COMPOSITIONAL VERIFICATION AND SPECIFICATION OF REFINEMENT FOR REACTIVE SYSTEMS IN A DENSE TIME TEMPORAL LOGIC

Dissertation
zur Erlangung des Doktorgrades
der Technischen Fakultät
der Christian-Albrechts-Universität
zu Kiel

vorgelegt von
Antonio Cau

Kiel,
im August 1995

Berichterstatter:	Prof. Dr. Willem-Paul de Roever
	....
Tag der mündlichen Prüfung :	14 Dezember 1995 ....
Zum Druck genehmigt:	Kiel, den 14 Dezember 1995 ....

....

(Dekan)

Abstract

This thesis introduces a compositional dense time temporal logic for the composition and refinement of reactive systems. A reactive system is specified by a pair consisting of a machine and a condition on the computations of this machine. In order to compose reactive systems, each step in a computation has additionally composition information such as "this is a system step", or "this is an environment step" or "this is a communication step". By defining a merge operator that merges two steps into one step compositionality is achieved. Because a dense time temporal logic is used refinement can be expressed easily in this logic. Existing proof rules for refinement are reformulated in our formalism. The notion of relative refinement is introduced to handle refinement of systems that only under certain conditions are considered to be correct refinements. The proof rules for "normal" refinement are extended to handle relative refinement of systems. Relative refinement is used to formalize Dijkstra's development strategy for the solution of the readers/writers problem and to formalize a development strategy for certain fault tolerant systems. This development strategy is applied to the development of a fault tolerant storage system.

Acknowledgements

I would like to thank my advisor Willem-Paul de Roever for his guidance and his scientific support especially during the first two years of writing this thesis. Without his support this thesis would be just "spaghetti code". Special thanks go to Pierre Collette, the collaboration with whom was very agreeable and fruitful and led to many insights. I would like to thank all my colleagues of the group "Software Technology" at the Christian-Albrecht-University for their support, especially Yassine Lakhneche, who made many invaluable comments during the last stage of the thesis, Kai Engelhardt, who acted as a "finite variability condition" with respect to the changes I wanted to make in my thesis, and Qiwen Xu with whom I started to collaborate after he left the group. Also members of the other groups at the Christian Albrechts University are thanked for their comments, especially Thomas Wilke. I also want to thank Ruurd Kuiper for his help and comments during the first and last stage of the thesis. Finally I would like to thank the Personalrat and the Technical Faculty of the Christian Albrechts University in the persons of Reimer Hansen and Frank Paul for their efforts in extending my contract for 4 months, thus enabling me to finish this thesis. Last but not least I want to thank Änne Straßner for her (moral) support during the last stage of the thesis.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

Current formal methods are far from solving the problems in software development. The simplest view of the formal paradigm is that one starts with a formal specification and subsequently decomposes this specification in subspecifications which composed together form a correct refinement. These subspecifications are decomposed into "finer" subspecifications. This refinement process is continued until one gets subspecifications for which an implementation can easily be given. This view is too idealistic in a number of respects. First of all, most specifications of software are wrong (certainly most informal ones, unless they have been formally analyzed) and contain inconsistencies [PWT90]. Secondly, even if a formal specification is produced, this is only after a number of approximation steps because writing a correct specification is an even more difficult process than producing a correct implementation, and should therefore be structured, resulting in a number of increasingly less abstract layers with specifications which tend to increase in detail (and therefore become less readable [LGdR79]). Thirdly, even an incorrect refinement step may be useful in the sense that from this incorrect refinement step one can sometimes easier derive the correct refinement step. This is especially the case with intricate algorithms such as those concerning specific strategies for solving the mutual exclusion problem. An interesting illustration of this third view is provided by E.W. Dijkstra's "Tutorial on the split binary semaphore" [Dij79] in which he solves the readers/writers problem by subsequently improving incorrect refinement steps till they are correct. If this master of style prefers to approximate and finally arrive at his correct solution using formally "incorrect" intermediate stages, one certainly expects that a formally correct development process for that paradigm is difficult to find! The strategy described in [Dij79] is necessarily informal, reflecting the state of the art in 1979.

In Chapter 2 a dense time formalism is introduced for the specification and verification of refinement of systems based on [BKP86, DK90, KMP93, Sta84, Sta85, Sta88]. This formalism will be used to describe above strategy of incorrect intermediate stages. A dense time formalism is used because it allows one to deal with the stutter-problem (explained in section 2.1) and it enables one to express hiding of "internal" variables by existential quantification. Instead of using the assumption/commitment approach of [AL93a, AL93b, Jon83, MC81, PJ91, Pnu85, Sti88, Stø91, WD88, ZdBdR84, ZdRvEB84] , unified in [XCC94, CC94], in order to achieve compositionality an event variable is used that stores "compositionality information" like "this is a system step" or "this is an environement step" or "this is a communication step". A merging operator, first version defined in [Acz83], based on the one defined in [CC94] is introduced to merge this "compositionality information" of the components into "compositionality information" of the composed system. The use of event variables has as second advantage that existing proof rules for refinement like those in [Lam91, KMP93] can easily be extended to our framework. The notion of relative refinement is introduced to handle "incorrect" development steps. The system specification is therefore extended by a requirement that extracts the "good" computations of the system. The refinement proof rules are extended to handle relative refinement so that the correct part of incorrect development steps can be proven correct.

In Chapter 3 we present Dijkstra's development strategy of the readers/writers problem [Dij79] in our formalism. A preliminary version of this formalization, without proofs, appeared in [CKdR92] using the original formalism of [Sta84]. Our formalism preserves the flavour of the informal strategy in that it formalises Dijkstra's argumentation in terms of incorrect approximations to a correct program and provides a formal criterion for recognising when a formally correct end product, the correct program, has finally been reached.

In Chapter 4 we present a formal development strategy for the development of certain fault tolerant systems using our notion of relative refinement. A preliminary version of this strategy appeared in [CdR93b, CdR93a] using the original formalism of [Sta84]. The formal strategy is as follows: one starts with an implementation for a specified fault tolerant system. This implementation contains some faults, i.e., the refinement step is incorrect because of these faults. It is however relative correct because when these faults don't occur it is a correct implementation. In the next step we try to detect these faults, i.e., we construct a detection layer upon the previous implementation that stops that implementation when it detects an error caused by these faults. This is called a fail-stop implementation [LA90] and represents an improvement over the previous implementation because now at least the implementation stops on the occurrence of such a fault. The second implementation is also relatively correct because no occurrence of faults and the detection layer doesn't detect any error due to a fault then the second implementation is correct. In the third approximation we recover these errors, i.e., we don't stop anymore upon the detection of an error but merely recover the error by executing some special program that neutralizes that error. This third approximated refinement step is correct under the assumption that certain conditions are fulfilled, which exclude the occurrence of faults different from those whose errors are neutralized, i.e., it is again relative correct. This strategy is used for the development of a fault tolerant storage system, a so called stable storage.

Chapter 2

A Dense Model Formalism

2.1 Introduction

In this chapter we present a refinement method for reactive systems. A system is called reactive if it maintains some ongoing interaction with its environment, for example an operating system. This contrasts with transformational systems where from some input without further interaction output is produced. Because of this characteristic reactive systems should be described as sets of behaviours (histories). The underlying model for these behaviours is dense. The method which we present is based on the work of E.W. Stark [Sta84, Sta85, Sta88]. Here we present a framework which can model both CSP based and shared variable based concurrency, using the work of [BKP86, DK90, KMP93].

In section 2.2 reactive systems are specified by sets of histories together with a basis. A history is pair consisting of an event and a state function. The domains of these functions are the non-negative real numbers (the underlying dense model). The event function maps each non-negative real number to an event (an action occurring during the operation of the system and its environment) and the state function maps each real number to a state of the system and its environment. The intuition is that an occurrence of an action causes (potentially) a state change as illustrated in Figure 2.1. The basis is a pair consisting of an action basis and a process basis, where the action basis specifies the input and output channels over which the system communicates with its environment and the process basis specifies the local (only accessible by the system) and shared (accessible by both system and its environment) variables. Due to this basis composition of reactive systems corresponds to conjunction. Note that in for instance Lamport's work on TLA [Lam91, Lam94, Lam] this is not always the case: $x := 1 \| x := 1$ must be modeled as disjunction because conjunction leads to a "one process" specification $x := 1$. In our model however, it can be modeled as conjunction because the specification of one component also contains environmental information, especially about the other component. With a "conjoining" operator the histories of both components are merged into a history of the composite one. This conjoining operator based on [CC94] corresponds in our model almost to conjunction and is actually an extended version of Aczel's one [Acz83] because it also can handle CSP based concurrency whereas Aczel's one can only handle shared variable based concurrency.

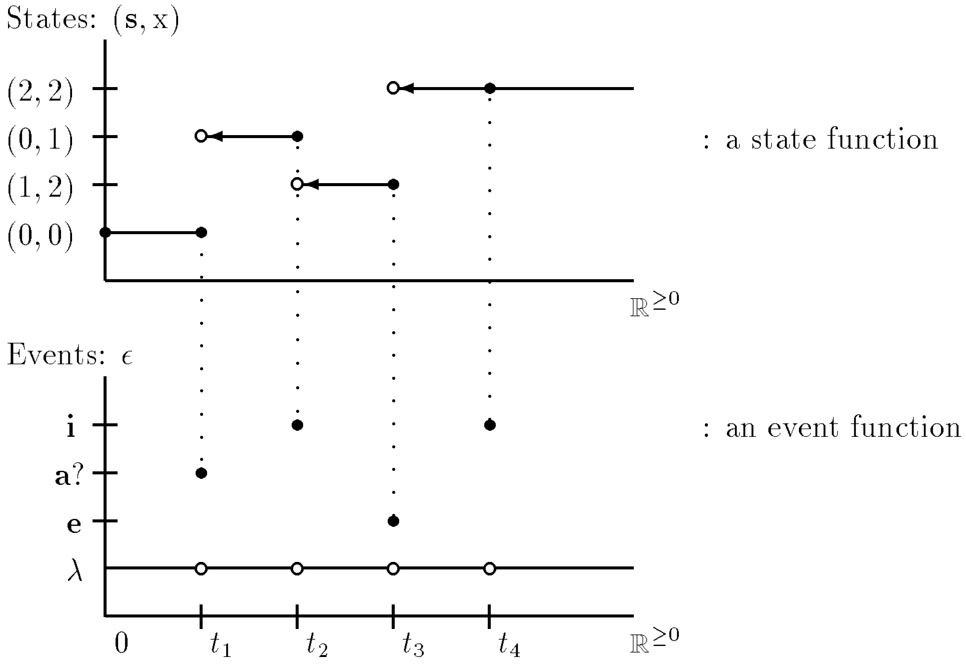

Figure 2.1: This picture illustrates the notion of state and event function, which together characterize the notion of computation of a machine. It illustrates the following computation: initially $(\mathbf{s}, \mathrm{x}) = (0, 0)$, the event $\mathbf{a}?$ changes x into 1, i.e., $\mathbf{s}$ doesn't change. In the interval $[0, t_1)$ there are only λ events. The event $\mathbf{i}$ at point t_2 changes $(\mathbf{s}, \mathrm{x})$ into $(1, 2)$, at point t_3 the event $\mathbf{e}$ changes $\mathbf{s}$ into 2 and at point t_4 the event $\mathbf{i}$ doesn't change $\mathbf{s}$ or x.

A notion of a machine is introduced for generating these histories, i.e., a history is a computation generated by a machine. With this machine notion only safety properties, i.e., sets of histories generated by a machine, of a system can be specified, so an extra condition on the computations of this machine is introduced for specifying liveness properties of the system.

The use of real numbers as domain for the event and state function handles the stutter problem. This problem, first observed by Lamport [Lam83, Lam89], is as follows. Given two behaviours of a system, let the first behaviour contain only consecutive snap-shots of the system that differ from each other whereas the second behaviour contains the same snap-shots but also some consecutive ones that are identical. This is called stuttering. From the viewpoint of an observer these behaviours are considered as equal. Consequently, any formalism that allows to distinguish between these behaviours is not abstract enough and has a power of discrimination which is too strong. An example of such a formalism is linear temporal logic with a next operator $\bigcirc$. In the present formalism this excessive expressive power is avoided as follows: state changes caused by events happen only now and then, so that in between each two consecutive changes there are uncountably many instants of time at which *nothing* happens. Consequently, it is impossible to count, or express, stutter steps. Furthermore the use of real numbers for defining the event and state function enables us to express hiding of variables as existential quantification and consider refinement as implication, even if there are more "states" on the abstract level than on the concrete level: let the history illustrated in Figure 2.1 be a history at the abstract level where x is the variable that should be hidden and let the history illustrated in Figure 2.2 be a history at the concrete level. The history of Figure 2.2 is a refinement of the history of Figure 2.1.

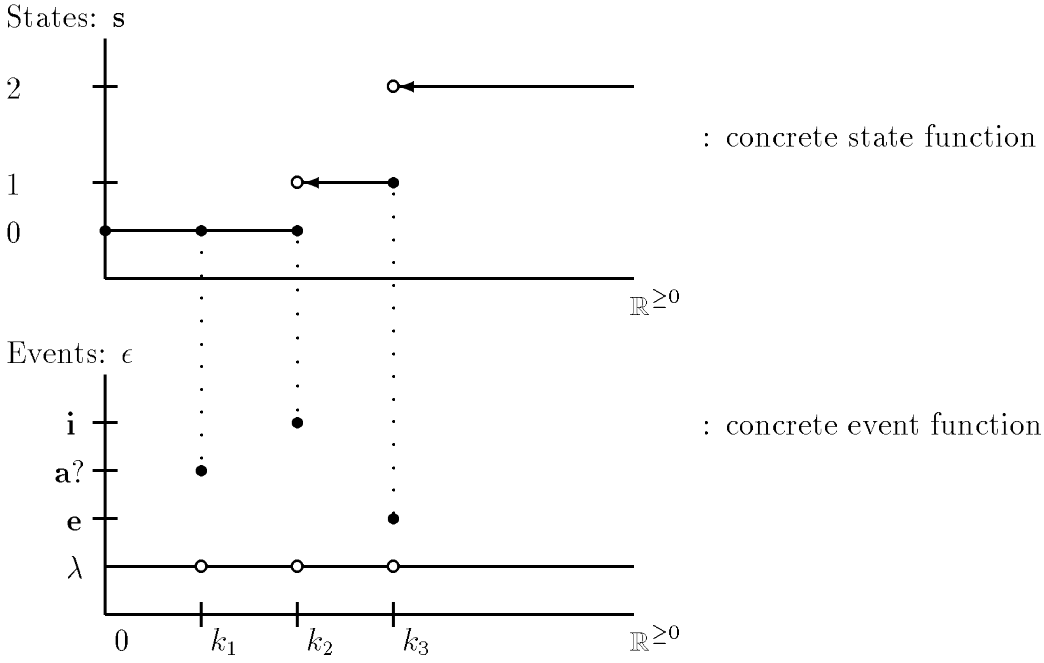

Figure 2.2: This picture illustrates the following concrete computation: initially $\mathbf{s} = (0)$, the event **a**? doesn't change **s**, the event **i** changes **s** into 1, and the event **e** changes **s** into 2.

A dense time temporal logic DTL based on histories is introduced in section 2.2.2. This logic is based on [Sta84, Sta85, BKP86, DK90, KMP93]. A salient feature of the dense time temporal logic is the "immediately after" operator $'$, in a version which Lamport [Lam83] approves of, i.e., it is stutter insensitive. In this logic the notion of a machine and the condition on the computations of that machine will be expressed. It is also possible to express in this logic whether a system refines another system, i.e, the set of histories of the first system is a subset of the histories of the second one and the "observable" part of the abstract basis (i.e., observable from outside of the component) is equal to the "observable" part of the concrete basis. In our model initial stuttering is incorporated by default (cf. [DK90]) and refinement can be expressed using implication and existential quantification.

In section 2.3 the notions of composition and refinement of systems are defined. Firstly in terms of histories (semantically) and secondly in the dense time temporal logic DTL (syntactically). It is also investigated how composition relates to refinement, i.e., the notion of compositional refinement [ZCdR92] is given. Compositional refinement means intuitively that if the components of an abstract composed system are refined by the components of a concrete composed system then the abstract composed system is refined by the concrete composed system, i.e., refinement is preserved under composition.

Section 2.4 gives proof rules for refinement based on those given in [Lam91, KMP93]. These proof rules split the proof of refinement of systems into (1) a proof of refinement of the safety parts of the systems and (2) a proof of refinement of the liveness part of the systems.

Section 2.5 explains how the formalism can be used to describe relative (incorrect) refinement steps as discussed in Chapter 1. Also the notion of relative composition is introduced which intuitively means that only restricted parts of the components are composed together. The notion of compositional refinement of section 2.3 is extended to compositional relative refinement. The proof rules for refinement of section 2.4 are extended to handle relative refinement. These proof rules are used extensively in the readers/writers example of Chapter 3 and the stable storage example of Chapter 4.

2.2 Specification of Reactive Systems

This section explains how reactive systems can be specified. Firstly they will be specified at the semantical level, i.e., by sets of histories. A history intuitively specifies which event occurs at a particular point and in what state the system is at that particular point. Secondly reactive systems are specified using the dense time temporal logic DTL.

2.2.1 Semantic Specification of Reactive Systems

In [Sta84] a method for specifying reactive systems is introduced. Such systems are characterized by sets of histories. A history is a pair consisting of an event function and a state function. An event function records at each point (i.e., element of the positive reals, including zero) which *event* occurs. An event is an instantaneous occurrence of an action during the operation of a system, that can be generated by that system or its environment and that is of interest at the given level of abstraction. Four kinds of actions are distinguished:

1. *communication* actions $\mathbf{a}?, \mathbf{b}!$, i.e., actions that transmit information over a channel. A channel is a connection between the system and its environment.

2. *system* actions $\mathbf{i}$, i.e., non-communication actions of the system.

3. *environment* actions $\mathbf{e}$, i.e., non-communication actions of the environment.

4. *silent* actions λ, i.e., actions that don't influence the status of the system.

Event states are introduced in order to record which event occurs during the operation of the system. An event state is like the usual notion of state with the exception that instead of normal program variables *event variables* are used. An event state is defined formally in the following definition.

Definition 1 (Event variable and event state)
Let Chan *denote the set of all channels. Let* $\mathfrak{E}$ *denote the set of event variables with typical elements* $\epsilon, \epsilon_0, \epsilon_1, \ldots$. *Event variable* ϵ *will record which action occurs during the operation of the system, and the event variables* $\epsilon_0, \epsilon_1, \ldots$ *are auxiliary event variables recording which*

actions occur in components of the system. Let $\mathfrak{A}$ denote the set of actions, with typical elements $\mathbf{i}$ *(denoting system actions),* $\mathbf{e}$ *(denoting environment actions),* $\mathbf{a}?, \mathbf{b}!$[1] ... *denoting respectively an input communication action over channel* $\mathbf{a}$ *and an output communication action over channel* $\mathbf{b}$*, and* λ *denoting the silent action. An event state is a mapping* δ *from* $\mathfrak{E}$ *to* $\mathfrak{A}$*. Let* Δ *denote the set of all event states.*

An state function records at each point (a non-negative real number) the *process state*, i.e. the usual notion of state of a system and its environment. In order to distinguish the normal variables from the event variables the normal variables are called here *process variables*. Three kind of process variables are distinguished:

1. *shared* process variables which are "shared" between a system and its environment, and

2. *local* process variables which are only accessible by a system.

