cap \overline{b} \subseteq W_w(si \cap b) \tag{55}$$

The proof requires the following property:

$$\forall G \cdot (G \in \mathcal{S} \wedge a \mapsto b \in \mathcal{E}(G) \Rightarrow si \cap a \subseteq Y(si \cap b)(G)(si \cap b)) \tag{56}$$

$a \mapsto b \in \mathcal{E}(G)$

$\equiv$ { (54) }

$si \cap a \cap \overline{b} \subseteq S(a \cup b) \cap \overline{G(\varnothing)} \cap G(b)$

$\Rightarrow$ { $si \subseteq S(si)$, conjunctive S and G }

$si \cap a \cap \overline{b} \subseteq S(si \cap a \cup si \cap b) \cap \overline{G(\varnothing)} \cap G(si \cap b)$

$\Rightarrow$

$si \cap a \subseteq si \cap b \cup S(si \cap a \cup si \cap b) \cap \overline{G(\varnothing)} \cap G(si \cap b)$

$\Rightarrow$

$si \cap a \cup si \cap b \subseteq si \cap b \cup S(si \cap a \cup si \cap b) \cap \overline{G(\varnothing)} \cap G(si \cap b)$

$\equiv$ { set transformers }

$si \cap a \cup si \cap b \subseteq (\overline{si \cap b} \Longrightarrow \mathsf{grd}(G) \cap G(si \cap b) \mid S)(si \cap a \cup si \cap b)$

$\Rightarrow$ { greatest fixpoint property }

$si \cap a \subseteq \mathsf{FIX}(\overline{si \cap b} \Longrightarrow \mathsf{grd}(G) \cap G(si \cap b) \mid S)$

$\equiv$ { (21) }

$si \cap a \subseteq Y(si \cap b)(G)(si \cap b)$

□

Proof of (55)

1. $\forall G \cdot (G \in \mathcal{S} \Rightarrow (a \mapsto b \in \mathcal{E}(G) \Rightarrow si \cap a \subseteq Y(si \cap b)(G)(si \cap b)))$; (56)
2. $\exists G \cdot (G \in \mathcal{S} \wedge a \mapsto b \in \mathcal{E}(G)) \Rightarrow si \cap a \subseteq W_w(si \cap b)$; 1 and (22).
3. $a \mapsto b \in \bigcup G \cdot (G \in \mathcal{S} \mid \mathcal{E}(G)) \Rightarrow si \cap a \subseteq W_w(si \cap b)$; 2
4. $a \mapsto b \in \mathcal{E}_w \Rightarrow si \cap a \subseteq W_w(si \cap b)$; 3 and (26)
5. $a \mapsto b \in \mathcal{E}_w \Rightarrow si \cap a \subseteq si \cap b \cup W_w(si \cap b)$; 4, $si \cap b \subseteq W_w(si \cap b)$
6. $a \mapsto b \in \mathcal{E}_w \Rightarrow si \cap a \cap \overline{b} \subseteq W_w(si \cap b)$; 5

□

B.5.2 Proof of Premise (b)

$a \subseteq b \Rightarrow a \mapsto b \in \mathcal{E}_w$ (57)

1. $a \subseteq b$; premise
2. $si \cap a \cap \overline{b} = \varnothing$; 1
3. $\forall G \cdot (G \in \mathcal{S} \Rightarrow si \cap a \cap \overline{b} \subseteq S(a \cup b) \cap \overline{G(\varnothing)} \cap G(b))$; 2
4. $\forall G \cdot (G \in \mathcal{S} \Rightarrow a \mapsto b \in \mathcal{E}(G))$; 3 and (54)
5. $a \mapsto b \in \bigcup G \cdot (G \in \mathcal{S} \mid \mathcal{E}(G))$; 4
6. $a \mapsto b \in \mathcal{E}_w$; 5 (26)

□

B.5.3 Proof of Premise (c)

$si \cap a \subseteq b \Rightarrow a \mapsto b \in \mathcal{E}_w$ (58)

1. $si \cap a \subseteq b$; premise
2. $si \cap a \cap \overline{b} = \varnothing$; 1
3. $\forall G \cdot (G \in \mathcal{S} \Rightarrow si \cap a \cap \overline{b} \subseteq S(a \cup b) \cap \overline{G(\varnothing)} \cap G(b))$; 2
4. $\forall G \cdot (G \in \mathcal{S} \Rightarrow a \mapsto b \in \mathcal{E}(G))$; 3 and (54)
5. $a \mapsto b \in \bigcup G \cdot (G \in \mathcal{S} \mid \mathcal{E}(G))$; 4
6. $a \mapsto b \in \mathcal{E}_w$; 5 (26)