3. *rigid* variables which are not changed by the system and its environment, i.e., which are used for specification purposes.

The process state is defined formally in the following definition.

Definition 2 (Process variable and process state)
A process state is a mapping from variables to values. Let $\mathfrak{V}$ *denote the set of shared variables with typical elements* $\mathrm{s}, \ldots$*, and* $\mathfrak{X}$ *the set of local variables* ($\mathfrak{V} \cap \mathfrak{X} = \emptyset$) *with typical elements* $\mathrm{x}, \ldots$*, and* $\mathfrak{R}$ *the set of rigid variables with typical elements* $n, \ldots$*. A state is a mapping* σ *from* $\mathfrak{V} \cup \mathfrak{X} \cup \mathfrak{R}$ *to the set of values* Val*. Let* Σ *denote the set of all process states.*

As already said above, event and state functions are mappings from the non-negative reals to, respectively event and process states. Because of this some requirements are needed in order to specify "reasonable" histories. Here reasonable is used in the sense that in a bounded interval only a finite number of non-silent actions and process state changes can occur. This requirement is called the finite variability condition [BKP86]. Next several notions for functions from $\mathbb{R}^{\geq 0}$ (the positive reals including 0) to some domain D are introduced in order to define this requirement and to formally define the event and state functions.

Definition 3 (Left and right constant, limit)
Given function $f : \mathbb{R}^{\geq 0} \rightarrow D$*.*
f *is called* **left constant** *at* $t \in \mathbb{R}^{\geq 0}$*, if there exists a real number* t_0*,* $0 < t_0 < t$*, such that* $f(t_1) = d$ *for all* $t_1 \in (t_0, t)$*.* d *is called the* **left limit** *of* f *at* t*, and is denoted by* $\lim\limits_{t_1 \rightarrow t} f(t_1)$*.*
f *is called* **right constant** *at* $t \in \mathbb{R}^{\geq 0}$*, if there exists a real number* t_0*,* $t_0 > t$*, such that* $f(t_1) = d$ *for all* $t_1 \in (t, t_0)$*.* d *is called the* **right-limit** *of* f *at* t*, and is denoted by* $\lim\limits_{t \leftarrow t_1} f(t_1)$*.*

[1]In this chapter we omit the value part of the communication, i.e., which value is transmitted, in order to ease the formalism a little bit. In the example of the stable storage we will use this value part although it is not formally introduce in this chapter

Definition 4 (Left and right continuous, discontinuous)
Given function $f : \mathbb{R}^{\geq 0} \rightarrow D$.
f *is called* **left continuous**, *if* $f(t) = \lim_{t_1 \rightarrow t} f(t_1)$ *for every* $t > 0$.
f *is called* **right continuous**, *if* $f(t) = \lim_{t \leftarrow t_1} f(t_1)$ *for every* $t \geq 0$.
f *is called* **discontinuous** *at* t, *if* $f(t) \neq \lim_{t_1 \rightarrow t} f(t_1)$ *or* $f(t) \neq \lim_{t \leftarrow t_1} f(t_1)$.
f *is called* **strongly discontinuous** *at* t, *if* $f(t) \neq \lim_{t_1 \rightarrow t} f(t_1)$ *and* $f(t) \neq \lim_{t \leftarrow t_1} f(t_1)$.

Definition 5 (Finite variability)
Given function $f : \mathbb{R}^{\geq 0} \rightarrow D$.
f *has the* **finite variability** *property iff* f *has only finitely many points of discontinuity in any interval* $[a, b]$, $0 \leq a \leq b$, $a, b \in \mathbb{R}^{\geq 0}$.

Now *event* and *state* functions can be defined. [DK90] states that initial stuttering is needed in order to express refinement in a logic with the help of existential quantification and implication. We must first define what stuttering, in the sense of [DK90], is in our setting. In our setting a stutter step is a step in which a non-communication action doesn't change the state. So here this initial stuttering can included by requiring that in the first interval the event function has the constant value λ and the state function remains constant there. Furthermore a state should remain constant for an interval of points in order to be observable. Also non-λ events are considered to be single points. Another possibility would be for the events to remain constant during an interval of points. The intuitive meaning of a history is that the points of non-λ event occurrence mark the state changes. For the non-λ events the question to be answered is: at which point of the interval should the state change take place? Answer: at the last point of the interval of the event. So for events only the last point of the interval is interesting because it marks the state change. So why consider an interval if only its last point is interesting? This is the explanation of the choice made here that the non-λ events occur only at single points. This is captured by the following definitions.

Definition 6 (restriction)
For $g : A_1 \rightarrow A_2$, $A_0 \subseteq A_1$ *define* $g|^1_{A_0} : A_0 \rightarrow A_2$ *as* $g|^1_{A_0}(x) = g(x)$ *for* $x \in A_0$. *If* A_0 *is a set containing only one element* x *then we will write* $g|^1_x$ *instead of* $g|^1_{\{x\}}$.
For $g : A_1 \rightarrow (A_2 \rightarrow A_3)$, $A_0 \subseteq A_2$ *define* $g|^2_{A_0} : A_1 \rightarrow (A_0 \rightarrow A_3)$ *as* $g|^2_{A_0}(t)(x) = g(t)(x)$ *for* $x \in A_0$. *Again if* A_0 *is a set containing only one element* x *then we will write* $g|^2_x$ *instead of* $g|^2_{\{x\}}$

Definition 7 (Event function)
An **event function** ψ *is a function from* $\mathbb{R}^{\geq 0}$ *to* Δ, *such that* $\psi|^2_\epsilon$ *has the finite variability condition,* $\psi(0)(\epsilon) = \lambda$ *(i.e. initial stuttering) and for all points* t, ψ *is strongly discontinuous at* t *iff* $\psi(t)(\epsilon) \neq \lambda$ *(i.e. an event function is almost constant* λ*). Let* Ψ *denote the set of all event functions.*

Figure 2.1 illustrates the notion of event function. At point t_1 event **a**? occurs, at point t_2 event **i** occurs, at point t_3 event **e** occurs, and at all other points event λ occurs. Points t_1, t_2 and t_3 are here the strongly discontinuous points.

Definition 8 (State function)
A **state function** θ *is a left continuous function from* $\mathbb{R}^{\geq 0}$ *to* Σ *such that for all* $n \in \mathfrak{R}$ *and* $t \in \mathbb{R}^{\geq 0}$, $\theta(t)(n) = \theta(0)(n)$ *(i.e., the rigid variables don't change at all), and for all* $x \in \mathfrak{V} \cup \mathfrak{X}$, $\theta|_x^2$ *satisfies the finite variability property and* $\theta|_x^2(0)(x) = \lim_{0 \leftarrow t_1} \theta|_x^2(t_1)(x)$ *(i.e. initial stuttering). Let* Θ *denote the set of all state functions.*

Figure 2.1 illustrates the notion of state function. In interval $[0, t_1]$ the system is in state $(\mathbf{s}, \mathrm{x}) = (0, 0)$, in interval $(t_1, t_2]$ in state $(\mathbf{s}, \mathrm{x}) = (0, 1)$, in interval $(t_2, t_3]$ in state $(\mathbf{s}, \mathrm{x}) = (1, 2)$ and in interval $(t_2, \infty]$ in state $(\mathbf{s}, \mathrm{x}) = (2, 2)$. The event $\mathbf{i}$ at t_4 is an illustration of a non-λ stutter step.

The following definition combines the notions of state function and event function into the notion of history. Two requirements are imposed on the combination of event and state function in order to be a history. The first requirement is that silent actions don't give rise to process state changes. The second requirement is that communication actions don't change the shared variables; this requirement is imposed in order to model CSP [Hoa84] like processes.

Definition 9 (History)
A **history** h *is a pair* $\langle \psi, \theta \rangle$, *where* ψ *is an event function and* θ *is a state function s.t. a* λ *action doesn't change the values of variables from* $\mathfrak{V} \cup \mathfrak{X}$, *i.e.:*

$$\forall t : \psi(t)(\epsilon) = \lambda \rightarrow \theta(t) = \lim_{t \leftarrow t_1} \theta(t_1)$$

and a communication action doesn't change the values of shared variables, i.e.:

$$\forall t : \psi(t)(\epsilon) = \mathbf{a}? \rightarrow \theta(t)|_{\mathfrak{V}}^1 = \lim_{t \leftarrow t_1} \theta(t_1)|_{\mathfrak{V}}^1$$
$$\forall t : \psi(t)(\epsilon) = \mathbf{a}! \rightarrow \theta(t)|_{\mathfrak{V}}^1 = \lim_{t \leftarrow t_1} \theta(t_1)|_{\mathfrak{V}}^1$$

Let $\mathcal{H}$ *denote the set of all histories.*

The following definition defines when a history is stutter equivalent to another history. A *history collapse* function is introduced that takes a history and collapses it in such a way that the non-stutter steps only occur at discrete points (elements of $\mathbb{N}$) and at all remaining points stutter steps occur. Also a restricted version of the history stutter equivalence relation is defined, namely, restricted to the process state information. The last one will be used to define a "process state history stutter insensitive" logic DTL. This logic will be restricted to a special kind of formulae in order to obtain the "history stutter insensitive" logic.

Definition 10 (History collapse, stutter equivalent)
Given history $h \in \mathcal{H}$, *the* **history collapse** *denoted* $\natural_{\mathfrak{h}}(h)$ *is a function from* $\mathcal{H}$ *to* $\mathcal{H}$ *defined as* $\natural_{\mathfrak{h}}(h) \triangleq h \circ \mathrm{di}(h)$ *where* $\mathrm{di}(h)$ *is the* **discretization** *bijection for* h *from* $\mathbb{R}^{\geq 0}$ *to* $\mathbb{R}^{\geq 0}$ *and is defined as follows:*
Let $\mathrm{tt}(h, k)$ *be the function from* $\mathcal{H} \times \mathbb{N}$ *to* $\mathbb{R}^{\geq 0}$ *that gives the point in* $\mathbb{R}^{\geq 0}$ *of the k-th change in h, formally:*

$$\mathrm{tt}(h, 0) \triangleq 0$$
for $k > 0$,
$$\mathrm{tt}(h, k) \triangleq \; min(t : \; t > \mathrm{tt}(h, k-1) \wedge (\psi(t)(\epsilon) \notin \{\lambda, \mathbf{i}, \mathbf{e}\} \vee \theta(t) \neq \lim_{\mathrm{tt}(h,k-1) \leftarrow t_1} \theta(t_1)))$$

Let $nn(h)$ denote the number of non-stutter points of h. Then the discretization bijection $\mathrm{di}(h)$ *for h is defined as follows:*

$$\mathrm{di}(h)(t) \triangleq$$
$$\begin{cases} \mathrm{tt}(h,k) + (t-k) * (\mathrm{tt}(h,k+1) - \mathrm{tt}(h,k)) & nn(h) < \infty \wedge 0 \leq k < nn(h) \\ & \wedge k \leq t \leq k+1 \\ \mathrm{tt}(h,k) + (t-k) & nn(h) < \infty \wedge k = nn(h) \wedge k \leq t \\ \mathrm{tt}(h,k) + (t-k) * (\mathrm{tt}(h,k+1) - \mathrm{tt}(h,k)) & nn(h) = \infty \wedge 0 \leq k \wedge k \leq t \leq k+1 \end{cases}$$

The inverse discretization of h is denoted $\mathrm{di}^{-1}(h)$*.*
Given histories $h_0, h_1 \in \mathcal{H}$, h_0 is **history stutter equivalent** *to h_1 denoted $h_0 \simeq_h h_1$ iff*

$$\begin{array}{ll} nn(h_0) = nn(h_1), & \textit{and} \\ \theta_{\natural_{\mathfrak{h}}(h_0)} = \theta_{\natural_{\mathfrak{h}}(h_1)}, & \textit{and} \\ \psi_{\natural_{\mathfrak{h}}(h_0)}(k) = \psi_{\natural_{\mathfrak{h}}(h_1)}(k), & k \leq nn(h_0) \end{array}$$

i.e., the number of non-stutter steps should be equal, the state information should be equal in both collapsed histories and the event information should be equal in the points of non-stuttering. A restricted version of the history stutter equivalence relation is the one that considers only the process state information, i.e., h_0 is **history process state stutter equivalent** *to h_1 denoted $h_0 \simeq_{\theta_h} h_1$ iff*

$$\begin{array}{ll} nn(h_0) = nn(h_1), & \textit{and} \\ \theta_{\natural_{\mathfrak{h}}(h_0)} = \theta_{\natural_{\mathfrak{h}}(h_1)}, & \end{array}$$

Application of above definition to the history of Figure 2.1 results in: $\mathrm{tt}(h,0) = 0$, $\mathrm{tt}(h,1) = t_1$, $\mathrm{tt}(h,2) = t_2$, $\mathrm{tt}(h,3) = t_3$, and $\mathrm{tt}(h,k) = \infty$ for $k > 3$ and $nn(h) = 3$. The discretization function $\mathrm{di}(h)t$ is as follows:

$$\begin{cases} t * t_1 & 0 \leq t \leq 1 \\ t_1 + (t-1) * (t_2 - t_1) & 1 \leq t \leq 2 \\ t_2 + (t-2) * (t_3 - t_2) & 2 \leq t \leq 3 \\ t_3 + (t-3) & 3 \leq t \end{cases}$$

The collapsed history $\natural_{\mathfrak{h}}(h_0)$ is illustrated in Figure 2.3.

The following theorem relates histories to a special kind of infinite sequences of pairs of event and process states, in which sequences start with an λ action, followed by possibly stuttering actions, then followed by exactly one non-stuttering action etc. Furthermore should every non-λ event be surrounded by λ-events. These kind of sequences are inspired by those defined in [KMP93]. For these kind of sequences a *sequence collapse* is defined that removes all finite stuttering; with the help of this collapse operator the sequence stutter equivalence operator is defined.

Definition 11 (Infinite sequences)
Define a sequence element as a pair (δ, σ) of an event and a process state. Let sel_i $(i \geq 0)$ be

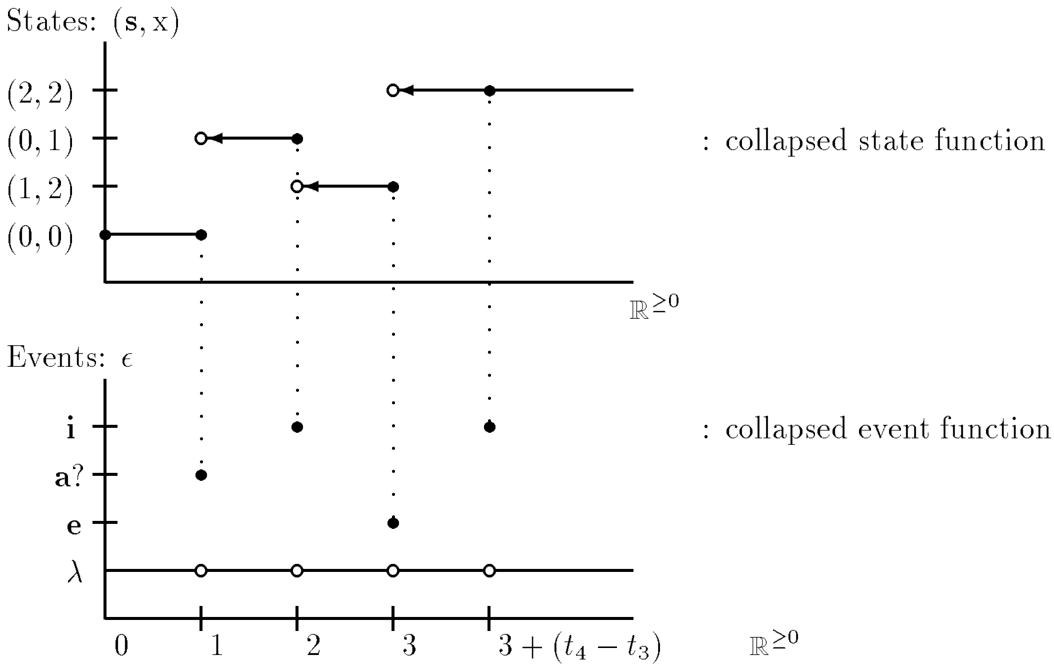

Figure 2.3: This picture illustrates the collapsed history of Figure 2.1

the pair (δ_i, σ_i) *then the sequence seq is a infinite sequence of the form* $seq_0 sel_0 seq_1 sel_1 \ldots$ *where* $sel_i = (\delta_i, \sigma_i)$ *is such that*

$$\delta_i(\epsilon) \neq \lambda,$$
$$(\delta_i(\epsilon) = \mathbf{a}? \vee \delta_i(\epsilon) = \mathbf{a}!) \rightarrow \sigma_i|^1_{\mathfrak{V}} = \sigma_{i+1}|^1_{\mathfrak{V}}$$
$$\delta_i(\epsilon) \in \{\mathbf{i}, \mathbf{e}\} \rightarrow \sigma_i \neq \sigma_{i+1}$$

and seq_i *is a sequence of the form* $(\delta_{i1}, \sigma_i)^{n_i}((\delta_{i2}, \sigma_i)(\delta_{i1}, \sigma_i)^{k_i})^{l_i}$ *where* $n_i > 0$*,* $k_i > 0$ *and* $l_i \geq 0$*, and* $\delta_{i1}(\epsilon) = \lambda$ *and* $\delta_{i2}(\epsilon) \in \{\mathbf{i}, \mathbf{e}\}$*.*
Let SEQ denote the set of all such sequences. Let seq be a sequence of the above form then $\natural_{\mathfrak{s}}(seq) = (sel'_i)_{i \geq 0}$ *is the stutter free sequence obtained from seq by deleting all finite stuttering from seq. Formally: Let* $ns(seq)$ *denote the number of non-stutter steps in seq, if* $ns(seq) = \infty$*:*

$$\begin{array}{ll} sel'_{2*i+1} = sel_i & 0 \leq i \\ sel'_{2*i} = (\delta_{i1}, \sigma_i) & 0 \leq i \end{array}$$

if $ns(seq) < \infty$*:*

$$\begin{array}{ll} sel'_{2*i+1} = sel_i & 0 \leq i < ns(seq) \\ sel'_{2*i+1} = (\delta_{k1}, \sigma_k) & k = ns(seq) \wedge k \leq i \\ sel'_{2*i} = (\delta_{i1}, \sigma_i) & 0 \leq i \leq ns(seq) \\ sel'_{2*i} = (\delta_{k1}, \sigma_k) & k = ns(seq) \wedge k \leq i \end{array}$$

Let seq_0 *and* seq_1 *be sequences then* seq_0 *is stutter equivalent to* seq_1 *denoted* $seq_0 \simeq_s seq_1$ *iff: let* $\natural_{\mathfrak{s}}(seq_0) = (sel^0_i)_{i \geq 0}$ *and* $\natural_{\mathfrak{s}}(seq_1) = (sel^1_i)_{i \geq 0}$*,*

$$\begin{array}{ll} ns(seq_0) = ns(seq_1) & \textit{and} \\ \sigma^0_i = \sigma^1_i & \textit{and} \\ \delta^0_i(\epsilon) = \delta^1_i(\epsilon) & \end{array}$$

The relationship between the sequences and histories is that there exists a function from the stutter equivalence classes of histories to the stutter equivalence classes of sequences and a function from the stutter equivalence classes of sequences to the stutter equivalence classes of histories.

Theorem 1 (Relationship between histories and infinite sequences)
Let $h \in \mathcal{H}/\simeq_h$ *then* $(sel_i)_{i\geq 0} \in SEQ/\simeq_s$ *where* sel_i *is as follows:*
if $nn(h) < \infty$*:*

$$\begin{array}{ll} sel_{2*i+1} = h(i) & 0 \leq i < nn(h) \\ sel_{2*i} = \lim\limits_{i \leftarrow t_1} h(t_1) & 0 \leq i \leq nn(h) \\ sel_{2*i+1} = \lim\limits_{k \leftarrow t_1} h(t_1) & k = nn(h) \wedge k \leq i \\ sel_{2*i} = \lim\limits_{k \leftarrow t_1} h(t_1) & k = nn(h) \wedge k \leq i \end{array}$$

if $nn(h) = \infty$*:*

$$\begin{array}{ll} sel_{2*i+1} = h(i) & 0 \leq i \\ sel_{2*i} = \lim\limits_{i \leftarrow t_1} h(t_1) & 0 \leq i \end{array}$$

Let $seq = (sel_i)_{i\geq 0} \in SEQ/\simeq_s$ *then* $h \in \mathcal{H}/\simeq_h$ *where* h *is as follows:*
if $ns(seq) < \infty$*:*

$$\begin{array}{ll} h(0) = sel_0 & \\ h(t) = sel_{2*t-1} & t \in \mathbb{N} \wedge 0 < t \leq ns(seq) \\ h(t) = sel_{2*t} & t \in \mathbb{N} \wedge t > ns(seq) \\ h(t) = sel_{2*i} & i < t < i+1 \end{array}$$

if $ns(seq) = \infty$*:*

$$\begin{array}{ll} h(0) = sel_0 & \\ h(t) = sel_{2*t-1} & t \in \mathbb{N} \\ h(t) = sel_{2*i} & i < t < i+1 \end{array}$$

The following sequence corresponds to the history of figure 2.3:

$$\begin{array}{llll} seq = (\delta_i, \sigma_i)_{i\geq 0}, & & & \\ \delta_0(\epsilon) = \lambda & \sigma_0(\mathbf{s}) = 0 & \sigma_0(\mathrm{x}) = 0 & \\ \delta_1(\epsilon) = \mathbf{a}? & \sigma_1(\mathbf{s}) = 0 & \sigma_1(\mathrm{x}) = 0 & \\ \delta_2(\epsilon) = \lambda & \sigma_2(\mathbf{s}) = 0 & \sigma_2(\mathrm{x}) = 1 & \\ \delta_3(\epsilon) = \mathbf{i} & \sigma_3(\mathbf{s}) = 0 & \sigma_3(\mathrm{x}) = 1 & \\ \delta_4(\epsilon) = \lambda & \sigma_4(\mathbf{s}) = 1 & \sigma_4(\mathrm{x}) = 2 & \\ \delta_5(\epsilon) = \mathbf{e} & \sigma_5(\mathbf{s}) = 1 & \sigma_5(\mathrm{x}) = 2 & \\ \delta_i(\epsilon) = \lambda & \sigma_i(\mathbf{s}) = 2 & \sigma_i(\mathrm{x}) = 2 & i > 5 \end{array}$$

The basis is a pair consisting of a *process basis*, specifying the local and shared variables of the system, and a *action basis* which specifies the input and output communication channels of a system. The following definition introduces basis and history sets that constrain a specific process basis, i.e., specific sets of shared variables and local variables are constrained to change in specific ways, the variables outside this process basis can change without restriction, with exception of the rigid variables which do not change at all.

Definition 12 (Basis, history set constraining a basis)
A **basis** *(denoted by B) is a pair (B^A, B^P), where B^A (called* **action basis***) is a pair* $(\mathrm{In}, \mathrm{Out})$ *where* In *is a set of input communication channels and* Out *is a set of output communication channels, and where B^P (called* **process basis***) is a tuple* (V, X) *where* V *a finite set of shared variables and* X *a finite set of local variables.*
Given a history $h \in \mathcal{H}$ and process basis B^P then the **process basis restriction** *of h denoted $h|^2_{B^P}$ is defined as $\langle \psi, \theta|^2_{\mathrm{V}\cup\mathrm{X}} \rangle$.*
Given a set of histories H and process basis B^P then H **is constrained by** *B^P iff $\forall h_1, h_2 \in \mathcal{H} : h_1|^2_{B^P} = h_2|^2_{B^P} \rightarrow (h_1 \in H \leftrightarrow h_2 \in H)$.*

The following definition introduces the notion of *history specification* which is a pair consisting of a basis and a set of histories constraining the process basis.

Definition 13 (History specification of a system)
A **history specification** *of a system (denoted $\mathcal{S}$) is a pair (B, H) where B is a basis and H is a set of histories constraining process basis B^P such that an environment action* **e** *doesn't change the local variables of the system:*

$$\forall t : \psi(t)(\epsilon) = \mathbf{e} \rightarrow \theta(t)|^1_{\mathrm{X}} = \lim_{t \leftarrow t_1} \theta(t_1)|^1_{\mathrm{X}}$$

The following definition introduces several notions from topology ([Wri87]) needed for the definition of safety and liveness sets of histories. These definitions of safety and liveness are based on those of [AS85]. Informally a safety set of histories consists of histories where nothing "bad" happens and a liveness set of histories consists of histories where something "good" eventually happens.

Definition 14 (Safety and liveness set)
Let H be a set of histories and $h \in \mathcal{H}$.

- *The prefix of h of length t denoted $h\downharpoonright_t$ is defined as*

$$h\downharpoonright_t (t_0) \triangleq \begin{cases} \langle \psi(t_0), \theta(t_0) \rangle & 0 \leq t_0 \leq t \\ \langle \psi(0), \theta(t) \rangle & t_0 > t \end{cases}$$

  Thus for $t_0 > t$ only stutter actions occur in $h\downharpoonright_t$.

- *The* **distance function** *d from $\mathcal{H} \times \mathcal{H} \rightarrow \mathbb{R}^{\geq 0}$ is defined as:*

$$d(h_1, h_2) \triangleq \begin{cases} 0 & \text{if } h_1 = h_2 \\ 1 & \text{if } h_1(0) \neq h_2(0) \\ 2^{-\sup\{t \in \mathbb{R}^{\geq 0} | h_1\downharpoonright_t = h_2\downharpoonright_t\}} & \text{otherwise} \end{cases}$$

  $(\mathcal{H}, d)$ is a metric space.

- *H is called d-***open** *iff*

$$\forall h \in H : \exists \varepsilon > 0 : \forall h_1 : d(h, h_1) < \varepsilon \rightarrow h_1 \in H$$

- *The topology with* $\{H \subseteq \mathcal{H} \mid H$ *is d-open* $\}$ *as its basis is called the* d **induced topology** *of* $(\mathcal{H}, d)$ *denoted* τ_d.

- H *is called a* τ_d-**environment** *of* h *iff*

  $$\exists H_1 \in \tau_d : h \in H_1 \wedge H_1 \subseteq H$$

- *The* **interior** *of* H *denoted* $in(H)$ *is defined as*

  $$\{h \in \mathcal{H} \mid H \text{ is a } \tau_d \text{ environment of } h\}$$

- *The* **closure** *of* H *denoted* $cl(H)$ *is defined as* $\mathcal{H} \setminus (in(\mathcal{H} \setminus H))$.

- H *is a* **safety set** *iff* $cl(H) = H$.

- H *is a* **liveness set** *iff* $cl(H) = \mathcal{H}$.

Note: the only set that is both a safety and a liveness set is $\mathcal{H}$ [AS85].

A specification method for systems that uses only sets of histories is not attractive. Therefore the notion of machine is introduced. A machine consists of a set of states and a state-transition relation. The intention is that the set of computations (i.e. histories) of a machine associated to a system should correspond to the history specification of this system. A machine however can only generate safety sets of histories [AS87]. Therefore, a liveness set is specified as a condition on the set of computations (histories) of a machine. Next the formal definition of a machine is given.

Definition 15 (Machine)
The machine specification M *of a system is a triple* (B, I, T) *where:*

- B*: the* basis *of* M*; a tuple* $((\mathrm{In}, \mathrm{Out}), (\mathrm{V}, \mathrm{X}))$. *Note: the shared variables will be printed in bold faced style in order to distinguish them from the local variables.*

- I *: a non-empty subset of* Σ*, the set of initial states, such that*

  - $\forall \sigma_0, \sigma_1 \in \Sigma : (\sigma_0|^1_{\mathrm{V}\cup\mathrm{X}} = \sigma_1|^1_{\mathrm{V}\cup\mathrm{X}}) \to (\sigma_0 \in I \leftrightarrow \sigma_1 \in I)$, *i.e., it constrains the variables from* $\mathrm{V} \cup \mathrm{X}$ *only.*

- T *: the state-transition relation (finite),* $T \subseteq \Delta \times \Sigma^2$*, such that*

  - $\forall \sigma_0, \sigma_1 \in \Sigma, \delta \in \Delta : \langle \delta, \sigma_0, \sigma_1 \rangle \in T \to \sigma_0|^1_{\mathfrak{R}} = \sigma_1|^1_{\mathfrak{R}}$, *i.e., the rigid variables don't change at all.*
  - $\forall \sigma_0, \sigma_1, \sigma_2, \sigma_3 \in \Sigma, \delta \in \Delta : (\sigma_0|^1_{\mathrm{V}\cup\mathrm{X}} = \sigma_2|^1_{\mathrm{V}\cup\mathrm{X}} \wedge \sigma_1|^1_{\mathrm{V}\cup\mathrm{X}} = \sigma_3|^1_{\mathrm{V}\cup\mathrm{X}}) \to (\langle \delta, \sigma_0, \sigma_1 \rangle \in T \leftrightarrow \langle \delta, \sigma_2, \sigma_3 \rangle \in T)$, *i.e.* T *constrains* B^P *only.*
  - $\forall \sigma_0, \sigma_1 \in \Sigma, \delta \in \Delta : (\langle \delta, \sigma_0, \sigma_1 \rangle \in T \wedge (\delta(\epsilon) = \mathbf{a}? \vee \delta(\epsilon) = \mathbf{a}!)) \to \sigma_0|^1_{\mathrm{V}} = \sigma_1|^1_{\mathrm{V}}$, *i.e., a communication action doesn't change the values of shared variables, and*
  - $\forall \sigma_0, \sigma_1 \in \Sigma, \delta \in \Delta : (\langle \delta, \sigma_0, \sigma_1 \rangle \in T \wedge \delta(\epsilon) = \mathbf{e}) \to \sigma_0|^1_{\mathrm{X}} = \sigma_0|^1_{\mathrm{X}}$, *i.e., an environment action doesn't change the values of local variables of the system.*

- $\forall \sigma_0, \sigma_1 \in \Sigma, \delta \in \Delta : \langle \delta, \sigma_0, \sigma_1 \rangle \in T \rightarrow (\delta(\epsilon) \notin \{\lambda, \mathbf{i}, \mathbf{e}\} \vee \sigma_0 \neq \sigma_1)$, *i.e., no stutter transitions are specified.*

The following example is an illustration of the notion of machine.

Example 1
$M = (B, I, T)$ *where:*

1. **Basis:** $B = ((\mathrm{In}, \mathrm{Out}), (\mathrm{V}, \mathrm{X}))$ *where*

$$\begin{array}{lcl} \mathrm{In} & \triangleq & \{\mathbf{a}\} \\ \mathrm{Out} & \triangleq & \emptyset \\ \mathrm{V} & \triangleq & \{\mathbf{v}\} \\ \mathrm{X} & \triangleq & \{\mathrm{u}\} \end{array}$$

2. **Initial States:**

$$I : \{\sigma \in \Sigma \mid \sigma(\mathrm{u}) = 0 \textit{ and } \sigma(\mathbf{v}) = 0\}$$

3. **Transitions:**
T:
$\{\langle \delta, \sigma_0, \sigma_1 \rangle \in \Delta \times \Sigma^2 \mid$

   (a) $(\delta(\epsilon) = \mathbf{a}? \textit{ and } \sigma_0(\mathrm{u}) = 0 \textit{ and } \sigma_1(\mathrm{u}) = 1 \textit{ and } \sigma_1(\mathbf{v}) = \sigma_0(\mathbf{v}))$ *or*

   (b) $(\delta(\epsilon) = \mathbf{i} \textit{ and } \sigma_0(\mathrm{u}) = 1 \textit{ and } \sigma_0(\mathbf{v}) = 1 \textit{ and } \sigma_1(\mathrm{u}) = 2 \textit{ and } \sigma_1(\mathbf{v}) = 0)$ *or*

   (c) $(\delta(\epsilon) = \mathbf{e} \textit{ and } \sigma_1(\mathrm{u}) = \sigma_0(\mathrm{u}) \textit{ and } \sigma_1(\mathbf{v}) = \sigma_0(\mathbf{v}) + 1)\}$

The concepts of event and state functions are related by the notion of *computation* of a machine M. A computation of M intuitively expresses that an event function and a state function fit together in that at any point t any triple consisting of (1) the event occurring at t, (2) the state just before and including t, and (3) the state just after t, belongs to the state transition relation of M (see fig. 2.1). Because a state-transition relations don't contain stutter steps but histories do, a set of stutter transitions should be defined in order to relate machine computations to histories.

Definition 16 (Computation)
Let $h = \langle \psi, \theta \rangle \in \mathcal{H}$ *and* $t \in \mathbb{R}^{\geq 0}$*, then define the* **step** *occurring at* t *in* h *by:*
$Step_h(t) = \langle \psi(t), \theta(t), \lim_{t \leftarrow t_1} \theta(t_1) \rangle$.
Define the set of **stutter** *steps denoted* STU *as* $\{\langle \delta, \sigma_0, \sigma_1 \rangle \mid \delta(\epsilon) \in \{\lambda, \mathbf{i}, \mathbf{e}\} \wedge \sigma_0 = \sigma_1\}$.
A **computation of a machine** $M = (B, I, T)$ *is a history* $h = \langle \psi, \theta \rangle \in \mathcal{H}$ *such that:*

$\theta(0) \in I$ *and*
$\forall t : Step_h(t) \in T \vee Step_h(t) \in \mathrm{STU}$.

Let the set of all computations of M *be defined as:*
$Comp(M) \triangleq \{h \in \mathcal{H} \mid h \textit{ is a computation of } M\}$.

Lemma 1 (Machine is safety)
Given machine $M = (B, I, T)$ then

$Comp(M)$ is a safety set.

A proof of this lemma is given in [AL91] (it is also repeated in the appendix). The *machine specification* of a system now consists of a machine M and a set of histories L constraining the basis of this machine such that the closure of the intersection of $Comp(M)$ and L equals $Comp(M)$. This is the *machine closedness* property of a system specification introduced in [AFK88, AL91]. Let $A \rightarrow B$ denote $\bar{A} \bigcup B$. By a result of [AS85] every set of histories can be written as the intersection of a safety set and a liveness set namely $cl(Comp(M) \cap L) \bigcap cl(Comp(M) \cap L) \rightarrow (Comp(M) \cap L)$. By the machine closedness property this can be written as $Comp(M) \bigcap Comp(M) \rightarrow L$. This means that $Comp(M)$ specifies the safety properties and $Comp(M) \rightarrow L$ the liveness properties of the system.

Definition 17 (Machine specification of a system)
A **machine specification** *$\mathcal{S}$ of a system is a pair $(B, Comp(M) \cap L)$ where M is a machine with basis B and L a set of histories constraining only B^P such that $cl(Comp(M) \cap L) = Comp(M)$. The set of computations of $\mathcal{S}$, denoted $Comp(\mathcal{S})$, is defined as $Comp(M) \cap L$.*

2.2.2 DTL Specification of Reactive Systems

As mentioned above, the local properties are described by a machine and the liveness properties are described as a set of histories. The dense time temporal logic DTL is introduced to describe both kind of properties. The one used here is a mixture of dense time temporal logics defined in [Sta84, Sta85, BKP86, DK90, KMP93].

Definition 18 (Syntax of DTL)
The syntax of DTL is defined in Table 2.1 where value $\mu \in Val$, rigid variable $n \in \mathfrak{R}$, observable variable $\mathbf{v} \in \mathfrak{V}$, local variable $\mathrm{x} \in \mathfrak{X}$, event variable $\epsilon \in \mathfrak{E}$ and channel $\mathbf{a} \in \mathrm{Chan}$.

Table 2.1: Syntax of DTL

	Rigid Expressions
$rexp ::=$	$\mu \mid n \mid n' \mid \grave{n} \mid rexp_1 + rexp_2 \mid \ldots$
	Expressions
$exp ::=$	$rexp \mid \mathbf{v} \mid \mathbf{v}' \mid \grave{\mathbf{v}} \mid \mathrm{x} \mid \mathrm{x}' \mid \grave{\mathrm{x}} \mid exp_1 + exp_2 \mid \ldots$
	Event Expressions
$evexp ::=$	$\mathbf{a}? \mid \mathbf{a}! \mid \mathbf{i} \mid \mathbf{e} \mid \lambda \mid \epsilon \mid \epsilon' \mid \grave{\epsilon}$
	Temporal formulae
$p ::=$	$\mathbf{true} \mid exp_1 = exp_2 \mid exp_1 < exp_2 \mid evexp_1 = evexp_2 \mid \neg p \mid p_1 \vee p_2$
	$p_1 \hat{\mathcal{U}}\ p_2 \mid p_1 \hat{\mathcal{S}}\ p_2 \mid \exists \mathrm{x}.p \mid \exists \epsilon.p \mid \exists n.p$

The informal semantics of the most interesting constructs are as follows:

- $\grave{\mathrm{x}}$ denotes the *previous value* of x,

- x denotes the *current value* of x,
- x$'$ denotes the *next value* of x,
- ϵ denotes the *current action* value of ϵ,
- $\grave{\epsilon}$ denotes the *previous action* valueof ϵ,
- ϵ' denotes the *next action* value of ϵ,
- $p_1 \ \widehat{\mathcal{U}}\ p_2$ denotes strict (present not included in the future) until operator from temporal logic,
- $p_1 \ \widehat{\mathcal{S}}\ p_2$ denotes strict (present not included in the past) since operator from temporal logic,
- $\exists \mathrm{x}.p$ denotes *existential quantification over local variable* x of p, i.e., hiding,
- $\exists \epsilon.p$ denotes *existential quantification over event variable* ϵ of p, i.e., hiding.

A *state expression* is an expression without any primed variables. A *state formula* is a formula build from state expressions without $\widehat{\mathcal{U}}$ and $\widehat{\mathcal{S}}$ operators.

Table 2.2 lists some frequently used abbreviations: The following example 2 gives some DTL formulae

Example 2 (Some DTL formulae)
$\Big(\epsilon = \mathbf{a}_0 \wedge \mathrm{x} = 0 \wedge \mathrm{x}' = 1\Big)$ *(a state-transition),*
$\Box \mathrm{x} > 0$ *(a safety property),*
and $\Box(\mathrm{x} = 0 \rightarrow \Diamond \mathrm{x} > 0)$ *(a liveness property).*

Before we give the semantics of DTL formulae we define for a variable x (local process or event) the x-variant of a history.