□

B.5.4 Proof of Premise (d)

$$\forall r \cdot (r \subseteq u \Rightarrow W_w(r) \mapsto r \in \mathcal{L}_w) \tag{59}$$

The proof requires the following property:

$$\forall (G, r) \cdot (G \in \mathcal{S} \wedge r \subseteq u \Rightarrow Y(r)(G)(r) \mapsto r \in \mathcal{E}(G)) \tag{60}$$

1. $S(Y(r)(G)(r)) \subseteq S(Y(r)(G)(r) \cup r)$; monotony of S
2. $Y(r)(G)(r) = r \cup \mathsf{grd}(G) \cap G(r) \cap S(Y(r)(G)(r))$; (21)
3. $Y(r)(G)(r) \cap \overline{r} \subseteq \mathsf{grd}(G) \cap G(r) \cap S(Y(r)(G)(r) \cup r)$; 2, 1
4. $si \cap Y(r)(G)(r) \cap \overline{r} \subseteq Y(r)(G)(r) \cap \overline{r}$; trivial
5. $Y(r)(G)(r) \mapsto r \in \mathcal{E}(G)$; 4, 3 and (26)

□

Proof of (59)

1. $\forall G \cdot (G \in \mathcal{S} \Rightarrow Y(r)(G)(r) \mapsto r \in \mathcal{E}(G))$; from (60)
2. $\forall G \cdot (G \in \mathcal{S} \Rightarrow \mathcal{E}(G) \subseteq \mathcal{E}_w)$; def. $\mathcal{E}_w$
3. $\forall G \cdot (G \in \mathcal{S} \Rightarrow Y(r)(G)(r) \mapsto r \in \mathcal{E}_w)$; 2 and 1
4. $\forall G \cdot (G \in \mathcal{S} \Rightarrow Y(r)(G)(r) \mapsto r \in \mathcal{L}_w)$; def. $\mathcal{L}_w$
5. $\{ Y(r)(G)(r) \mid G \in \mathcal{S} \} \times \{r\} \subseteq \mathcal{L}_w$; 4
6. $\bigcup(\{ Y(r)(G)(r) \mid G \in \mathcal{S} \}) \mapsto r \in \mathcal{L}_w$; 5 and SDR
7. $\bigcup G \cdot (G \in \mathcal{S} \mid Y(r)(G)(r)) \mapsto r \in \mathcal{L}_w$; 6
8. $W_w(r) \mapsto r \in \mathcal{L}_w$; 7 and def. F

□

C Proofs of section 3.1.3

C.1 Proof of (9): $\forall \alpha \cdot (f^\alpha \subseteq \mathsf{fix}(f))$

Successor ordinal:

$$
\begin{array}{ll}
& f^\alpha \subseteq \mathsf{fix}(f) \\
\Rightarrow & \\
& f(f^\alpha) \subseteq f(\mathsf{fix}(f)) \\
\Rightarrow & \\
& f^{\alpha+1} \subseteq \mathsf{fix}(f)
\end{array}
$$

Limit ordinal:

$$
\begin{array}{lll}
& \forall \beta \cdot (\beta < \alpha \Rightarrow f^\beta \subseteq \mathsf{fix}(f)) & \\
\Rightarrow & & \{ \text{ monotony } \} \\
& \forall \beta \cdot (\beta < \alpha \Rightarrow f(f^\beta) \subseteq f(\mathsf{fix}(f))) & \\
\Rightarrow & & \{ \text{ fixpoint def. } \} \\
& \forall \beta \cdot (\beta < \alpha \Rightarrow f(f^\beta) \subseteq \mathsf{fix}(f)) & \\
\Rightarrow & & \\
& \bigcup \beta \cdot (\beta < \alpha \mid f(f^\beta)) \subseteq \mathsf{fix}(f) & \\
\equiv & & \{ \text{ def. iterate } \} \\
& f^\alpha \subseteq \mathsf{fix}(f) &
\end{array}
$$

□

C.2 Proof of (11): $\mathcal{F}(r)^\alpha \mapsto r \in \mathcal{L} \Rightarrow \mathcal{F}(r)^{\alpha+1} \mapsto r \in \mathcal{L}$

Successor ordinal

1. $\mathcal{F}(r)^\alpha \mapsto r \in L$	; ind. hyp.
2. $W(\mathcal{F}(r)^\alpha) \mapsto \mathcal{F}(r)^\alpha \in L$	; from hyp. (c) th. 2
3. $r \mapsto r \in L$	; hyp. (b) th. 2, SBR
4. $r \cup W(\mathcal{F}(r)^\alpha) \mapsto r \in L$	; 3, 2 and SDR
6. $\mathcal{F}(r)(\mathcal{F}(r)^\alpha) \mapsto r \in L$	; 5 and (5)
7. $\mathcal{F}(r)^{\alpha+1} \mapsto r \in L$	; 6 and def. iterate

□

D Proofs of Section 3.3

D.1 Termination Set of Fair Loop: $\mathsf{pre}(Y(q)(G)) = \mathsf{fix}(\overline{q} \cap G(\varnothing) \Longrightarrow (\overline{S(q)} \mid S))$

$$
\begin{array}{ll}
& \mathsf{pre}(Y(q)(G)) \\
= & \qquad \{ \text{ def. of } \mathsf{pre} \} \\
& Y(q)(G)(u) \\
= & \qquad \{ \ (17) \ \} \\
& q \cup ((S \mathbin{;} Y(q)(G)) \triangledown (\mathsf{grd}(G) \mid G))(u) \\
= & \qquad \{ \ (2),\ X = (S \mathbin{;} Y(q)(G)),\ Z = (\mathsf{grd}(G) \mid G) \ \} \\
& q \cup ((X(u) \cup Z(u)) \cap (\overline{X(\varnothing)} \cup Z(u)) \cap (X(u) \cup \overline{Z(\varnothing)})) \\
= & \qquad \{ \ G(u) = u,\ Z(u) = \mathsf{grd}(G),\ \overline{Z(\varnothing)} = u \ \} \\
& q \cup ((X(u) \cup \mathsf{grd}(G)) \cap (\overline{X(\varnothing)} \cup \mathsf{grd}(G))) \\
= & \qquad \{ \text{ distributivity } \} \\
& q \cup \mathsf{grd}(G) \cup (X(u) \cap \overline{X(\varnothing)}) \\
= & \qquad \{ \ X = (S \mathbin{;} Y(q)(G)), \text{ set transformer } \} \\
& q \cup \mathsf{grd}(G) \cup (S(Y(q)(G)(u)) \cap \overline{S(Y(q)(G)(\varnothing))}) \\
= & \qquad \{ \text{ def. } \mathsf{grd}(Y(q)(G)),\ \mathsf{grd}(G) \text{ and set transformer } \} \\
& (\overline{q} \cap G(\varnothing) \Longrightarrow (\overline{S(q)} \mid S))(Y(q)(G)(u)) \\
= & \qquad \{ \text{ extreme solution of recursive equation } \} \\
& \mathsf{fix}(\overline{q} \cap G(\varnothing) \Longrightarrow (\overline{S(q)} \mid S))
\end{array}
$$

□

D.2 Liberal of $Y(q)(G)$: $\mathcal{L}(Y(q)(G))(r) = \mathsf{FIX}(\overline{q} \Longrightarrow (\mathsf{grd}(G) \cap G(r) \mid S))$

For $r \subseteq u \wedge r \neq u$:

$$
\begin{array}{ll}
& \mathcal{L}(Y(q)(G))(r) \\
= & \qquad \{ \ (17), \text{ Liberal set transformer of guard and dovetail } \} \\
& q \cup \mathcal{L}(S \mathbin{;} Y(q))(r) \cap \mathcal{L}(\mathsf{grd}(G) \mid G)(r) \\
= & \qquad \{ \ r \neq u,\ \mathcal{L}(\mathsf{grd}(G) \mid G)(r) = \mathsf{grd}(G) \cap \mathcal{L}(G)(r), \mathcal{L}(G)(r) = G(r) \ \} \\
& q \cup \mathcal{L}(S \mathbin{;} Y(q))(r) \cap \mathsf{grd}(G) \cap G(r) \\
= & \qquad \{ \text{ Liberal set transformer of sequencing, } \mathcal{L}(S)(r) = S(r) \ \} \\
& q \cup S(\mathcal{L}(Y(q))(r)) \cap \mathsf{grd}(G) \cap G(r) \\
= & \qquad \{ \text{ Liberal set transformer of guarded and preconditioned events } \} \\
& (\overline{q} \Longrightarrow \mathsf{grd}(G) \cap G(r) \mid S)(\mathcal{L}(Y(q)(G))(r)) \\
= & \qquad \{ \text{ extreme solution of recursive equation } \} \\
& \mathsf{FIX}(\overline{q} \Longrightarrow \mathsf{grd}(G) \cap G(r) \mid S)
\end{array}
$$