Definition 19 (x-variant, ϵ-variant and n-variant of a history)
Let $h, h_1 \in \mathcal{H}$.
Let $\mathrm{x} \in \mathfrak{X}$ then h_1 is a x*-variant of h if $\psi_1 = \psi$ and $\theta_1|^2_{(\mathfrak{V}\cup\mathfrak{X}\cup\mathfrak{N})\backslash\{\mathrm{x}\}} = \theta|^2_{(\mathfrak{V}\cup\mathfrak{X}\cup\mathfrak{N})\backslash\{\mathrm{x}\}}$.*
Let $\mathrm{X} \subseteq \mathfrak{X}$ then h_1 is a X*-variant of h if $\psi_1 = \psi$ and $\theta_1|^2_{(\mathfrak{V}\cup\mathfrak{X}\cup\mathfrak{N})\backslash\mathrm{X}} = \theta|^2_{(\mathfrak{V}\cup\mathfrak{X}\cup\mathfrak{N})\backslash\mathrm{X}}$.*
Let $\epsilon \in \mathfrak{E}$ then h_1 is a ϵ-variant of h if $\psi_1|^2_{\mathfrak{E}\backslash\{\epsilon\}} = \psi|^2_{\mathfrak{E}\backslash\{\epsilon\}}$ and $\theta_1 = \theta$.
Let $n \in \mathfrak{N}$ then h_1 is a n-variant of h if $\psi_1 = \psi$ and $\theta_1|^2_{(\mathfrak{V}\cup\mathfrak{X}\cup\mathfrak{N})\backslash\{n\}} = \theta|^2_{(\mathfrak{V}\cup\mathfrak{X}\cup\mathfrak{N})\backslash\{n\}}$.

In the following definition the semantics of DTL is given without using valuation functions for expressions, i.e., this valuation function is implicitly defined by $\models$. By convention, boolean values are not explicitly denoted, i.e., we shall write $(h, t) \models$ **true** rather than $(h, t) \models$ **true** $\triangleq tt$.

Definition 20 (Semantics of DTL)
Let $h \in \mathcal{H}$, $t \in \mathbb{R}^{\geq 0}$, $n \in \mathfrak{N}$, $\mathbf{v} \in \mathfrak{V}$, $\mathrm{x} \in \mathfrak{X}$, and $\epsilon \in \mathfrak{E}$.

- $(h, t) \models \mu \ \triangleq \ \mu,$

Table 2.2: Used abbreviations

false $\triangleq$ $\neg$**true**	
$p_1 \rightarrow p_2 \triangleq \neg p_1 \vee p_2$	p_1 implies p_2
$p_1 \wedge p_2 \triangleq \neg(\neg p_1 \vee \neg p_2)$	p_1 and p_2
$p_1 \leftrightarrow p_2 \triangleq (p_1 \rightarrow p_2) \wedge (p_1 \leftarrow p_2)$	p_1 equivalent p_2
$\forall \mathrm{x}.p \triangleq \neg\exists \mathrm{x}.\neg p$	for all x p
$\exists \mathrm{X}.p \triangleq \exists \mathrm{x}_0.\ldots.\exists \mathrm{x}_n.p$	hiding over $\mathrm{X} = \{\mathrm{x}_0, \ldots, \mathrm{x}_n\}$
$\widehat{\Diamond} p \triangleq$ **true** $\widehat{\mathcal{U}}\ p$	strict eventually p,
$\widehat{\Box} p \triangleq \neg\widehat{\Diamond}\neg p$	strict always p,
$\bigcirc p \triangleq p\ \widehat{\mathcal{U}}$ **true**	is for some time going to be uninterruptedly p,
$\Diamond p \triangleq p \vee \widehat{\Diamond} p$	non-strict eventually,
$\Box p \triangleq p \wedge \widehat{\Box} p$	non-strict always,
$p_1 \mathcal{U} p_2 \triangleq p_2 \vee (p_1 \wedge (p_1\ \widehat{\mathcal{U}}\ p_2))$	non-strict until,
$\widehat{\diamondminus} p \triangleq$ **true** $\widehat{\mathcal{S}}\ p$	strict once p,
$\widehat{\boxminus} p \triangleq \neg\widehat{\diamondminus}\neg p$	strict has-always-been p,
$\ominus p \triangleq p\ \widehat{\mathcal{S}}$ **true**	has for some time been uninterruptedly p,
$\widetilde{\ominus} p \triangleq \neg\ominus\neg p$	has arbitrarily recently been p,
first $\triangleq \widetilde{\ominus}$**false**	first position in a history,
$\diamondminus p \triangleq p \vee \widehat{\diamondminus} p$	non-strict once,
$\boxminus p \triangleq p \wedge \widehat{\boxminus} p$	non-strict has-always-been,
$p_1 \mathcal{S} p_2 \triangleq p_2 \vee (p_1 \wedge (p_1\ \widehat{\mathcal{S}}\ p_2))$	non-strict since,
$p_1 \Rightarrow p_2 \triangleq \Box(p_1 \rightarrow p_2)$	p_1 entails p_2
$p_1 \Leftrightarrow p_2 \triangleq \Box(p_1 \leftrightarrow p_2)$	p_1 is congruent p_2

- $(h,t) \models n \ \triangleq\ \theta(0)(n)$,
- $(h,t) \models n' \ \triangleq\ \theta(0)(n)$,
- $(h,t) \models \grave{n} \ \triangleq\ \theta(0)(n)$,
- $(h,t) \models \mathrm{x} \ \triangleq\ \theta(t)(\mathrm{x})$,
- $(h,t) \models \mathbf{v} \ \triangleq\ \theta(t)(\mathbf{v})$,
- $(h,0) \models \grave{\mathrm{x}} \ \triangleq\ \theta(0)(\mathrm{x})$
  $t > 0$: $(h,t) \models \grave{\mathrm{x}} \ \triangleq\ \lim\limits_{t_1 \rightarrow t} \theta(t_1)(\mathrm{x})$
- $(h,0) \models \grave{\mathbf{v}} \ \triangleq\ \theta(0)(\mathbf{v})$
  $t > 0$: $(h,t) \models \grave{\mathbf{v}} \ \triangleq\ \lim\limits_{t_1 \rightarrow t} \theta(t_1)(\mathbf{v})$
- $(h,t) \models \mathrm{x}' \triangleq \lim\limits_{t \leftarrow t_1} \theta(t_1)(\mathrm{x})$

- $(h,t) \models \mathbf{v}' \triangleq \lim_{t \leftarrow t_1} \theta(t_1)(\mathbf{v})$
- $(h,t) \models exp_1 + exp_2 \triangleq (h,t) \models exp_1 \ + \ (h,t) \models exp_2$,
- $(h,t) \models exp_1 - exp_2 \triangleq (h,t) \models exp_1 \ - \ (h,t) \models exp_2$,
- $(h,t) \models \mathbf{a}? \ \triangleq \ \mathbf{a}?$,
- $(h,t) \models \mathbf{a}! \ \triangleq \ \mathbf{a}!$,
- $(h,t) \models \mathbf{i} \ \triangleq \ \mathbf{i}$,
- $(h,t) \models \mathbf{e} \ \triangleq \ \mathbf{e}$,
- $(h,t) \models \lambda \ \triangleq \ \lambda$,
- $(h,t) \models \epsilon \ \triangleq \ \psi_h(t)(\epsilon)$,
- $(h,0) \models \grave{}\epsilon \ \triangleq \ \psi(0)(\epsilon)$
  $t > 0$: $(h,t) \models \grave{}\epsilon \ \triangleq \ \lim_{t_1 \to t} \psi(t_1)(\epsilon)$,
- $(h,t) \models \epsilon' \triangleq \lim_{t \leftarrow t_1} \psi(t_1)(\epsilon)$,
- $(h,t) \models \mathbf{true}$,
- $(h,t) \models exp_1 = exp_2$ *iff* $(h,t) \models exp_1 \ = \ (h,t) \models exp_2$,
- $(h,t) \models evexp_1 = evexp_2$ *iff* $(h,t) \models evexp_1 \ = \ (h,t) \models evexp_2$,
- $(h,t) \models exp_1 < exp_2$ *iff* $(h,t) \models exp_1 \ < \ (h,t) \models exp_2$,
- $(h,t) \models \neg p$ *iff* $(h,t) \not\models p$,
- $(h,t) \models p_1 \vee p_2$ *iff* $(h,t) \models p_1$ *or* $(h,t) \models p_2$,
- $(h,t) \models p_1 \ \widehat{\mathcal{U}} \ p_2$ *iff there exists a* $t_0 > t$, $(h,t_0) \models p_2$ *and for all* $t_1 \in (t,t_0)$, $(h,t_1) \models p_1$,
- $(h,t) \models p_1 \ \widehat{\mathcal{S}} \ p_2$ *iff there exists a* $t_0 < t$, $(h,t_0) \models p_2$ *and for all* $t_1 \in (t_0,t)$, $(h,t_1) \models p_1$.
- $(h,t) \models \exists \mathrm{x}.p$ *iff* $(h_1,t) \models p$, *for some* h_1, *a* x*-variant of* h.
- $(h,t) \models \exists \epsilon.p$ *iff* $(h_1,t) \models p$, *for some* h_1, *a* ϵ*-variant of* h.
- $(h,t) \models \exists n.p$ *iff* $(h_1,t) \models p$, *for some* h_1, *a* n*-variant of* h.

Definition 21 (Satisfiability, validity)
For a DTL formula p and a history $h \in \mathcal{H}$, h **satisfies** *p denoted $h \models p$ iff $(h, 0) \models p$.*
A DTL formula p is **satisfiable** *iff $h \models p$ for some history $h \in \mathcal{H}$.*
A DTL formula p is **valid**, *denoted $\models p$, iff $h \models p$ for all histories $h \in \mathcal{H}$.*
*Given a system $\mathcal{S}$ with basis B and set of computations $Comp(\mathcal{S})$ then a DTL formula is $\mathcal{S}$-***valid**, *denoted $\mathcal{S} \models p$ iff $h \models p$ for all histories $h \in Comp(\mathcal{S})$.*
Given a temporal formula p then the set of histories satisfying p denoted $Hist(p)$ is defined as $\{h \mid h \models p\}$.

The following theorem states that the logic DTL is history process state stutter insensitive. Later on a restricted version of DTL is considered in order to make it history stutter insensitive.

Theorem 2 (DTL is history process state stutter insensitive)
Let $rexp$ be a rigid expression, exp be an expression, $evexp$ an event expression and p a temporal formula then

$$
\begin{array}{ll}
a & \forall t, h_0, h_1 : h_0 \simeq_{\theta_h} h_1 \rightarrow ((h_0, t) \models rexp = (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models rexp) \\
b & \forall t, h_0, h_1 : h_0 \simeq_{\theta_h} h_1 \rightarrow ((h_0, t) \models exp = (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models exp) \\
c & \forall t, h_0, h_1 : h_0 \simeq_{\theta_h} h_1 \rightarrow ((h_0, t) \models evexp = (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models evexp) \\
d & \forall t, h_0, h_1 : h_0 \simeq_{\theta_h} h_1 \rightarrow ((h_0, t) \models p \textit{ iff } (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models p)
\end{array}
$$

The following definitions introduce substitution.

Definition 22 (Non-rigid process variable substitution in expressions)
Define substitution of $w \in \mathfrak{V} \cup \mathfrak{X}$ by state expression exp in expression exp_0 denoted $exp_0\,[exp/w]$ as follows, using $\equiv$ for syntactic equality:

- $rexp\,[exp/w] \equiv rexp$

- $\mathbf{v}\,[exp/w] \equiv \begin{cases} exp & \textit{if } \mathbf{v} \equiv w \\ \mathbf{v} & \textit{if } \mathbf{v} \not\equiv w \end{cases}$

- $\mathbf{v}'\,[exp/w] \equiv \begin{cases} \mathrm{exp}' & \textit{if } \mathbf{v} \equiv w \\ \mathbf{v}' & \textit{if } \mathbf{v} \not\equiv w \end{cases}$

  where exp' *denotes the operation of "priming after" all occurrences of variables in exp (note: exp is a state expression so all variables in exp are unprimed).*

- $\grave{}\mathbf{v}\,[exp/w] \equiv \begin{cases} \grave{}\mathrm{exp} & \textit{if } \mathbf{v} \equiv w \\ \grave{}\mathbf{v} & \textit{if } \mathbf{v} \not\equiv w \end{cases}$

  where $\grave{}\mathrm{exp}$ *denotes the operation of "priming before" all occurrences of variables in exp.*

- $\mathrm{x}\,[exp/w] \equiv \begin{cases} exp & \textit{if } \mathrm{x} \equiv w \\ \mathrm{x} & \textit{if } \mathrm{x} \not\equiv w \end{cases}$

- $\mathrm{x}'\,[exp/w] \equiv \begin{cases} \mathrm{exp}' & \textit{if } \mathrm{x} \equiv w \\ \mathrm{x}' & \textit{if } \mathrm{x} \not\equiv w \end{cases}$

- $\grave{\mathrm{x}}\,[exp/w] \equiv \begin{cases} \grave{\mathrm{exp}} & \textit{if}\ \mathrm{x} \equiv w \\ \grave{\mathrm{x}} & \textit{if}\ \mathrm{x} \not\equiv w \end{cases}$

- $(exp_1 + exp_2)\,[exp/w] \equiv exp_1\,[exp/w] + exp_2\,[exp/w]$

- $\ldots$

Definition 23 (Rigid variable substitution in expressions)
Define substitution of $n \in \mathfrak{R}$ *by state rigid expression* $rexp$ *in expression* exp_0 *denoted* $exp_0\,[rexp/n]$ *as follows, using* $\equiv$ *for syntactic equality:*

- $\mu\,[rexp/n] \equiv \mu,$

- $n_0\,[rexp/n] \equiv \begin{cases} rexp & \textit{if}\ n \equiv n_0 \\ n_0 & \textit{if}\ n \not\equiv n_0 \end{cases}$

- $n_0'\,[rexp/n] \equiv \begin{cases} rexp' & \textit{if}\ n \equiv n_0 \\ n_0' & \textit{if}\ n \not\equiv n_0 \end{cases}.$

- $\grave{n}_0\,[rexp/n] \equiv \begin{cases} \grave{rexp} & \textit{if}\ n \equiv n_0 \\ \grave{n}_0 & \textit{if}\ n \not\equiv n_0 \end{cases}.$

- $w\,[rexp/n] \equiv w,\ w \in \mathfrak{V} \cup \mathfrak{X},$

- $w'\,[rexp/n] \equiv w',\ w \in \mathfrak{V} \cup \mathfrak{X}$

- $\grave{w}\,[rexp/n] \equiv \grave{w},\ w \in \mathfrak{V} \cup \mathfrak{X}$

- $(exp_1 + exp_2)\,[rexp/n] \equiv exp_1\,[rexp/n] + exp_2\,[rexp/n],$

- $\ldots$

Definition 24 (Event variable substitution in event expressions)
Define substitution of $\epsilon \in \mathfrak{E}$ *by state event expression* $evexp$ *in* $evexp_0$ *denoted* $evexp_0\,[evexp/\epsilon]$ *as follows, using* $\equiv$ *for syntactic equality:*

- $\lambda\,[evexp/\epsilon] \equiv \lambda,$

- $\mathbf{a}?\,[evexp/\epsilon] \equiv \mathbf{a}?,$

- $\mathbf{a}!\,[evexp/\epsilon] \equiv \mathbf{a}!,$

- $\mathbf{i}\,[evexp/\epsilon] \equiv \mathbf{i},$

- $\mathbf{e}\,[evexp/\epsilon] \equiv \mathbf{e},$

- $\epsilon_0\,[evexp/\epsilon] \equiv \begin{cases} evexp & \textit{if}\ \epsilon_0 \equiv \epsilon \\ \epsilon_0 & \textit{if}\ \epsilon_0 \not\equiv \epsilon \end{cases}$

- $\epsilon_0'\,[evexp/\epsilon] \equiv \begin{cases} evexp' & \textit{if}\ \epsilon_0 \equiv \epsilon \\ \epsilon_0' & \textit{if}\ \epsilon_0 \not\equiv \epsilon \end{cases}$

- $`\epsilon_0\,[evexp/\epsilon] \equiv \begin{cases} `evexp & \textit{if } \epsilon_0 \equiv \epsilon \\ `\epsilon_0 & \textit{if } \epsilon_0 \not\equiv \epsilon \end{cases}$

Definition 25 (Process and event variable substitution in temporal formulae) *Define substitution for a non-rigid process variable $w \in \mathfrak{V} \cup \mathfrak{X}$ by state expression exp in a temporal formula p, denoted $p\,[exp/w]$, as follows:*

- $\mathbf{true}\,[exp/w] \equiv \mathbf{true}$
- $(exp_1 = exp_2)\,[exp/w] \equiv exp_1\,[exp/w] = exp_2\,[exp/w]$
- $(evexp_1 = evexp_2)\,[exp/w] \equiv (evexp_1 = evexp_2)$
- $(exp_1 < exp_2)\,[exp/w] \equiv exp_1\,[exp/w] < exp_2\,[exp/w]$
- $(\neg p)\,[exp/w] \equiv \neg(p\,[exp/w])$
- $(p_1 \vee p_2)\,[exp/w] \equiv p_1\,[exp/w] \vee p_2\,[exp/w]$
- $(p_1\ \widehat{\mathcal{U}}\ p_2)\,[exp/w] \equiv (p_1\,[exp/w])\ \widehat{\mathcal{U}}\ (p_2\,[exp/w])$
- $(p_1\ \widehat{\mathcal{S}}\ p_2)\,[exp/w] \equiv (p_1\,[exp/w])\ \widehat{\mathcal{S}}\ (p_2\,[exp/w])$
- $(\exists \mathrm{x}.p)\,[exp/w] \equiv \exists \mathrm{x}.(p\,[exp/w])$ *if* $\mathrm{x} \notin var(exp) \cup \{w\})$.
- $(\exists \epsilon.p)\,[exp/w] \equiv \exists \epsilon.(p\,[exp/w])$,
- $(\exists n.p)\,[exp/w] \equiv \exists n.(p\,[exp/w])$

Define substitution of rigid process variable $n \in \mathfrak{R}$ by state rigid expression $rexp$ in temporal formula p denoted $p\,[rexp/n]$ as follows:

- $\mathbf{true}\,[rexp/n] \equiv \mathbf{true}$
- $(exp_1 = exp_2)\,[rexp/n] \equiv exp_1\,[rexp/n] = exp_2\,[rexp/n]$
- $(evexp_1 = evexp_2)\,[rexp/n] \equiv (evexp_1 = evexp_2)$
- $(exp_1 < exp_2)\,[rexp/n] \equiv exp_1\,[rexp/n] < exp_2\,[rexp/n]$
- $(\neg p\,[rexp/n]) \equiv \neg(p\,[rexp/n])$
- $(p_1 \vee p_2)\,[rexp/n] \equiv p_1\,[rexp/n] \vee p_2\,[rexp/n]$
- $(p_1\ \widehat{\mathcal{U}}\ p_2)\,[rexp/n] \equiv (p_1\,[rexp/n])\ \widehat{\mathcal{U}}\ (p_2\,[rexp/n])$
- $(p_1\ \widehat{\mathcal{S}}\ p_2)\,[rexp/n] \equiv (p_1\,[rexp/n])\ \widehat{\mathcal{S}}\ (p_2\,[rexp/n])$
- $(\exists \mathrm{x}.p)\,[rexp/n] \equiv \exists \mathrm{x}.(p\,[rexp/n])$,
- $(\exists \epsilon.p)\,[rexp/n] \equiv \exists \epsilon.(p\,[rexp/n])$,
- $(\exists n_0.p)\,[rexp/n] \equiv \exists n_0.(p\,[rexp/n])$, *if* $n_0 \notin var(rexp) \cup \{n\})$.

Define substitution of event variable $\epsilon \in \mathfrak{E}$ *by state event expression* $evexp$ *in temporal formula* p *denoted* $p\,[evexp/\epsilon]$ *as follows:*

- $\mathbf{true}\,[evexp/\epsilon] \equiv \mathbf{true}$
- $(exp_1 = exp_2)\,[evexp/\epsilon] \equiv (exp_1 = exp_2)$
- $(evexp_1 = evexp_2)\,[evexp/\epsilon] \equiv (evexp_1\,[evexp/\epsilon] = evexp_2\,[evexp/\epsilon])$
- $(exp_1 < exp_2)\,[evexp/\epsilon] \equiv (exp_1 < exp_2)$
- $(\neg p)\,[evexp/\epsilon] \equiv \neg(p\,[evexp/\epsilon])$
- $(p_1 \vee p_2)\,[evexp/\epsilon] \equiv (p_1\,[evexp/\epsilon]) \vee (p_2\,[evexp/\epsilon])$
- $(p_1\ \widehat{\mathcal{U}}\ p_2)\,[evexp/\epsilon] \equiv (p_1\,[evexp/\epsilon])\ \widehat{\mathcal{U}}\ (p_2\,[evexp/\epsilon])$
- $(p_1\ \widehat{\mathcal{S}}\ p_2)\,[evexp/\epsilon] \equiv (p_1\,[evexp/\epsilon])\ \widehat{\mathcal{S}}\ (p_2\,[evexp/\epsilon])$
- $(\exists \mathrm{x}.p)\,[evexp/\epsilon] \equiv \exists \mathrm{x}.(p\,[evexp/\epsilon])$
- $(\exists \epsilon_0.p)\,[evexp/\epsilon] \equiv \exists \epsilon_0.(p\,[evexp/\epsilon])$ *where* $\epsilon_0 \notin evar(evexp) \cup \{\epsilon\}$.

The following introduces the *history variant* of a history.

Definition 26 (History variant)
The **history variant** *of a history with respect to non-rigid process variable* $w \in \mathfrak{V} \cup \mathfrak{X}$, *and a state expression* exp, *denoted by* $(h : w \rightsquigarrow exp)$, *is defined for* $w_1 \in \mathfrak{V} \cup \mathfrak{X}$ *as follows: Let* $\mu \in Val$ *and* $\sigma \in \Sigma$ *then*

$$(\sigma : w \mapsto \mu)(w_1) \triangleq \begin{cases} \mu & \text{if } w_1 \equiv w \\ \sigma(w_1) & \text{if } w_1 \not\equiv w \end{cases}$$

then

$$(h : w \rightsquigarrow exp)(t_0) \triangleq \langle \psi_h(t_0), (\theta_h(t_0) : w \mapsto (h, t_0) \models exp)\rangle$$

The **history variant** *of a history with respect to rigid process variable* $n \in \mathfrak{R}$, *and a state rigid expression* $rexp$, *denoted by* $(h : n \rightsquigarrow rexp)$, *is defined for* $n_1 \in \mathfrak{R}$ *as follows: Let* $\mu \in Val$ *and* $\sigma \in \Sigma$ *then*

$$(\sigma : n \mapsto \mu)(n_1) \triangleq \begin{cases} \mu & \text{if } n_1 \equiv n \\ \sigma(n_1) & \text{if } n_1 \not\equiv n \end{cases}$$

then

$$(h : n \rightsquigarrow rexp)(t_0) \triangleq \langle \psi_h(t_0), (\theta_h(t_0) : n \mapsto (h, t_0) \models rexp)\rangle$$

The **history variant** *of a history with respect to event variable* $\epsilon \in \mathfrak{E}$, *and a state event expression* $evexp$, *denoted by* $(h : \epsilon \rightsquigarrow evexp)$, *is defined for* $\epsilon_1 \in \mathfrak{E}$ *as follows: Let* $\mathbf{a} \in \mathfrak{A}$ *and* $\delta \in \Delta$ *then*

$$(\delta : \epsilon \mapsto \mathbf{a})(\epsilon_1) \triangleq \begin{cases} \mathbf{a} & \text{if } \epsilon_1 \equiv \epsilon \\ \delta(\epsilon_1) & \text{if } \epsilon_1 \not\equiv \epsilon \end{cases}$$

then

$$(h:\epsilon \rightsquigarrow evexp)(t_0) \triangleq \langle(\psi_h(t_0):\epsilon \mapsto (h,t_0) \models evexp), \theta_h(t_0)\rangle$$

The following substitution lemma holds.

Lemma 2 (Substitution lemma)
Let exp_0 be an expression, exp be a state expression, $w \in \mathfrak{V} \cup \mathfrak{X}$, $rexp$ be a state rigid expression, $n \in \mathfrak{R}$, $evexp_0$ an event expression, $evexp$ a state event expression, $\epsilon \in \mathfrak{E}$, and p a temporal formula. Then the following holds:

- *a* $(h,t) \models exp_0[exp/w] = ((h:w \rightsquigarrow exp),t) \models exp_0$
- *b* $(h,t) \models exp_0[rexp/n] = ((h:n \rightsquigarrow rexp),t) \models exp_0$
- *c* $(h,t) \models evexp_0[evexp/\epsilon] = ((h:\epsilon \rightsquigarrow evexp),t) \models evexp_0$
- *d* $(h,t) \models p[exp/w]$ *iff* $((h:w \rightsquigarrow exp),t) \models p$
- *e* $(h,t) \models p[rexp/n]$ *iff* $((h:n \rightsquigarrow rexp),t) \models p$
- *f* $(h,t) \models p[evexp/\epsilon]$ *iff* $((h:\epsilon \rightsquigarrow evexp),t) \models p$

The following proof system for DTL is inspired on [Bur82, Bur84, BKP86, MP89]. An erroneous variant of it appeared in [BKP86] where these authors state that it is "an almost verbatim copy of [Bur84]" indeed "almost" their axiom F5 was not copied well. Furthermore a link with the proof system of [KMP93] is established via axioms $AX7b$–$AX7f$, i.e., these axioms are needed for deriving their proof system. Note: because the models of [Bur82, Bur84] need not to satisfy the finite variability condition, and the persistency condition (once in an interval "going back or forward" doesn't bring you outside that interval, and the induction axiom. This is the crucial differrence between the model of [KMP93] and ours and the one in [Bur82, Bur84]. The differrence between the model of [KMP93] and our model is that we have additional compositionality information as reflected in axioms AX0, AX5 and AX6.

The proof system is for the pure logic, i.e., it is not meant for a specific reactive system. Axioms AX0-AX9 characterize our notion of histories; they should follow from the definition of history (Def. 9), and, because a history is a pair consisting of a event and a state function, also from Definition 7 and 8. Ax10 and Ax11 are the axioms for substitution and quantification. Axioms F1-F7 are the axioms of the future part of DTL and P1-P7 the past part. As rules we take standard ones, i.e., the modus ponus, generalization, specialization, instantiation and universal generalization.

Definition 27 (Proof system for DTL)
Let $n \in \mathfrak{R}$, $\mathbf{v} \in \mathfrak{V}$, $w \in \mathfrak{V} \cup \mathfrak{X}$, $\mathrm{x} \in \mathfrak{X}$ and $\epsilon \in \mathfrak{E}$.

Axioms *All the axioms for state formulae.*

$$AX0: \quad (\epsilon = \mathbf{a}? \vee \epsilon = \mathbf{a}! \vee \epsilon = \mathbf{i} \vee \epsilon = \mathbf{e}) \Rightarrow (\epsilon' = \lambda \wedge {}^{`}\epsilon = \lambda)$$

Non-λ actions are points surrounded by λ actions conform Definition 7.

$$AX1: \quad \mathbf{first} \rightarrow \epsilon = \lambda \wedge \mathbf{v}' = \mathbf{v} \wedge \mathrm{x}' = \mathrm{x}$$

The initially stuttering requirement conform Definition 7 and 8.

$$AX2: \quad \Box(\grave{\mathrm{x}} = \mathrm{x} \wedge \grave{\mathbf{v}} = \mathbf{v})$$

The process variables are left continuous variables conform Definition 8.

$$AX3: \quad \bigcirc(\mathrm{x}' = \mathrm{x} \wedge \mathbf{v}' = \mathbf{v}) \wedge (((\mathrm{x}' \neq \mathrm{x} \vee \mathbf{v}' \neq \mathbf{v}) \Rightarrow \bigcirc(\mathrm{x}'' = \mathrm{x}' \wedge \mathbf{v}'' = \mathbf{v}'))$$

The value of process variables are maintained during an interval, conform Definition 8.

$$AX4: \quad \Box(n = n' \wedge n = \grave{n})$$

The rigid variables don't change at all conform Definition 8.

$$AX5: \quad (\epsilon = \mathbf{a}? \vee \epsilon = \mathbf{a}!) \Rightarrow \mathbf{v}' = \mathbf{v}$$

Communication actions don't change the shared variables conform Definition 9.

$$AX6: \quad \epsilon = \lambda \Rightarrow (\mathbf{v}' = \mathbf{v} \wedge \mathrm{x}' = \mathrm{x})$$

A λ action causes no state change.

$$\begin{array}{ll} AX7a: & \widehat{\Diamond} p \Rightarrow \widehat{\Diamond}\widehat{\Diamond} p \\ AX7b: & \neg\bigcirc p \Rightarrow \bigcirc\neg p \\ AX7c: & \neg\ominus p \Rightarrow \ominus\neg p) \\ AX7d: & \bigcirc\ominus p \Rightarrow \bigcirc p \\ AX7e: & \ominus\bigcirc p \Rightarrow \ominus p \\ AX7f: & (p \wedge p \Rightarrow \bigcirc p \wedge \ominus p \Rightarrow p) \rightarrow \Box p \end{array}$$

The underlying structure is dense (a), and satisfies the finite variability condition (b & c), and is persistent (d & e). Axiom (f) is the induction axiom. For an explanation of d–f see [KMP93].

$$AX8: \quad \Box\widehat{\Diamond}\mathbf{true}$$

There is no last element, i.e., the future is unbounded.

$$AX9: \quad \Box\widehat{\Diamond}\widehat{\diamondminus}\widehat{\boxminus}\mathbf{false}$$

There exists a first element.

$$\begin{array}{lll} AX10: & & (exp_1 = exp_2) \Rightarrow (p\,[exp_1/w] \leftrightarrow p\,[exp_2/w]) \\ & \wedge & (rexp_1 = rexp_2) \Rightarrow (p\,[rexp_1/n] \leftrightarrow p\,[rexp_2/n]) \\ & \wedge & (evexp_1 = evexp_2) \Rightarrow (p\,[evexp_1/\epsilon] \leftrightarrow p\,[evexp_2/\epsilon]) \end{array}$$

where p is a state formula and none of the variables appearing in respectively exp_1, exp_2, $rexp_1$, $rexp_2$, $evexp_1$ *and* $evexp_2$ *is quantified in p.*
Replacement of equal expressions.

$$\begin{array}{lll} AX11: & & (\forall \mathrm{x}.p) \Rightarrow p\,[exp/\mathrm{x}] \\ & \wedge & (\forall n.p) \Rightarrow p\,[rexp/n] \\ & \wedge & (\forall \epsilon.p) \Rightarrow p\,[evexp/\epsilon] \end{array}$$

where none of the variables appearing in exp, rexp and evexp is quantified in p.
Quantifier instantiation.

$$F1: \ \widehat{\Box}(p \rightarrow q) \Rightarrow (r\ \widehat{\mathcal{U}}\ p \rightarrow r\ \widehat{\mathcal{U}}\ q)$$

$\widehat{\mathcal{U}}$ *is monotonic in its second argument.*

$$F2: \ \widehat{\Box}(p \rightarrow q) \Rightarrow (p\ \widehat{\mathcal{U}}\ r \rightarrow q\ \widehat{\mathcal{U}}\ r)$$

$\widehat{\mathcal{U}}$ *is monotonic in its first argument.*

$$F3: \ (p \wedge r\ \widehat{\mathcal{U}}\ q) \Rightarrow (r\ \widehat{\mathcal{U}}\ (q \wedge r\ \widehat{\mathcal{S}}\ p))$$

The relation of reflection holding between past and future.

$$F4: \ (q\ \widehat{\mathcal{U}}\ p \wedge \neg(r\ \widehat{\mathcal{U}}\ p)) \Rightarrow q\ \widehat{\mathcal{U}}\ (q \wedge \neg r)$$

$$F5: \ q\ \widehat{\mathcal{U}}\ p \Rightarrow (q \wedge q\ \widehat{\mathcal{U}}\ p)\ \widehat{\mathcal{U}}\ p$$

$$F6: \ q\ \widehat{\mathcal{U}}\ (q \wedge q\ \widehat{\mathcal{U}}\ p) \Rightarrow q\ \widehat{\mathcal{U}}\ p$$

$$F7: \ (q\ \widehat{\mathcal{U}}\ p \wedge s\ \widehat{\mathcal{U}}\ r) \Rightarrow (q \wedge s)\ \widehat{\mathcal{U}}\ (p \wedge r) \vee (q \wedge s)\ \widehat{\mathcal{U}}\ (p \wedge s) \vee (q \wedge s)\ \widehat{\mathcal{U}}\ (q \wedge r)$$

The underlying structure is linear.

$$P1: \ \widehat{\boxminus}(p \rightarrow q) \Rightarrow (r\ \widehat{\mathcal{S}}\ p \rightarrow r\ \widehat{\mathcal{S}}\ q)$$

$\widehat{\mathcal{S}}$ *is monotonic in its second argument.*

$$P2: \ \widehat{\boxminus}(p \rightarrow q) \Rightarrow (p\ \widehat{\mathcal{S}}\ r \rightarrow q\ \widehat{\mathcal{S}}\ r)$$

$\widehat{\mathcal{S}}$ *is monotonic in its first argument.*

$$P3: \ (p \wedge r\ \widehat{\mathcal{S}}\ q) \Rightarrow (r\ \widehat{\mathcal{S}}\ (q \wedge r\ \widehat{\mathcal{U}}\ p))$$

The relation of reflection holding between past and future.

$$P4: \quad (q\ \widehat{\mathcal{S}}\ p \wedge \neg(r\ \widehat{\mathcal{S}}\ p)) \Rightarrow q\ \widehat{\mathcal{S}}\ (q \wedge \neg r)$$

$$P5: \quad q\ \widehat{\mathcal{S}}\ p \Rightarrow (q \wedge q\ \widehat{\mathcal{S}}\ p)\ \widehat{\mathcal{S}}\ p$$

$$P6: \quad q\ \widehat{\mathcal{S}}\ (q \wedge q\ \widehat{\mathcal{S}}\ p) \Rightarrow q\ \widehat{\mathcal{S}}\ p$$

$$P7: \quad (q\ \widehat{\mathcal{S}}\ p \wedge s\ \widehat{\mathcal{S}}\ r) \Rightarrow (q \wedge s)\ \widehat{\mathcal{S}}\ (p \wedge r) \vee (q \wedge s)\ \widehat{\mathcal{S}}\ (p \wedge s) \vee (q \wedge s)\ \widehat{\mathcal{S}}\ (q \wedge r)$$

The underlying structure is linear.

Rules

$$\frac{p,\ p \rightarrow q}{q}$$

The Modus Ponus.

$$\frac{p}{\widehat{\Box} p} \quad \textit{for state formula } p \textit{ in which all occurrences of parameterized sentence symbols in } p \textit{ are rigid}$$

Generalization.

$$\frac{\Box p}{p} \textit{for state formula } p$$

Specialization.

$$\frac{p}{p\,[p_1/p_0]} \textit{where } p_1 \textit{ doesn't contain variables which are bound in } p$$

Instantiation.

$$\frac{p_0 \Rightarrow p_1}{p_0 \Rightarrow \forall \mathrm{x}.p_1} \textit{for } \mathrm{x} \textit{ not free in } p_0$$

$$\frac{p_0 \Rightarrow p_1}{p_0 \Rightarrow \forall n.p_1} \textit{for } n \textit{ not free in } p_0$$

$$\frac{p_0 \Rightarrow p_1}{p_0 \Rightarrow \forall \epsilon.p_1} \textit{for } \epsilon \textit{ not free in } p_0$$

Universal Generalization.

The following definition characterizes a machine M in DTL. This kind of DTL formulae is history stutter insensitive.

Definition 28 (Machine in DTL)
Given basis $B = ((\mathrm{In}, \mathrm{Out}), (\mathrm{V}, \mathrm{X}))$. *Let* $\mathrm{In}?$ *be defined as* $\{\mathbf{a}? \mid a \in \mathrm{In}\}$ *and let* $\mathrm{Out}!$ *be defined as* $\{\mathbf{a}! \mid a \in \mathrm{Out}\}$. *Let* I *be a DTL formula over* $\mathrm{V} \cup \mathrm{X}$ *without the* $\widehat{\mathcal{S}}$, $\widehat{\mathcal{U}}$ *and* $\exists$ *operators. Let* $\mathcal{T}$ *be a finite set of DTL formulae* τ *of the form* $(event_\tau \wedge trans_\tau)$ *where* $event_\tau$ *is of the form* $\epsilon = a_\tau$ *where* $a_\tau \in \{\mathbf{i}, \mathbf{e}\} \cup \mathrm{In}? \cup \mathrm{Out}!$, *and* $trans_\tau$ *a DTL formula over* $\mathrm{V} \cup \mathrm{X}$ *and* $\mathrm{V}' \cup \mathrm{X}'$ *(variables primed with ') without the* $\widehat{\mathcal{S}}$, $\widehat{\mathcal{U}}$ *and* $\exists$ *operators such that* $(\epsilon = \mathbf{e} \Rightarrow \bigwedge_{\mathrm{x} \in \mathrm{X}} \mathrm{x}' = \mathrm{x})$, *i.e., an environment action doesn't change the local variables of the system. Define the stutter step, denoted by* **stut**, *as* $\epsilon = \lambda \vee (\epsilon = \mathbf{i} \wedge (\mathrm{V}, \mathrm{X})' = (\mathrm{V}, \mathrm{X})) \vee (\epsilon = \mathbf{e} \wedge (\mathrm{V}, \mathrm{X})' = (\mathrm{V}, \mathrm{X}))$. *Let* T *be the DTL formula* $\mathbf{stut} \vee \bigvee_{\tau \in \mathcal{T}} \tau$. *A machine in DTL is defined as* $(B, \mathrm{I} \wedge \Box \mathrm{T})$.

Lemma 3
Given a machine in DTL $(B, \mathrm{I} \wedge \Box \mathrm{T})$ *then there exists a semantic machine* $M = (B, I, T)$ *such that* $Comp(M) = Hist(\mathrm{I} \wedge \Box \mathrm{T})$.

The following example is an illustration of a machine in DTL.