For $r = u$ we prove:

$$\mathcal{L}(X(q)(G))(u) = u$$

First, we note that equality $\mathcal{L}(X(q)(G))(u) = \mathsf{FIX}(\overline{q} \Longrightarrow S)$ holds:

$$
\begin{array}{ll}
& \mathcal{L}(Y(q)(G))(u) \\
= & \qquad \{ \text{ (17), Liberal set transformer of guard and dovetail } \} \\
& q \cup \mathcal{L}(S \,;\, Y(q))(u) \cap \mathcal{L}(\mathsf{grd}(G) \mid G)(u) \\
= & \qquad \{ \text{ } \mathcal{L}(\mathsf{grd}(G) \mid G)(u) = u \text{ } \} \\
& q \cup \mathcal{L}(S \,;\, Y(q))(u) \\
= & \qquad \{ \text{ } S(u) = u, \text{ set transformers } \} \\
& (\overline{q} \Longrightarrow S)(\mathcal{L}(Y(q)(G))(u)) \\
= & \qquad \{ \text{ extreme solution } \} \\
& \mathsf{FIX}(\overline{q} \Longrightarrow S)
\end{array}
$$

As $(\overline{q} \Longrightarrow S)(u) = u$ holds, it follows: $u \subseteq \mathsf{FIX}(\overline{q} \Longrightarrow S)$. Therefore, $\mathcal{L}(X(q)(G))(u) = u$ follows from $u \subseteq \mathsf{FIX}(\overline{q} \Longrightarrow S)$ and equality. □

D.3 Proof of (20): $\mathcal{L}(Y(q)(G))(r) \subseteq \mathsf{pre}(Y(q)(G))$

$$
\begin{array}{ll}
& \mathcal{L}(Y(q)(G))(r) \\
= & \qquad \{ \text{ (19) and fixpoint property } \} \\
& q \cup \mathsf{grd}(G) \cap G(r) \cap S(\mathcal{L}(Y(q)(G))(r)) \\
\subseteq & \qquad \{ \text{ set theory } \} \\
& q \cup \mathsf{grd}(G) \\
\subseteq & \qquad \{ \text{ set theory } \} \\
& q \cup \mathsf{grd}(G) \cup \overline{S(q)} \cap S(\mathsf{pre}(Y(q)(G))) \\
= & \qquad \{ \text{ set transformers } \} \\
& (\overline{q} \cap G(\varnothing) \Longrightarrow (\overline{S(q)} \mid S))(\mathsf{pre}(Y(q)(G))) \\
= & \qquad \{ \text{ (18) and fixpoint property } \} \\
& \mathsf{pre}(Y(q)(G))
\end{array}
$$

□

D.4 Monotonicity of Fair Loop: $a \subseteq b \Rightarrow Y(q)(G)(a) \subseteq Y(q)(G)(b)$

Let a and b be two subsets of u, $F(q)(a)$ and $F(q)(b)$ be the following set transformers:

$$
\begin{array}{l}
F(q)(a) = (\overline{q} \Longrightarrow G(a) \cap \mathsf{grd}(G) \mid S) \\
F(q)(b) = (\overline{q} \Longrightarrow G(b) \cap \mathsf{grd}(G) \mid S)
\end{array}
$$

$a \subseteq b$

$\Rightarrow$ { Monotonicity of G }

$G(a) \subseteq G(b)$

$\Rightarrow$ { set theory }

$\forall r \cdot (r \subseteq u \Rightarrow (q \cup G(a) \cap \mathsf{grd}(G) \cap S(r)) \subseteq (q \cup G(b) \cap \mathsf{grd}(G) \cap S(r)))$

$\equiv$ { set transformers }

$\forall r \cdot (r \subseteq u \Rightarrow (\overline{q} \Longrightarrow G(a) \cap \mathsf{grd}(G) \mid S)(r) \subseteq (\overline{q} \Longrightarrow G(b) \cap \mathsf{grd}(G) \mid S)(r))$

$\equiv$ { def. $F(q)(a)$ and $F(q)(b)$ }

$\forall r \cdot (r \subseteq u \Rightarrow F(q)(a)(r) \subseteq F(q)(b)(r))$

$\Rightarrow$ { set theory }

$\forall r \cdot (r \subseteq u \Rightarrow (r \subseteq F(q)(a)(r)) \Rightarrow r \subseteq F(q)(b)(r))$

$\Rightarrow$ { set theory }

$\{\, r \mid r \subseteq u \wedge r \subseteq F(q)(a)(r) \,\} \subseteq \{\, r \mid r \subseteq u \wedge r \subseteq F(q)(b)(r) \,\}$

$\Rightarrow$ { set theory }

$\bigcup(\{\, r \mid r \subseteq u \wedge r \subseteq F(q)(a)(r) \,\}) \subseteq \bigcup(\{\, r \mid r \subseteq u \wedge r \subseteq F(q)(b)(r) \,\})$