Example 3
Machine M *in example 1 as DTL-formula:*

1. **Basis:** $B = ((\mathrm{In}, \mathrm{Out}), (\mathrm{V}, \mathrm{X}))$ *where*

$$\begin{array}{lcl} \mathrm{In} & \triangleq & \{a\}, \\ \mathrm{Out} & \triangleq & \emptyset, \\ \mathrm{V} & \triangleq & \{\mathbf{v}\}, \\ \mathrm{X} & \triangleq & \{\mathrm{u}\} \end{array}$$

2. **Initial States:**
$\mathrm{I} \triangleq (\mathbf{v}, \mathrm{u}) = (0, 0)$

3. **Transitions:**
$$\begin{array}{l} \mathrm{T} \triangleq \\ \big(\epsilon = \mathbf{a}? \wedge \mathrm{u} = 0 \wedge (\mathbf{v}, \mathrm{u})' = (\mathbf{v}, 1)\big) \ \vee \\ \big(\epsilon = \mathbf{i} \wedge (\mathbf{v}, \mathrm{u}) = (1, 1) \wedge (\mathbf{v}, \mathrm{u})' = (0, 2)\big) \ \vee \\ \big(\epsilon = \mathbf{e} \wedge (\mathbf{v}, \mathrm{u})' = (\mathbf{v} + 1, \mathrm{u})\big) \ \vee \\ \mathbf{stut} \end{array}$$

The machine specification of a system in DTL is as follows.

Definition 29 (Machine specification of a system in DTL)
Given a machine $(B, \mathrm{I} \wedge \Box \mathrm{T})$ *in DTL. Let* $\mathrm{WF} \subseteq \mathcal{T}$ *be the set of weak fair transitions and* $\mathrm{SF} \subseteq \mathcal{T}$ *be the set of strong fair transitions. For* $\tau \in \mathcal{T}$ *define the enabledness condition for* τ *denoted* $En(\tau)$ *as* $\exists \bar{v}_0 . \tau\,[\bar{v}_0 / \bar{v}']$ *where* $\tau\,[\bar{v}_0 / \bar{v}']$ *denotes the substitution of* $\bar{v}_0$ *(a list of variables not in* $\mathrm{V} \cup \mathrm{X}$*) for* $\bar{v}'$ *(the list of primed variables in* τ*). Let* L *be the DTL formula* $\bigwedge_{\tau \in \mathrm{WF}} (\Diamond \Box En(\tau) \rightarrow \Box \Diamond \tau) \wedge \bigwedge_{\tau \in \mathrm{SF}} (\Box \Diamond En(\tau) \rightarrow \Box \Diamond \tau)$. *The* **machine specification** *of a system in DTL is then a tuple* $(B, \mathrm{I} \wedge \Box \mathrm{T} \wedge \mathrm{L})$.

Note: in above definition L is such that $cl(Hist(\mathrm{I} \wedge \Box\mathrm{T}) \cap Hist(\mathrm{L})) = Hist(\mathrm{I} \wedge \Box\mathrm{T})$, i.e., it satisfies the machine closedness property. With this the following lemma is straight forward.

Lemma 4
Given DTL machine specification $(B, \mathrm{I} \wedge \Box\mathrm{T} \wedge \mathrm{L})$ *of a system, there exists a semantic machine specification* $\mathcal{S} = (B, Comp(M) \cap L)$ *such that* $Comp(M) \cap L = Hist(\mathrm{I} \wedge \Box\mathrm{T} \wedge \mathrm{L})$.

2.3 Refinement and Composition of Reactive System Specifications

In this section the notion of *refinement* and *composition* of reactive systems is introduced. Intuitively refinement means that the set of histories of a concrete system is a subset of the set of histories of an abstract system. Composition means that the histories of the component systems are "merged" into composite histories, i.e., the histories of the composed system. Our merge operator is based on the merge operator of Aczel [Acz83]. Both are first defined at the semantic level and then for the DTL specifications.

2.3.1 Semantic Refinement and Composition of Specifications

In this section refinement and composition of reactive systems is defined at the semantical level. Refinement means that the set of histories of a concrete system is a subset of the set of histories of an abstract system. Because histories also contains local information the subset relation doesn't correspond directly with refinement. The local information should first be projected away. The following definition captures this projection of local information.

Definition 30 (Observable system specification)
Given system specification $\mathcal{S} = (B, H)$ *where* $B = ((\mathrm{In}, \mathrm{Out}), (\mathrm{V}, \mathrm{X}))$. *The* **observable system specification** *is defined as* $(\mathfrak{O}(B), \mathcal{O}_{\mathrm{X}}(H))$ *where* $\mathfrak{O}(B)$ *denotes the observable basis and is defined as* $\mathfrak{O}(B) \triangleq ((\mathrm{In}, \mathrm{Out}), \mathrm{V}, \emptyset)$ *and* $\mathcal{O}_{\mathrm{X}}(H)$ *denotes the set of observable histories corresponding to* H *and is defined as*

$$\{h \in \mathcal{H} \mid \exists h_1 \in H : h \textit{ is an } \mathrm{X}\textit{-variant of } h_1\}$$

Definition 31 (Refinement of systems)
Given concrete system $\mathcal{S}_c \triangleq (B_c, H_c)$ *and abstract system* $\mathcal{S}_a \triangleq (B_a, H_a)$.
$\mathcal{S}_c$ **refines** $\mathcal{S}_a$ *denoted by* $\mathcal{S}_c$ **ref** $\mathcal{S}_a$ *iff* $\mathfrak{O}(B_c) = \mathfrak{O}(B_a)$ *and* $\mathcal{O}_{\mathrm{X}_c}(H_c) \subseteq \mathcal{O}_{\mathrm{X}_a}(H_a)$.

A more general definition of refinement would be one wherein both the abstract and concrete system are composed of subsystems. Therefore the notion of *composition* is introduced. Intuitively the composition of two systems is that *matching* histories are merged into one history. A history of one system matches a history of the other system if for all time points t

(1) the state information of the two histories at time t are same and

(2a) in both histories the λ-action occurs at time t or

(2b) in both histories the environment action $\mathbf{e}$ occurs at time t or

(2c) in one history at time t a process action $\mathbf{i}$ occurs and in the other one an environment action $\mathbf{e}$ occurs at time t or

(2d) in both histories at time t a communication action $\mathbf{a}$ occurs which is an input action in one of them and an output action in the other one

(2e) in one history at time t a communication action occurs which is not an communication action in the other one and in the other history an environment action $\mathbf{e}$ occurs.

So if the two components each perform an $\mathbf{i}$ action this prohibited because we want to model interleaving where only communication actions can possible occur simultaneously. Two matching histories are then merged into one history by (1) "copying" the state-information of the two histories; and in case (2a) the resulting event becomes λ, and in case (2b) the resulting event becomes $\mathbf{e}$, and in case (2c) the resulting event becomes $\mathbf{i}$, and in case (2d) the resulting event becomes $\mathbf{i}$, and in case (2e) the resulting event becomes the communication action.

Definition 32 (Composition of two systems)
Given systems $\mathcal{S}_i = (B_i, H_i)$ *with* $B_i = ((\mathrm{In}_i, \mathrm{Out}_i), (\mathrm{V}_i, \mathrm{X}_i))$ $(i = 1, 2)$ *such that* $\mathrm{In}_1 \cap \mathrm{In}_2 = \emptyset$, $\mathrm{Out}_1 \cap \mathrm{Out}_2 = \emptyset$ *and* $\mathrm{X}_1 \cap \mathrm{X}_2 = \emptyset$. *The* **composed system** $\mathcal{S} = \mathcal{S}_1 \parallel \mathcal{S}_2$ *is defined as* (B, H) *with* $B \triangleq ((\mathrm{In}_1 \setminus \mathrm{Out}_2 \cup \mathrm{In}_2 \setminus \mathrm{Out}_1, \mathrm{Out}_1 \setminus \mathrm{In}_2 \cup \mathrm{Out}_2 \setminus \mathrm{In}_1), (\mathrm{V}_1 \cup \mathrm{V}_2, \mathrm{X}_1 \cup \mathrm{X}_2))$ *and* $H \triangleq H_1 \bigotimes H_2$. *The* $\bigotimes$ *is the* **merge** *operator which merges the histories* $h_1 \in H_1$ *and* $h_2 \in H_2$ *into one history* h *and which is defined as follows:*

$$H_1 \bigotimes H_2 \triangleq \{h \in \mathcal{H} \mid \exists h_1 \in H_1, h_2 \in H_2. \otimes (h, h_1, h_2)\}$$

where for $h = \langle \psi, \theta \rangle$ *and* $h_j = \langle \psi_j, \theta_j \rangle$ $(j = 1, 2)$,
$\otimes(h, h_1, h_2)$ *iff*

$$
\begin{array}{ll}
- & \theta = \theta_1 \wedge \theta = \theta_2 \\
- & \forall t : \\
\vee & \psi(t)(\epsilon) = \lambda \wedge \psi_1(t)(\epsilon) = \lambda \wedge \psi_2(t)(\epsilon) = \lambda \\
\vee & \psi(t)(\epsilon) = \mathbf{e} \wedge \psi_1(t)(\epsilon) = \mathbf{e} \wedge \psi_2(t)(\epsilon) = \mathbf{e} \\
\vee & \psi(t)(\epsilon) = \mathbf{i} \wedge \psi_1(t)(\epsilon) = \mathbf{i} \wedge \psi_2(t)(\epsilon) = \mathbf{e} \\
\vee & \psi(t)(\epsilon) = \mathbf{i} \wedge \psi_1(t)(\epsilon) = \mathbf{e} \wedge \psi_2(t)(\epsilon) = \mathbf{i} \\
\vee & \exists \mathbf{a} \in \mathrm{In}_1 \cap \mathrm{Out}_2 : \psi(t)(\epsilon) = \mathbf{i} \wedge \psi_1(t)(\epsilon) = \mathbf{a}? \wedge \psi_2(t)(\epsilon) = \mathbf{a}! \\
\vee & \exists \mathbf{a} \in \mathrm{In}_2 \cap \mathrm{Out}_1 : \psi(t)(\epsilon) = \mathbf{i} \wedge \psi_1(t)(\epsilon) = \mathbf{a}! \wedge \psi_2(t)(\epsilon) = \mathbf{a}? \\
\vee & \exists \mathbf{a} \in \mathrm{In}_1 \setminus \mathrm{Out}_2 : \psi(t)(\epsilon) = \mathbf{a}? \wedge \psi_1(t)(\epsilon) = \mathbf{a}? \wedge \psi_2(t)(\epsilon) = \mathbf{e} \\
\vee & \exists \mathbf{a} \in \mathrm{Out}_1 \setminus \mathrm{In}_2 : \psi(t)(\epsilon) = \mathbf{a}! \wedge \psi_1(t)(\epsilon) = \mathbf{a}! \wedge \psi_2(t)(\epsilon) = \mathbf{e} \\
\vee & \exists \mathbf{a} \in \mathrm{In}_2 \setminus \mathrm{Out}_1 : \psi(t)(\epsilon) = \mathbf{a}? \wedge \psi_1(t)(\epsilon) = \mathbf{e} \wedge \psi_2(t)(\epsilon) = \mathbf{a}? \\
\vee & \exists \mathbf{a} \in \mathrm{Out}_2 \setminus \mathrm{In}_1 : \psi(t)(\epsilon) = \mathbf{a}! \wedge \psi_1(t)(\epsilon) = \mathbf{e} \wedge \psi_2(t)(\epsilon) = \mathbf{a}!
\end{array}
$$

The following Lemma expresses that the "making observable"-operation and the merge operator are monotonic and that the "making observable"-operation on the composed system is equal to the "making observable"-operation on the components.

Lemma 5 (Properties of $\mathcal{O}$ and $\otimes$)
Given systems (B_1, H_0), (B_1, H_1), (B_2, H_2) and (B_2, H_3) then

(a) $H_0 \subseteq H_1$ *implies* $H_0 \otimes H_2 \subseteq H_1 \otimes H_2$
(b) $\mathcal{O}_{\mathrm{X}_{12}}(H_1 \otimes H_2) = \mathcal{O}_{\mathrm{X}_1}(H_1) \otimes \mathcal{O}_{\mathrm{X}_2}(H_2)$
(c) $H_0 \subseteq H_1$ *implies* $\mathcal{O}_{\mathrm{X}_1}(H_0) \subseteq \mathcal{O}_{\mathrm{X}_1}(H_1)$
(d) $(H_0 \cap H_1) \otimes (H_2 \cap H_3) \subseteq (H_0 \otimes H_2) \cap (H_1 \otimes H_3)$

The following theorem of compositional refinement can be inferred from the above lemma.

Theorem 3 (Compositional refinement)
Given concrete systems $\mathcal{S}_i = (B_i, H_i)$ $(i = 1, 2)$ and abstract systems $\mathcal{S}_j = (B_j, H_j)$ $(j = 3, 4)$ such that $\mathfrak{O}(B_1) = \mathfrak{O}(B_3)$ and $\mathfrak{O}(B_2) = \mathfrak{O}(B_4)$ then $\mathcal{S}_1$ **ref** *$\mathcal{S}_3$ and $\mathcal{S}_2$* **ref** *$\mathcal{S}_4$ implies $\mathcal{S}_1 \parallel \mathcal{S}_2$* **ref** *$\mathcal{S}_3 \parallel \mathcal{S}_4$.*

It is very common that a shared variable is only used by the subcomponents of a system and not by the environment of the system. This variable acts then as a local variable for the system. The following definition introduces *encapsulation* which makes certain shared variables local to the system.

Definition 33 (Encapsulation)
Given system $\mathcal{S} = (B, H)$ where $B = ((\mathrm{In}, \mathrm{Out}), (\mathrm{V}, \mathrm{X}))$ then **encapsulation** *of V_1 in $\mathcal{S}$ with $\mathrm{V}_1 \subseteq \mathrm{V}$ is denoted by $\mathcal{S} \upharpoonright \mathrm{V}_1$ and defined by $(B_1, Enc_{\mathrm{V}_1}(H))$ where $B_1 \triangleq ((\mathrm{In}, \mathrm{Out}), (\mathrm{V} \setminus \mathrm{V}_1, \mathrm{X} \cup ren(\mathrm{V}_1)))$ where ren is a mapping from the shared variables to the local variables and intuitively "renames" the shared variables of V_1 to fresh local variables (not already in X). The encapsulation operator $Enc_{\mathrm{V}_1}(H)$ is defined as*

$$\{h \in \mathcal{H} \mid h \in H \wedge \forall t : \psi(t)(\epsilon) = \mathbf{e} \rightarrow \theta(t)|^1_{\mathrm{V}_1} = \lim_{t \leftarrow t_1} \theta(t_1)|^1_{\mathrm{V}_1}\}$$

As *ren* mapping in above definition we usually take the identity mapping (almost it transforms bold variables names to non-bold variables names) because those shared variables that we want to make local are not yet in the set of local variables. In the following when *ren* is not given this identity mapping should be assumed.

2.3.2 Refinement and Composition of DTL Specifications

In this section the refinement and composition notion of the previous section are translated into DTL by defining it for machine specifications (Def. 29). This means that first the *observable* machine specification should be defined in DTL.

Definition 34 (Observable machine specification in DTL)
Given machine specification $(B, \mathrm{I} \wedge \Box \mathrm{T} \wedge \mathrm{L})$ in DTL and then the corresponding **observable** *machine specification is defined as $(\mathfrak{O}(B), (\exists \mathrm{X} \,.\, (\mathrm{I} \wedge \Box \mathrm{T} \wedge \mathrm{L})))$.*

The following lemma expresses that existential quantification relates to the semantic notion of observable histories.

Lemma 6
Given DTL machine specification $\mathcal{S} = (B, \mathrm{I} \wedge \Box\mathrm{T} \wedge \mathrm{L})$ *then* $\mathcal{O}_{\mathrm{X}}(Hist(\mathrm{I} \wedge \Box\mathrm{T} \wedge \mathrm{L})) = Hist((\exists \mathrm{X} \,.\, (\mathrm{I} \wedge \Box\mathrm{T} \wedge \mathrm{L})))$

Theorem 4 (Refinement of machine specifications)
Given concrete machine specification $\mathcal{S}_c \triangleq (B_c, \mathrm{I}_c \wedge \Box\mathrm{T}_c \wedge \mathrm{L}_c)$ *where* $B_c \triangleq (B_c^A, (\mathrm{V}_c, \mathrm{X}_c))$ *and abstract machine specification* $\mathcal{S}_a \triangleq (B_a, \mathrm{I}_a \wedge \Box\mathrm{T}_a \wedge \mathrm{L}_a)$ *where* $B_a \triangleq (B_a^A, (\mathrm{V}_a, \mathrm{X}_a))$. *Then* $\mathcal{S}_c$ **refines** $\mathcal{S}_a$ *denoted* $\mathcal{S}_c$ **ref** $\mathcal{S}_a$ *iff*

$$
\begin{array}{l}
\mathfrak{O}(B_c) = \mathfrak{O}(B_a) \text{ and} \\
(\exists \mathrm{X}_c \,.\, (\mathrm{I}_c \wedge \Box\mathrm{T}_c \wedge \mathrm{L}_c)) \rightarrow (\exists \mathrm{X}_a \,.\, (\mathrm{I}_a \wedge \Box\mathrm{T}_a \wedge \mathrm{L}_a))
\end{array}
$$

Composition of DTL machine specifications can be defined in the same way as in the previous section.

Definition 35 (Composition of two DTL machine specifications)
Given DTL machine system specifications $\mathcal{S}_i \triangleq (B_i, \mathrm{I}_i \wedge \Box\mathrm{T}_i \wedge \mathrm{L}_i)$ *where* $B_i \triangleq (B_i^A, B_i^P)$, *for* $i = 1, 2$. *Let* ${}_{B_1^A}\odot_{B_2^A}(\epsilon, \epsilon_1, \epsilon_2)$ *be defined as*

$$
\begin{array}{lll}
\Box(& & \\
& \vee & \epsilon = \lambda \wedge \epsilon_1 = \lambda \wedge \epsilon_2 = \lambda \\
& \vee & \epsilon = \mathbf{e} \wedge \epsilon_1 = \mathbf{e} \wedge \epsilon_2 = \mathbf{e} \\
& \vee & \epsilon = \mathbf{i} \wedge \epsilon_1 = \mathbf{i} \wedge \epsilon_2 = \mathbf{e} \\
& \vee & \epsilon = \mathbf{i} \wedge \epsilon_1 = \mathbf{e} \wedge \epsilon_2 = \mathbf{i} \\
& \vee & \bigvee_{\mathbf{a} \in \mathrm{In}_1 \cap \mathrm{Out}_2} \epsilon = \mathbf{i} \wedge \epsilon_1 = \mathbf{a}? \wedge \epsilon_2 = \mathbf{a}! \\
& \vee & \bigvee_{\mathbf{a} \in \mathrm{In}_2 \cap \mathrm{Out}_1} \epsilon = \mathbf{i} \wedge \epsilon_1 = \mathbf{a}! \wedge \epsilon_2 = \mathbf{a}? \\
& \vee & \bigvee_{\mathbf{a} \in \mathrm{In}_1 \setminus \mathrm{Out}_2} \epsilon = \mathbf{a}? \wedge \epsilon_1 = \mathbf{a}? \wedge \epsilon_2 = \mathbf{e} \\
& \vee & \bigvee_{\mathbf{a} \in \mathrm{Out}_1 \setminus \mathrm{In}_2} \epsilon = \mathbf{a}! \wedge \epsilon_1 = \mathbf{a}! \wedge \epsilon_2 = \mathbf{e} \\
& \vee & \bigvee_{\mathbf{a} \in \mathrm{In}_2 \setminus \mathrm{Out}_1} \epsilon = \mathbf{a}? \wedge \epsilon_1 = \mathbf{e} \wedge \epsilon_2 = \mathbf{a}? \\
& \vee & \bigvee_{\mathbf{a} \in \mathrm{Out}_2 \setminus \mathrm{In}_1} \epsilon = \mathbf{a}! \wedge \epsilon_1 = \mathbf{e} \wedge \epsilon_2 = \mathbf{a}! \\
) & &
\end{array}
$$

Then the **composed** *machine system specification* $\mathcal{S}$ *is defined as* (B, H) *where*

$$
\begin{array}{lll}
\mathrm{H} & \triangleq & \exists \epsilon_1, \epsilon_2 . {}_{B_1^A}\odot_{B_2^A}(\epsilon, \epsilon_1, \epsilon_2) \wedge (\mathrm{I}_1 \wedge \Box\mathrm{T}_1 \wedge \mathrm{L}_1)\,[\epsilon_1/\epsilon] \wedge (\mathrm{I}_2 \wedge \Box\mathrm{T}_2 \wedge \mathrm{L}_2)\,[\epsilon_2/\epsilon] \\
B & \triangleq & ((\mathrm{In}_1 \setminus \mathrm{Out}_2 \cup \mathrm{In}_2 \setminus \mathrm{Out}_1, \mathrm{Out}_1 \setminus \mathrm{In}_2 \cup \mathrm{Out}_2 \setminus \mathrm{In}_1), (\mathrm{V}_1 \cup \mathrm{V}_2, \mathrm{X}_1 \cup \mathrm{X}_2)).
\end{array}
$$

This definition can be easily extended for n DTL specifications. One has then to define a predicate $\odot_{\bar{B}^A}(\epsilon, \bar{\epsilon})$ corresponding to the operation of merging n components.

Theorem 5 (Semantic merge is almost conjunction)
Given machine system specifications $(B_i, \mathrm{I}_i \wedge \Box\mathrm{T}_i \wedge \mathrm{L}_i)$ *where* $B_i \triangleq ((\mathrm{In}_i, \mathrm{Out}_i), (\mathrm{V}_i, \mathrm{X}_i))$, *for* $i = 1, 2$ *and composed machine system specification as in definition 35, i.e.,* (B, H) *where* $\mathrm{H} \triangleq \exists \epsilon_1, \epsilon_2 . {}_{B_1^A}\odot_{B_2^A}(\epsilon, \epsilon_1, \epsilon_2) \wedge (\mathrm{I}_1 \wedge \Box\mathrm{T}_1 \wedge \mathrm{L}_1)\,[\epsilon_1/\epsilon] \wedge (\mathrm{I}_2 \wedge \Box\mathrm{T}_2 \wedge \mathrm{L}_2)\,[\epsilon_2/\epsilon]$ *and* $B \triangleq ((\mathrm{In}_1 \setminus \mathrm{Out}_2 \cup \mathrm{In}_2 \setminus \mathrm{Out}_1, \mathrm{Out}_1 \setminus \mathrm{In}_2 \cup \mathrm{Out}_2 \setminus \mathrm{In}_1), (\mathrm{V}_1 \cup \mathrm{V}_2, \mathrm{X}_1 \cup \mathrm{X}_2))$ *then*

$$
Hist(\mathrm{I}_1 \wedge \Box\mathrm{T}_1 \wedge \mathrm{L}_1) \bigotimes Hist(\mathrm{I}_2 \wedge \Box\mathrm{T}_2 \wedge \mathrm{L}_2) = Hist(\mathrm{H})
$$

Encapsulation of shared variables for DTL specifications is defined as follows.

Definition 36 (Encapsulation)
Given machine specification $\mathcal{S} \triangleq (B, \mathrm{H})$ *then* **encapsulation** *of* V_1 *in* $\mathcal{S}$ *with* $\mathrm{V}_1 \subseteq \mathrm{V}$ *denoted by* $\mathcal{S} \restriction \mathrm{V}_1$ *is defined as* $(B_1, \mathrm{H} \wedge (\epsilon = \mathbf{e} \Rightarrow \mathrm{V}_1' = \mathrm{V}_1))$ *where* $B_1 \triangleq (\mathrm{E}, \mathrm{V} \backslash \mathrm{V}_1, \mathrm{X} \cup \mathrm{V}_1)$.

The following theorem states that above definition indeed captures encapsulation.

Theorem 6
Given machine specification $\mathcal{S} \triangleq (B, \mathrm{H})$ *and given set of shared variables* $\mathrm{V}_1 \subseteq \mathrm{V}$ *then*

$$Enc_{\mathrm{V}_1}(Hist(\mathrm{H})) = Hist(\mathrm{H} \wedge (\epsilon = \mathbf{e} \Rightarrow \mathrm{V}_1' = \mathrm{V}_1))$$

Example 4
Abstract machine specification $\mathcal{S}_a \triangleq (B, \mathrm{I} \wedge \Box\mathrm{T} \wedge \mathrm{L})$ *is refined by the composition of concrete machines specifications* $\mathcal{S}_{c_1} \triangleq (B_1, \mathrm{I}_1 \wedge \Box\mathrm{T}_1 \wedge \mathrm{L}_1)$ *and* $\mathcal{S}_{c_2} \triangleq (B_2, \mathrm{I}_2 \wedge \Box\mathrm{T}_2 \wedge \mathrm{L}_2)$.

The abstract machine specification $\mathcal{S}_a$ *is defined as follows:*

1. **Basis** $B = ((\mathrm{In}, \mathrm{Out}), (\mathrm{V}, \mathrm{X}))$

$$\begin{array}{lcl} \mathrm{In} & \triangleq & \{\mathbf{b}\}, \\ \mathrm{Out} & \triangleq & \{\mathbf{a}\}, \\ \mathrm{V} & \triangleq & \{\mathrm{s}\}, \\ \mathrm{X} & \triangleq & \{\mathrm{x}\} \end{array}$$

2. **Initial States**

$$\mathrm{I} \triangleq (\mathrm{s}, \mathrm{x}) = (0, 0)$$

3. **Transitions**
$\mathrm{T} \triangleq$

$$\begin{array}{l} \vee \ \big(\epsilon = \mathbf{a}! \wedge \mathrm{x} = 0 \wedge (\mathrm{s}, \mathrm{x})' = (\mathrm{s}, 1)\big) \\ \vee \ \big(\epsilon = \mathbf{b}? \wedge \mathrm{x} = 1 \wedge (\mathrm{s}, \mathrm{x})' = (\mathrm{s}, 2)\big) \\ \vee \ \big(\epsilon = \mathbf{i} \wedge (\mathrm{s}, \mathrm{x}) = (1, 2) \wedge (\mathrm{s}, \mathrm{x})' = (0, \mathrm{x})\big) \\ \vee \ \big(\epsilon = \mathbf{e} \wedge (\mathrm{s}, \mathrm{x})' = (1, \mathrm{x})\big) \\ \vee \ \mathbf{stut}_a \end{array}$$

These transitions are illustrated in figure 2.4. Note: the stutter transitions are not drawn in all subsequent figures in order to minimize the number of edges.

4. **Liveness**

$$\mathrm{L} \triangleq \mathbf{true}$$

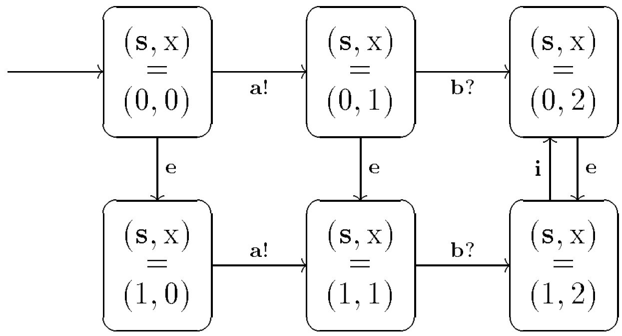

Figure 2.4: Abstract machine

The definition of $\mathcal{S}_{c_1}$ *is as follows:*

1. **Basis** $B_1 = ((\mathrm{In}_1, \mathrm{Out}_1), (\mathrm{V}_1, \mathrm{X}_1))$

$$
\begin{array}{lll}
\mathrm{In}_1 & \triangleq & \{\mathbf{c}\}, \\
\mathrm{Out}_1 & \triangleq & \{\mathbf{a}\}, \\
\mathrm{V}_1 & \triangleq & \{\mathrm{s}\}, \\
\mathrm{X}_1 & \triangleq & \{\mathrm{t}\}
\end{array}
$$

2. **Initial States**

$$\mathrm{I}_1 \triangleq (\mathrm{s}, \mathrm{t}) = (0, 0)$$

3. **Transitions**
$\mathrm{T}_1 \triangleq$

$$
\begin{array}{l}
\vee \ \Big(\epsilon = \mathbf{a}! \wedge \mathrm{t} = 0 \wedge (\mathrm{s}, \mathrm{t})' = (\mathrm{s}, 1)\Big) \\
\vee \ \Big(\epsilon = \mathbf{c}? \wedge \mathrm{t} = 1 \wedge (\mathrm{s}, \mathrm{t})' = (\mathrm{s}, 2)\Big) \\
\vee \ \Big(\epsilon = \mathbf{e} \wedge (\mathrm{s}, \mathrm{t})' = (1, \mathrm{t})\Big) \\
\vee \ \Big(\epsilon = \mathbf{e} \wedge (\mathrm{s}, \mathrm{t})' = (0, \mathrm{t})\Big) \\
\vee \ \mathbf{stut}_1
\end{array}
$$

These transitions are illustrated in figure 2.5

4. **Liveness**

$$\mathrm{L}_1 \triangleq \mathbf{true}$$

The definition of $\mathcal{S}_{c_2}$ *is as follows:*

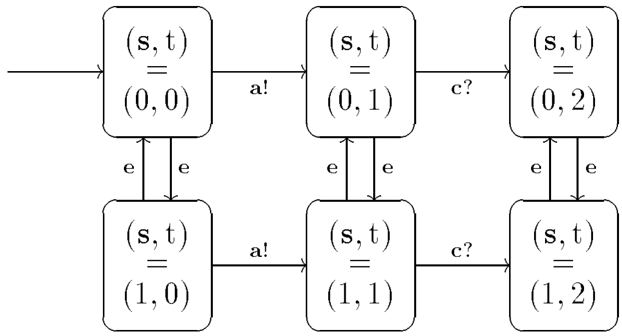

Figure 2.5: Concrete machine 1

1. **Basis** $B_2 = ((\mathrm{In}_2, \mathrm{Out}_2), (\mathrm{V}_2, \mathrm{X}_2))$

$$\begin{array}{lcl} \mathrm{In}_2 & \triangleq & \{\mathbf{b}\}, \\ \mathrm{Out}_2 & \triangleq & \{\mathbf{c}\}, \\ \mathrm{V}_2 & \triangleq & \{\mathrm{s}\}, \\ \mathrm{X}_2 & \triangleq & \{\mathrm{u}\} \end{array}$$

2. **Initial States**

$$\mathrm{I}_2 \triangleq (\mathrm{s}, \mathrm{u}) = (0, 0)$$

3. **Transitions**
$\mathrm{T}_2 \triangleq$

$$\begin{array}{l} \vee \ \left(\epsilon = \mathbf{c}! \wedge \mathrm{u} = 0 \wedge (\mathrm{s}, \mathrm{u})' = (\mathrm{s}, 1)\right) \\ \vee \ \left(\epsilon = \mathbf{b}? \wedge \mathrm{u} = 1 \wedge (\mathrm{s}, \mathrm{u})' = (\mathrm{s}, 2)\right) \\ \vee \ \left(\epsilon = \mathbf{i} \wedge (\mathrm{s}, \mathrm{u}) = (1, 2) \wedge (\mathrm{s}, \mathrm{u})' = (0, \mathrm{u})\right) \\ \vee \ \left(\epsilon = \mathbf{e} \wedge (\mathrm{s}, \mathrm{u})' = (1, \mathrm{u})\right) \\ \vee \ \mathbf{stut}_2 \end{array}$$

These transitions are illustrated in figure 2.6

4. **Liveness**
$\mathrm{L}_2 \triangleq \mathbf{true}$

According to definition 35 the composition of $\mathcal{S}_{c_1}$ and $\mathcal{S}_{c_2}$ is as follows:

$$\begin{array}{lll} (& ((\mathrm{In}_1 \setminus \mathrm{Out}_2 \cup \mathrm{In}_2 \setminus \mathrm{Out}_1, \mathrm{Out}_1 \setminus \mathrm{In}_2 \cup \mathrm{Out}_2 \setminus \mathrm{In}_1), (\mathrm{V}_1 \cup \mathrm{V}_2, \mathrm{X}_1 \cup \mathrm{X}_2)) & , \\ & \exists \epsilon_1, \epsilon_2 . ({}_{B_1^A} \odot_{B_2^A} (\epsilon, \epsilon_1, \epsilon_2) \wedge (\mathrm{I}_1 \wedge \Box \mathrm{T}_1 \wedge \mathrm{L}_1)\,[\epsilon_1/\epsilon] \wedge (\mathrm{I}_2 \wedge \Box \mathrm{T}_2 \wedge \mathrm{L}_2)\,[\epsilon_2/\epsilon]) &) \end{array}$$

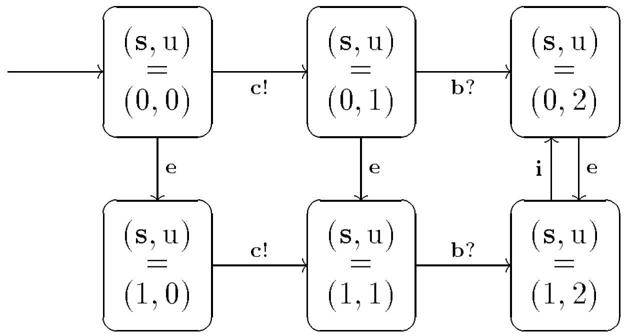

Figure 2.6: Concrete machine 2

where

$$
\begin{array}{lcl}
\mathrm{In}_1 \setminus \mathrm{Out}_2 \cup \mathrm{In}_2 \setminus \mathrm{Out}_1 & = & \{\mathbf{a}\} \\
\mathrm{Out}_1 \setminus \mathrm{In}_2 \cup \mathrm{Out}_2 \setminus \mathrm{In}_1 & = & \{\mathbf{b}\} \\
\mathrm{V}_1 \cup \mathrm{V}_2 & = & \{\mathrm{s}\} \\
\mathrm{X}_1 \cup \mathrm{X}_2 & = & \{\mathrm{t}, \mathrm{u}\} \\
\mathrm{I}_1\,[\epsilon_1/\epsilon] \wedge \mathrm{I}_2\,[\epsilon_2/\epsilon] & = & (\mathrm{s}, \mathrm{t}, \mathrm{u}) = (0, 0, 0) \\
\mathrm{T}_1\,[\epsilon_1/\epsilon] \wedge \mathrm{T}_2\,[\epsilon_2/\epsilon] & = & \Big[\vee \Big(\epsilon_1 = \mathbf{a}! \wedge \mathrm{t} = 0 \wedge (\mathrm{s}, \mathrm{t})' = (\mathrm{s}, 1)\Big) \\
& & \ \vee \Big(\epsilon_1 = \mathbf{c}? \wedge \mathrm{t} = 1 \wedge (\mathrm{s}, \mathrm{t})' = (\mathrm{s}, 2)\Big) \\
& & \ \vee \Big(\epsilon_1 = \mathbf{e} \wedge (\mathrm{s}, \mathrm{t})' = (1, \mathrm{t})\Big) \\
& & \ \vee \Big(\epsilon_1 = \mathbf{e} \wedge (\mathrm{s}, \mathrm{t})' = (0, \mathrm{t})\Big) \\
& & \ \vee \mathbf{stut}_1\,[\epsilon_1/\epsilon]\Big] \\
& & \wedge \\
& & \Big[\vee \Big(\epsilon_2 = \mathbf{c}! \wedge \mathrm{u} = 0 \wedge (\mathrm{s}, \mathrm{u})' = (\mathrm{s}, 1)\Big) \\
& & \ \vee \Big(\epsilon_2 = \mathbf{b}? \wedge \mathrm{u} = 1 \wedge (\mathrm{s}, \mathrm{u})' = (\mathrm{s}, 2)\Big) \\
& & \ \vee \Big(\epsilon_2 = \mathbf{i} \wedge (\mathrm{s}, \mathrm{u}) = (1, 2) \wedge (\mathrm{s}, \mathrm{u})' = (0, \mathrm{u})\Big) \\
& & \ \vee \Big(\epsilon_2 = \mathbf{e} \wedge (\mathrm{s}, \mathrm{u})' = (1, \mathrm{u})\Big) \\
& & \ \vee \mathbf{stut}_2\,[\epsilon_2/\epsilon]\Big] \\
\mathrm{L}_1\,[\epsilon_1/\epsilon] \wedge \mathrm{L}_2\,[\epsilon_2/\epsilon] & = & \mathbf{true}
\end{array}
$$

Let $\mathrm{H}_c \triangleq \exists \epsilon_1, \epsilon_2 . ({}_{B_1^A} \odot_{B_2^A} (\epsilon, \epsilon_1, \epsilon_2) \wedge (\mathrm{I}_1 \wedge \Box \mathrm{T}_1 \wedge \mathrm{L}_1)\,[\epsilon_1/\epsilon] \wedge (\mathrm{I}_2 \wedge \Box \mathrm{T}_2 \wedge \mathrm{L}_2)\,[\epsilon_2/\epsilon])$ *and* $\mathrm{H}_a \triangleq \mathrm{I} \wedge \Box \mathrm{T} \wedge \mathrm{L}$, *then the composition of* $\mathcal{S}_{c_1}$ *and* $\mathcal{S}_{c_2}$ *refines* $\mathcal{S}_a$ *iff*

(1) $\mathfrak{O}(B_c) = \mathfrak{O}(B)$
(2) $\models (\exists \mathrm{t}, \mathrm{u} \,.\, (\mathrm{H}_c)) \rightarrow (\exists \mathrm{x} \,.\, (\mathrm{H}_a))$

The following section will show that both conditions hold. Hence we have refinement.

2.4 Proving Refinement of Reactive System Specifications

This section explains how refinement of reactive systems can be proved. The standard technique of Abadi & Lamport [AL91] is used, i.e., refinement is proven by providing a refinement mapping from the concrete system to the abstract system. Firstly we give its definition at the semantic level and then for DTL specifications.

2.4.1 Proving Semantic Refinement of Specifications

Refinement of reactive systems is proved by means of a *refinement mapping* from the concrete system to the abstract system. A refinement mapping maps a history at the concrete level to a history at the abstract level, more specifically, it maps the states appearing in the concrete history to states appearing in the abstract history.

Definition 37 (Refinement mapping between systems)
Given concrete system $\mathcal{S}_c \triangleq (B_c, H_c)$ *and abstract system* $\mathcal{S}_a \triangleq (B_a, H_a)$ *s.t.* $\mathfrak{O}(B_c) = \mathfrak{O}(B_a)$. *A* **refinement mapping** *from* $\mathcal{S}_c$ *to* $\mathcal{S}_a$ *is a mapping* f *from states appearing in histories of* H_c *to states appearing in histories of* H_a*, i.e.,* f *is mapping from with* $f : \Sigma \rightarrow \Sigma$ *s.t.*

- *The values of observable variables are not changed, i.e., for all* $\sigma \in \Sigma$*:* $\sigma|^1_{\mathrm{V}_c} = f(\sigma)|^1_{\mathrm{V}_c}$.
- *For all* $h_c \in H_c$ *there exists a* $h_a \in H_a$ *s.t. for all* $t \in \mathbb{R}^{\geq 0}$, $\psi_c(t) = \psi_a(t)$ *and* $\theta_a(t) = f(\theta_c(t))$.