$\Rightarrow$ { def. $\mathsf{FIX}(f)$, $F(q)(a)$ and $F(q)(b)$ }

$\mathsf{FIX}(\overline{q} \Longrightarrow G(a) \cap \mathsf{grd}(G) \mid S) \subseteq \mathsf{FIX}(\overline{q} \Longrightarrow G(b) \cap \mathsf{grd}(G) \mid S)$

$\equiv$ { (21) }

$Y(q)(G)(a) \subseteq Y(q)(G)(b)$

□

D.5 Guard of Fair Loop: $\mathsf{grd}(Y(q)(G)) = \overline{q}$

$\mathsf{grd}(Y(q)(G))$

$=$ { def. guard }

$\overline{Y(q)(G)(\varnothing)}$

$=$ { (17) }

$\overline{q \cup ((S \,;\, Y(q)(G)) \triangledown (\mathsf{grd}(G) \mid G))(\varnothing)}$

$=$ { set theory }

$\overline{q} \cap \overline{((S \,;\, Y(q)(G)) \triangledown (\mathsf{grd}(G) \mid G))(\varnothing)}$

$=$ { def. guard dovetail }

$\overline{q} \cap (\mathsf{grd}(S \,;\, Y(q)(G)) \cup \mathsf{grd}(\mathsf{grd}(G) \mid G))$

$=$ { $\mathsf{grd}(\mathsf{grd}(G) \mid G) = u$ }

$\overline{q}$

□

D.6 Strictness of W_w: $W_w(\varnothing) = \varnothing$

$W_w(\varnothing)$

$=$ { (22) }

$\bigcup G \cdot (G \in \mathcal{S} \mid Y(\varnothing)(G)(\varnothing))$

$=$ { def. of grd }

$\bigcup G \cdot (G \in \mathcal{S} \mid \overline{\mathsf{grd}(Y(\varnothing)(G))})$

$=$ { $\mathsf{grd}(Y(\varnothing)(G)) = \overline{\varnothing}$ }

$\bigcup G \cdot (G \in \mathcal{S} \mid \overline{\overline{\varnothing}})$

$=$

$\varnothing$

□

D.7 Monotonicity of W_w: $a \subseteq b \Rightarrow W_w(a) \subseteq W_w(b)$

First we prove, for any subset a and b of u, $a \subseteq b \Rightarrow Y(a)(G)(b) \subseteq Y(b)(G)(b)$.
Let $T(a) = \mathsf{FIX}(\overline{a} \Longrightarrow (\mathsf{grd}(G) \wedge G(b) \mid S))$:

$$
\begin{array}{ll}
& a \subseteq b \\
\Rightarrow & \{\ \text{for any } G \in \mathcal{S}\ \} \\
& a \cup \mathsf{grd}(G) \cap G(b) \cap S(T(a)) \subseteq b \cup \mathsf{grd}(G) \cap G(b) \cap S(T(a)) \\
\equiv & \{\ \text{prop. } \mathsf{FIX}\ \} \\
& T(a) \subseteq b \cup \mathsf{grd}(G) \cap G(b) \cap S(T(a)) \\
\equiv & \{\ \text{guarded set transformer}\ \} \\
& T(a) \subseteq (\overline{b} \Longrightarrow \mathsf{grd}(G) \cap G(b) \mid S)(T(a)) \\
\Rightarrow & \{\ \text{prop. } \mathsf{FIX}\ \} \\
& T(a) \subseteq \mathsf{FIX}(\overline{b} \Longrightarrow \mathsf{grd}(G) \cap G(b) \mid S) \\
\equiv & \{\ (21)\ \} \\
& Y(a)(G)(b) \subseteq Y(b)(G)(b)
\end{array}
$$

Now, the proof of monotonicity is:

$$
\begin{array}{ll}
& a \subseteq b \\
\Rightarrow & \{\ \text{monotonicity of } Y(q)(G) \text{ for } q = a \text{ and } G \in \mathcal{S}\ \} \\
& Y(a)(G)(a) \subseteq Y(a)(G)(b) \\
\Rightarrow & \{\ Y(a)(G)(b) \subseteq Y(b)(G)(b)\ \} \\
& Y(a)(G)(a) \subseteq Y(b)(G)(b) \\
\Rightarrow & \\
& Y(a)(G)(a) \subseteq \bigcup G' \cdot (G' \in \mathcal{S} \mid Y(b)(G')(b)) \\
\Rightarrow & \\
& \bigcup G \cdot (G \in \mathcal{S} \mid Y(a)(G)(a)) \subseteq \bigcup G' \cdot (G' \in \mathcal{S} \mid Y(b)(G')(b)) \\
\equiv & \{\ (22)\ \} \\
& W_w(a) \subseteq W_w(b)
\end{array}
$$

□

E Proofs of section 4

E.1 Proof of (30): $\forall n \cdot (n \in \mathbb{N} \Rightarrow v'(n) = \bigcup i \cdot (i \in \mathbb{N} \land i < n \mid v(i)))$

The proof is by induction over $\mathbb{N}$. The base case:

$$
\begin{array}{ll}
& v'(0) \\
= & \qquad \{\ \text{def. } v'\ \} \\
& \{\, z \mid z \in u \land V(z) < 0 \,\} \\
= & \qquad \{\ V \in u \to \mathbb{N}\ \} \\
& \varnothing \\
= & \qquad \{\ \text{empty range}\ \} \\
& \bigcup i \cdot (i \in \mathbb{N} \land i < 0 \mid v(i))
\end{array}
$$

Inductive step:

$$
\begin{array}{ll}
& v'(n) = \bigcup i \cdot (i \in \mathbb{N} \land i < n \mid v(i)) \\
\Rightarrow & \\
& v'(n) \cup v(n) = \bigcup i \cdot (i \in \mathbb{N} \land i < n \mid v(i)) \cup v(n) \\
\Rightarrow & \qquad \{\ \text{def. } v \text{ and } v'\ \} \\
& v'(n+1) = \bigcup i \cdot (i \in \mathbb{N} \land i < n+1 \mid v(i))
\end{array}
$$

□

E.2 Proof of (31): $\bigcup i \cdot (i \in \mathbb{N} \mid v'(i+1)) = \bigcup i \cdot (i \in \mathbb{N} \mid v(i))$

$$
\begin{array}{ll}
& \bigcup i \cdot (i \in \mathbb{N} \mid v'(i+1)) \\
= & \qquad \{\ \text{def. } v'\ \} \\
& \bigcup i \cdot (i \in \mathbb{N} \mid \{\, z \mid z \in u \land V(z) < i+1 \,\}) \\
= & \\
& \bigcup i \cdot (i \in \mathbb{N} \mid \{\, z \mid z \in u \land V(z) \leq i \,\}) \\
= & \\
& \bigcup i \cdot (i \in \mathbb{N} \mid \{\, z \mid z \in u \land V(z) = i \,\}) \\
= & \qquad \{\ \text{def. } v\ \} \\
& \bigcup i \cdot (i \in \mathbb{N} \mid v(i))
\end{array}
$$

□

E.3 Proof of (32): $\bigcup i \cdot (i \in \mathbb{N} \mid v(i)) = u$

$$
\begin{array}{ll}
& u \subseteq \bigcup i \cdot (i \in \mathbb{N} \mid v(i)) \\
\Leftarrow & \qquad \{\ \text{set. theory}\ \} \\
& \forall x \cdot (x \in u \Rightarrow x \in \bigcup i \cdot (i \in \mathbb{N} \mid v(i))) \\
\equiv & \\
& \forall x \cdot (x \in u \Rightarrow \exists i \cdot (i \in \mathbb{N} \land x \in v(i))) \\
\equiv & \qquad \{\ \text{def. } v\ \} \\
& \forall x \cdot (x \in u \Rightarrow \exists i \cdot (i \in \mathbb{N} \land V(x) = i)) \\
\Leftarrow & \\
& V \in u \to \mathbb{N}
\end{array}
$$

□

E.4 Proof of (33): $\forall n \cdot (n \in \mathbb{N} \Rightarrow \bigcup i \cdot (i \in \mathbb{N} \wedge i \leq n \mid v(i)) \cap p \subseteq f^{n+1})$

The proof is by induction. Base case:

1. $\forall n \cdot (n \in \mathbb{N} \Rightarrow v(n) \cap p \subseteq f(v'(n)))$; premise
2. $v(0) \cap p \subseteq f(v'(0))$; 1
3. $v(0) \cap p \subseteq f(\varnothing)$; 2 and def v'
4. $v(0) \cap p \subseteq f^1$; $f(\varnothing) = f^1$ (6)
5. $\bigcup i \cdot (i \in \mathbb{N} \wedge i \leq 0 \mid v(i)) \cap p \subseteq f^{0+1}$; 4

Inductive step:

1. $\bigcup i \cdot (i \in \mathbb{N} \wedge i \leq n \mid v(i)) \cap p \subseteq f^{n+1}$; Inductive hyp.
2. $f(\bigcup i \cdot (i \in \mathbb{N} \wedge i \leq n \mid v(i)) \cap p) \subseteq f(f^{n+1})$; 1 and monotonic f
3. $\forall n \cdot (n \in \mathbb{N} \Rightarrow v(n) \cap p \subseteq f(v'(n)))$; premise
4. $v(n+1) \cap p \subseteq f(v'(n+1))$; 3
5. $v'(n+1) = \bigcup i \cdot (i \in \mathbb{N} \wedge i \leq n \mid v(i))$; from (30)
6. $p \subseteq f(p)$; premise
7. $v(n+1) \cap p \subseteq f(v'(n+1)) \cap f(p)$; 6 and 4
8. $v(n+1) \cap p \subseteq f(v'(n+1) \cap p)$; 7 and conjunct. f
9. $v(n+1) \cap p \subseteq f(f^{n+1})$; 8, 5 and 2
10. $f^{n+1} \subseteq f^{n+2}$; from (6)
11. $\bigcup i \cdot (i \in \mathbb{N} \wedge i \leq n \mid v(i)) \cap p \subseteq f^{n+2}$; 10 and 1
12. $\bigcup i \cdot (i \in \mathbb{N} \wedge i \leq n \mid v(i)) \cap p \cup v(n+1) \cap p \subseteq f^{n+2}$; 11, 9 and (6)
13. $\bigcup i \cdot (i \in \mathbb{N} \wedge i \leq n+1 \mid v(i)) \cap p \subseteq f^{n+2}$; 12

□

E.5 Proof of (34): $\forall \alpha \cdot (\mathcal{F}_w(b)^\alpha \subseteq b \cup (\mathsf{grd}(S) \cap S(\mathsf{fix}(\mathcal{F}_w(b)))))$

The proof is given by transfinite induction considering the following abbreviations:

$$B = \mathsf{fix}(\mathcal{F}_w(b)) \tag{61}$$

$$F = \mathcal{F}_w(b) \tag{62}$$

Successor ordinal:

1. $\mathcal{F}_w(b)^\alpha \subseteq b \cup (\mathsf{grd}(S) \cap S(B))$; Ind. Hyp.
2. $\mathcal{F}_w(b)(F^\alpha) = b \cup W_w(F^\alpha)$; (23)
3. $\mathcal{F}_w(b)(F^\alpha) = b \cup \bigcup G \cdot (G \in \mathcal{S} \mid Y(F^\alpha)(G)(F^\alpha))$; 2 and (22)
4. $\mathcal{F}_w(b)(F^\alpha) = b \cup \bigcup G \cdot (G \in \mathcal{S} \mid \mathsf{FIX}(\overline{F^\alpha} \Longrightarrow \mathsf{grd}(G) \cap G(F^\alpha) \mid S))$; 3 and (21)
5. $\mathcal{F}_w(b)(F^\alpha) = b \cup \bigcup G \cdot (G \in \mathcal{S} \mid F^\alpha \cup (\mathsf{grd}(G) \cap G(F^\alpha) \cap S(Y(F^\alpha)(G)(F^\alpha))))$; 4
6. $\mathcal{F}_w(b)(F^\alpha) \subseteq b \cup \bigcup G \cdot (G \in \mathcal{S} \mid F^\alpha \cup (\mathsf{grd}(G) \cap S(Y(F^\alpha)(G)(F^\alpha))))$; 5
7. $\mathcal{F}_w(b)(F^\alpha) \subseteq b \cup \bigcup G \cdot (G \in \mathcal{S} \mid F^\alpha \cup (\mathsf{grd}(G) \cap S(W_w(F^\alpha))))$; 6 and (22)
8. $\mathcal{F}_w(b)(F^\alpha) \subseteq b \cup \bigcup G \cdot (G \in \mathcal{S} \mid F^\alpha \cup (\mathsf{grd}(S) \cap S(W_w(F^\alpha))))$; 7 $\mathsf{grd}(G) \subseteq \mathsf{grd}(S)$
9. $\mathcal{F}_w(b)(F^\alpha) \subseteq b \cup \bigcup G \cdot (G \in \mathcal{S} \mid F^\alpha \cup (\mathsf{grd}(S) \cap S(\mathcal{F}_w(b)(F^\alpha))))$; 8 and (23)
10. $\mathcal{F}_w(b)^{\alpha+1} \subseteq b \cup F^\alpha \cup (\mathsf{grd}(S) \cap S(\mathcal{F}_w(b)^{\alpha+1}))$; 9 and (6)
11. $\mathcal{F}_w(b)^{\alpha+1} \subseteq b \cup F^\alpha \cup (\mathsf{grd}(S) \cap S(B))$; 10 and (6)
12. $\mathcal{F}_w(b)^{\alpha+1} \subseteq b \cup (\mathsf{grd}(S) \cap S(B))$; 11 and 1

Limit ordinal:

1. $\forall \beta \cdot (\beta < \alpha \Rightarrow F^{\beta} \subseteq b \cup \mathsf{grd}(S) \cap S(B))$; Ind. Hyp
2. $F(F^{\beta}) = b \cup W_w(F^{\beta})$; (23), $\beta < \alpha$
3. $F(F^{\beta}) = b \cup \bigcup G \cdot (G \in \mathcal{S} \mid Y(F^{\beta})(G)(F^{\beta}))$; (22)
4. $F(F^{\beta}) = b \cup \bigcup G \cdot (G \in \mathcal{S} \mid \mathsf{FIX}(\overline{F^{\beta}} \Longrightarrow \mathsf{grd}(G) \cap G(F^{\beta}) \mid S))$; 3, (21)
5. $F(F^{\beta}) = b \cup \bigcup G \cdot (G \in \mathcal{S} \mid F^{\beta} \cup (\mathsf{grd}(G) \cap G(F^{\beta}) \cap S(Y(F^{\beta})(G)(F^{\beta}))))$; 4
6. $F(F^{\beta}) \subseteq b \cup F^{\beta} \cup (\mathsf{grd}(S) \cap S(F(F^{\beta})))$; 5, (22) and (23)
7. $F(F^{\beta}) \subseteq b \cup F^{\beta} \cup (\mathsf{grd}(S) \cap S(B))$; 6 and (9)
8. $F(F^{\beta}) \subseteq b \cup (\mathsf{grd}(S) \cap S(B))$; 7, 1 $\beta < \alpha$
9. $\bigcup \beta \cdot (b < \alpha \mid F(F^{\beta})) \subseteq b \cup (\mathsf{grd}(S) \cap S(B))$; 8
10. $F^{\alpha} \subseteq b \cup (\mathsf{grd}(S) \cap S(B))$; 9 and (6)

Using (34), the proof of sufficient conditions is as follows:

1. $\forall n \cdot (n \in \mathbb{N} \Rightarrow \overline{b} \cap v(n) \subseteq S(v'(n)))$; premise
2. $a \mapsto b \in \pounds_w$; premise
3. $\forall \alpha' \cdot (\mathcal{F}_w(b)^{\alpha'} \subseteq b \cup (\mathsf{grd}(S) \cap S(\mathsf{fix}(\mathcal{F}_w(b)))))$; (34)
4. $\exists \alpha \cdot (\mathsf{fix}(\mathcal{F}_w(b)) = \mathcal{F}_w(b)^{\alpha})$; Theorem 1
5. $\mathsf{fix}(\mathcal{F}_w(b)) \subseteq b \cup (\mathsf{grd}(S) \cap S(\mathsf{fix}(\mathcal{F}_w(b))))$; 4 and 3
6. $\mathsf{fix}(\mathcal{F}_w(b)) \subseteq \mathcal{F}_m(b)(\mathsf{fix}(\mathcal{F}_w(b)))$; 5 and (13)
7. $a \mapsto b \in \mathcal{T}_w$; 2, equality (29)
8. $a \subseteq \mathsf{fix}(\mathcal{F}_w(b))$; 7 and def. $\mathcal{T}_w$
9. $\mathsf{fix}(\mathcal{F}_w(b)) \cap \overline{b} \subseteq \mathsf{grd}(S)$; 5
10. $\forall n \cdot (n \in \mathbb{N} \Rightarrow \overline{b} \cap \mathsf{fix}(\mathcal{F}_w(b)) \cap v(n) \subseteq \mathsf{grd}(S) \cap S(v'(n)))$; 9 and 1
11. $\forall n \cdot (n \in \mathbb{N} \Rightarrow \mathsf{fix}(\mathcal{F}_w(b)) \cap v(n) \subseteq b \cup \mathsf{grd}(S) \cap S(v'(n)))$; 10
12. $\forall n \cdot (n \in \mathbb{N} \Rightarrow \mathsf{fix}(\mathcal{F}_w(b)) \cap v(n) \subseteq \mathcal{F}_m(b)(v'(n)))$; 11 and (13)
13. $\mathsf{fix}(\mathcal{F}_w(b)) \subseteq \mathsf{fix}(\mathcal{F}_m(b))$; 12, 6 and th. 3
14. $a \subseteq \mathsf{fix}(\mathcal{F}_m(b))$; 13 and 8
15. $a \mapsto b \in \mathcal{T}_m$; 14 and def. $\mathcal{T}_m$
16. $a \mapsto b \in \pounds_m$; 15, equality (16)

□