Lemma 7
Given concrete system $\mathcal{S}_c \triangleq (B_c, H_c)$ *and abstract system* $\mathcal{S}_a \triangleq (B_a, H_a)$ *s.t.* $\mathfrak{O}(B_c) = \mathfrak{O}(B_a)$. *If there exists a refinement mapping from* $\mathcal{S}_c$ *to* $\mathcal{S}_a$*, then* $\mathcal{S}_c$ **ref** $\mathcal{S}_a$.

The concept of refinement mappings can also be applied to machine specifications. A machine specification is of the form $(B, Comp(M) \cap L)$. Refinement means then that $f(Comp(M_c) \cap L_c) \subseteq Comp(M_a) \cap L_a$ for refinement mapping f. This can be split into (1) $f(Comp(M_c) \cap L_c) \subseteq Comp(M_a)$ and (2) $f(Comp(M_c) \cap L_c) \subseteq L_a$. From $f(Comp(M_c)) \subseteq Comp(M_a)$ follows (1) because $f(Comp(M_c) \cap L_c) \subseteq f(Comp(M_c))$. So the verification condition can be split into a condition on machines and a condition involving machines together with supplementary conditions. This leads to the following definition.

Definition 38 (Refinement mapping between machine specifications)
Given concrete machine specification $\mathcal{S}_c \triangleq (B_c, Comp(M_c) \cap L_c)$*, where* $M_c \triangleq (B_c, I_c, T_c)$*, and abstract machine specification* $\mathcal{S}_a \triangleq (B_a, Comp(M_a) \cap L_a)$*, where* $M_a \triangleq (B_a, I_a, T_a)$. *A* **refinement mapping** *from machine specification* $\mathcal{S}_c$ *to machine specification* $\mathcal{S}_a$ *is a mapping* $f : \Sigma \rightarrow \Sigma$ *s.t.*

- *For all* $\sigma \in \Sigma$, $\sigma|^1_{\mathrm{V}_c} = f(\sigma)|^1_{\mathrm{V}_c}$.
-
  - *For all* $\sigma_c \in I_c$*, there exist* $\sigma_a \in I_a$ *s.t.* $\sigma_a = f(\sigma_c)$.

– *For all* $\langle d, \sigma_{c1}, \sigma_{c2}\rangle \in T_c$, $\langle d, f(\sigma_{c1}), f(\sigma_{c2})\rangle \in T_a$ *or* $(f(\sigma_{c1}) = f(\sigma_{c2}) \wedge d(\epsilon) \in \{\lambda, \mathbf{i}, \mathbf{e}\}$.

– *For all* $h_c \in Comp(M_c) \cap L_c$ *there exist a* $h_a \in L_a$ *s.t. for all* $t \in \mathbb{R}^{\geq 0}$, $\psi_c(t) = \psi_a(t)$ *and* $f(\theta_c(t)) = \theta_a(t)$.

The following lemma expresses that refinement mappings are indeed sound for proving refinement of machine specifications.

Lemma 8
Given concrete machine specification $\mathcal{S}_c \triangleq (B_c, Comp(M_c) \cap L_c)$ *and abstract machine specification* $\mathcal{S}_a \triangleq (B_a, Comp(M_a) \cap L_a)$ *s.t.* $\mathfrak{O}(B_c) = \mathfrak{O}(B_a)$. *If there exists a refinement mapping from* $\mathcal{S}_c$ *to* $\mathcal{S}_a$ *then* $\mathcal{S}_c$ **ref** $\mathcal{S}_a$.

2.4.2 Proving Refinement of DTL Specifications

Proving refinement of machine specifications in DTL means according to Theorem 4 that the observable bases are equal and that a formula with two existential quantifications is valid. More specifically:
Given concrete machine specification $\mathcal{S}_c \triangleq (B_c, \mathrm{I}_c \wedge \Box \mathrm{T}_c \wedge \mathrm{L}_c)$ and abstract machine specification $\mathcal{S}_a \triangleq (B_a, \mathrm{I}_a \wedge \Box \mathrm{T}_a \wedge \mathrm{L}_a)$. Then $\mathcal{S}_c$ **refines** $\mathcal{S}_a$ is denoted $\mathcal{S}_c$ **ref** $\mathcal{S}_a$ and defined by

$\mathfrak{O}(B_c) = \mathfrak{O}(B_a)$ and
$(\exists \mathrm{X}_c\,.\,(\mathrm{I}_c \wedge \Box \mathrm{T}_c \wedge \mathrm{L}_c)) \;\rightarrow (\exists \mathrm{X}_a\,.\,(\mathrm{I}_a \wedge \Box \mathrm{T}_a \wedge \mathrm{L}_a))$

So we must have a rule to prove the following:

$$\exists \mathrm{x}_0.p_0 \rightarrow \exists \mathrm{x}_1.p_1$$

The following rule does the job:

$$\frac{p_0 \rightarrow p_1\,[exp/\mathrm{x}_1]}{\exists \mathrm{x}_0.p_0 \rightarrow \exists \mathrm{x}_1.p_1} \quad \begin{array}{l}\text{for } \mathrm{x}_0 \text{ not free in } p_1 \\ \text{none of the variables appearing in } exp \text{ is quantified in } p_1\end{array}$$

as the following derivation shows:

$$\begin{array}{ll}
 & p_0 \rightarrow p_1\,[exp/\mathrm{x}_1] \\
\rightarrow & \quad \%\ \textit{Generalization, prop.calc.} \\
 & p_0 \Rightarrow p_1\,[exp/\mathrm{x}_1] \\
\rightarrow & \quad \%\ \textit{contraposition} \\
 & \neg p_1\,[exp/\mathrm{x}_1] \Rightarrow \neg p_0 \\
\rightarrow & \quad \%\ \ Ax11 : \forall \mathrm{x}_1.\neg p_1 \Rightarrow \neg p_1\,[exp/\mathrm{x}_1] \text{ where none of the variables} \\
 & \qquad\quad \text{appearing in } exp \text{ is quantified in } \neg p_1, \text{Modus Ponus} \\
 & \forall \mathrm{x}_1.\neg p_1 \Rightarrow \neg p_0 \\
\rightarrow & \quad \%\ \text{Rule } (q_0 \Rightarrow q_1) \rightarrow q_0 \Rightarrow \forall \mathrm{x}_0.q_1, \text{ for } \mathrm{x}_0 \text{ not free in } q_0 \\
 & \forall \mathrm{x}_1.\neg p_1 \Rightarrow \forall \mathrm{x}_0.\neg p_0 \\
\rightarrow & \quad \%\ \Box p \rightarrow p, \text{Modus Ponus} \\
 & \forall \mathrm{x}_1.\neg p_1 \rightarrow \forall \mathrm{x}_0.\neg p_0 \\
= & \quad \%\ \textit{contraposition} \\
 & \exists \mathrm{x}_0.p_0 \rightarrow \exists \mathrm{x}_1.p_1
\end{array}$$

From the previous section it should be clear that this exp is exactly the refinement mapping f, and that the proof can be split in a safety part and a liveness part (i.e., the proof of $p_0 \rightarrow p_1 [exp/\mathrm{x}_1]$ of above rule is split into a safety and a liveness part). This culminates in the following proof rule for refinement based on similar ones in [Lam91, KMP93].

Rule 1 (Proof rule for refinement)
Given concrete machine specification $\mathcal{S}_c \triangleq (B_c, \mathrm{I}_c \wedge \Box\mathrm{T}_c \wedge \mathrm{L}_c)$ *and abstract machine specification* $\mathcal{S}_a \triangleq (B_a, \mathrm{I}_a \wedge \Box\mathrm{T}_a \wedge \mathrm{L}_a)$ *s.t.* $\mathfrak{O}(B_c) = \mathfrak{O}(B_a)$. *Let* f *be a refinement mapping from* $\mathcal{S}_c$ *to* $\mathcal{S}_a$ *then*

$$\frac{\begin{array}{l}\mathcal{S}_c \models \mathrm{I}_c \rightarrow \mathrm{I}_a [f/\mathrm{X}_a] \\ \mathcal{S}_c \models \mathrm{T}_c \rightarrow \mathrm{T}_a [f/\mathrm{X}_a] \\ \mathcal{S}_c \models \mathrm{L}_a [f/\mathrm{X}_a]\end{array}}{\models (\exists \mathrm{X}_c \,.\, (\mathrm{I}_c \wedge \Box\mathrm{T}_c \wedge \mathrm{L}_c)) \rightarrow (\exists \mathrm{X}_a \,.\, (\mathrm{I}_a \wedge \Box\mathrm{T}_a \wedge \mathrm{L}_a))}$$

When L_a is of the form

$$\bigwedge_{\tau \in \mathrm{WF}_a} (\Diamond\Box En(\tau) \rightarrow \Box\Diamond\tau) \wedge \bigwedge_{\tau \in \mathrm{SF}_a} (\Box\Diamond En(\tau) \rightarrow \Box\Diamond\tau)$$

(see Def. 29), the last premise of above rule can be split into

$$\begin{array}{l}\mathcal{S}_c \models \bigwedge_{\tau \in \mathrm{WF}_a} (\Diamond\Box En(\tau) \rightarrow \Box\Diamond\tau) [f/\mathrm{X}_a] \\ \mathcal{S}_c \models \bigwedge_{\tau \in \mathrm{SF}_a} (\Box\Diamond En(\tau) \rightarrow \Box\Diamond\tau) [f/\mathrm{X}_a] \,.\end{array}$$

This is equal to

$$\begin{array}{l}\mathcal{S}_c \models \bigwedge_{\tau \in \mathrm{WF}_a} (En(\tau) \Rightarrow \Diamond(En(\tau) \rightarrow \tau)) [f/\mathrm{X}_a] \\ \mathcal{S}_c \models \bigwedge_{\tau \in \mathrm{SF}_a} (\Box\Diamond En(\tau) \Rightarrow \Diamond\tau) [f/\mathrm{X}_a]\end{array}$$

using some temporal logic calculus. So one gets the following proof rule, similar rules appearing in [Lam91, KMP93].

Rule 2 (Proof rule for refinement)
Given concrete machine specification $\mathcal{S}_c \triangleq (B_c, \mathrm{I}_c \wedge \Box\mathrm{T}_c \wedge \mathrm{L}_c)$ *where* L_c *is of the form* $\bigwedge_{\tau \in \mathrm{WF}_c} (\Diamond\Box En(\tau) \rightarrow \Box\Diamond\tau) \wedge \bigwedge_{\tau \in \mathrm{SF}_c} (\Box\Diamond En(\tau) \rightarrow \Box\Diamond\tau)$. *Furthermore given abstract machine specification* $\mathcal{S}_a \triangleq (B_a, \mathrm{I}_a \wedge \Box\mathrm{T}_a \wedge \mathrm{L}_a)$ *where* L_a *is of the form* $\bigwedge_{\tau \in \mathrm{WF}_a} (\Diamond\Box En(\tau) \rightarrow \Box\Diamond\tau) \wedge \bigwedge_{\tau \in \mathrm{SF}_a} (\Box\Diamond En(\tau) \rightarrow \Box\Diamond\tau)$. *Let* $\mathfrak{O}(B_c) = \mathfrak{O}(B_a)$. *Let* f *be a refinement mapping from* $\mathcal{S}_c$ *to* $\mathcal{S}_a$ *then*

$$\frac{\begin{array}{l}\mathcal{S}_c \models \mathrm{I}_c \rightarrow \mathrm{I}_a [f/\mathrm{X}_a] \\ \mathcal{S}_c \models \mathrm{T}_c \rightarrow \mathrm{T}_a [f/\mathrm{X}_a] \\ \mathcal{S}_c \models \bigwedge_{\tau \in \mathrm{WF}_a} En(\tau) [f/\mathrm{X}_a] \Rightarrow \Diamond(En(\tau) [f/\mathrm{X}_a] \rightarrow \tau [f/\mathrm{X}_a]) \\ \mathcal{S}_c \models \bigwedge_{\tau \in \mathrm{SF}_a} \Box\Diamond En(\tau) [f/\mathrm{X}_a] \Rightarrow \Diamond\tau [f/\mathrm{X}_a]\end{array}}{\models (\exists \mathrm{X}_c \,.\, (\mathrm{I}_c \wedge \Box\mathrm{T}_c \wedge \mathrm{L}_c)) \rightarrow (\exists \mathrm{X}_a \,.\, (\mathrm{I}_a \wedge \Box\mathrm{T}_a \wedge \mathrm{L}_a))}$$

Rule 1 is used in the following example for proving refinement of example 4.

Example 5

From example 4 we have:

Let $\mathrm{H}_c \triangleq \exists \epsilon_1, \epsilon_2 . ({}_{B_1^A} \odot_{B_2^A} (\epsilon, \epsilon_1, \epsilon_2) \wedge (\mathrm{I}_1 \wedge \Box \mathrm{T}_1 \wedge \mathrm{L}_1)[\epsilon_1/\epsilon] \wedge (\mathrm{I}_2 \wedge \Box \mathrm{T}_2 \wedge \mathrm{L}_2)[\epsilon_2/\epsilon])$ *and* $\mathrm{H}_a \triangleq \mathrm{I} \wedge \Box \mathrm{T} \wedge \mathrm{L}$ *then the composition of* $\mathcal{S}_{c_1}$ *and* $\mathcal{S}_{c_2}$ *refines* $\mathcal{S}_a$ *iff*

(1) $\mathfrak{O}(B_c) = \mathfrak{O}(B)$
(2) $\models (\exists \mathrm{t}, \mathrm{u} . (\mathrm{H}_c)) \rightarrow (\exists \mathrm{x} . (\mathrm{H}_a))$

Because the observable bases are equal (1) holds. (2) is proven with rule 1. This means one has to find a refinement mapping f. *In order to find such a mapping the picture of the* $\mathcal{S}_{c1} \| \mathcal{S}_{c2}$ *is given. (Note only the reachable states are drawn):*

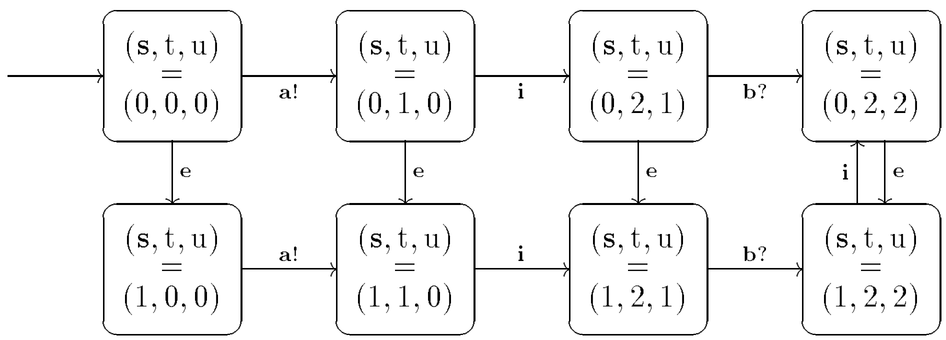

Figure 2.7: Transitions of $\mathcal{S}_{c1} \| \mathcal{S}_{c2}$

Relating the above figure with figure 2.4 one sees that f *is as defined follows:*

$$
\begin{array}{lll}
if & & \\
\quad \mathrm{t} = 0 \wedge \mathrm{u} = 0 & then & f(s,t,u) = \mathrm{t} \\
\quad \mathrm{t} = 1 \wedge \mathrm{u} = 0 & then & f(s,t,u) = \mathrm{t} \\
\quad \mathrm{t} = 2 \wedge \mathrm{u} = 1 & then & f(s,t,u) = \mathrm{t} - \mathrm{u} \\
\quad \mathrm{t} = 2 \wedge \mathrm{u} = 2 & then & f(s,t,u) = \mathrm{u} \\
fi & &
\end{array}
$$

The following premises should be valid in order to apply the rule:

- $\mathcal{S}_c \models (\mathrm{s}, \mathrm{t}, \mathrm{u}) = (0, 0, 0) \rightarrow ((\mathrm{s}, \mathrm{x}) = (0, 0))[f/\mathrm{x}]$

  Substitution means replacing x *by* t *because* $\mathrm{t} = 0 \wedge \mathrm{u} = 0$. *This results in:*

  $$(\mathrm{s}, \mathrm{t}, \mathrm{u}) = (0, 0, 0) \rightarrow (\mathrm{s}, \mathrm{t}) = (0, 0)$$

  This is valid.

- $\mathcal{S}_c \models \big(\epsilon = \mathbf{a!} \wedge \mathrm{t} = 0 \wedge (\mathrm{s}, \mathrm{t}, \mathrm{u})' = (\mathrm{s}, 1, \mathrm{u})\big)$
  $\rightarrow$
  $\big(\epsilon = \mathbf{a!} \wedge \mathrm{x} = 0 \wedge (\mathrm{s}, \mathrm{x})' = (\mathrm{s}, 1)\big)[f/\mathrm{x}]$

Substitution means replacing x *by* t *because* $\mathrm{t} = 0$*, and replacing* x′ *by* t′ *because* $\mathrm{t}' = 1$*. This results in:*

$$\begin{array}{l} \mathcal{S}_c \models \big(\epsilon = \mathbf{a}! \wedge \mathrm{t} = 0 \wedge (\mathbf{s}, \mathrm{t}, \mathrm{u})' = (\mathbf{s}, 1, \mathrm{u})\big) \\ \rightarrow \\ \big(\epsilon = \mathbf{a}! \wedge \mathrm{t} = 0 \wedge (\mathbf{s}, \mathrm{t})' = (\mathbf{s}, 1)\big) \end{array}$$

This is valid.

- $$\begin{array}{l} \mathcal{S}_c \models \big(\epsilon = \mathbf{b}? \wedge \mathrm{u} = 1 \wedge (\mathbf{s}, \mathrm{t}, \mathrm{u})' = (\mathbf{s}, \mathrm{t}, 2)\big) \\ \rightarrow \\ \big(\epsilon = \mathbf{b}? \wedge \mathrm{x} = 1 \wedge (\mathbf{s}, \mathrm{x})' = (\mathbf{s}, 2)\big)\,[f/\mathrm{x}] \end{array}$$

  Substitution means replacing x *by* $\mathrm{t} - \mathrm{u}$ *because* $\mathrm{u} = 1$*, and replacing* x′ *by* u′ *because* $\mathrm{u}' = 2$*. This results in:*

  $$\begin{array}{l} \mathcal{S}_c \models \big(\epsilon = \mathbf{b}? \wedge \mathrm{u} = 1 \wedge (\mathbf{s}, \mathrm{t}, \mathrm{u})' = (\mathbf{s}, \mathrm{t}, 2)\big) \\ \rightarrow \\ \big(\epsilon = \mathbf{b}? \wedge \mathrm{t} - \mathrm{u} = 0 \wedge (\mathbf{s}, \mathrm{u})' = (\mathbf{s}, 2)\big) \end{array}$$

  This is valid because from figure 2.7 one sees that $\mathrm{u} = 1 \Rightarrow \mathrm{t} = 2$ *holds.*

- $$\begin{array}{l} \mathcal{S}_c \models \big(\epsilon = \mathbf{e} \wedge (\mathbf{s}, \mathrm{t}, \mathrm{u})' = (1, \mathrm{t}, \mathrm{u})\big) \\ \rightarrow \\ \big(\epsilon = \mathbf{e} \wedge (\mathbf{s}, \mathrm{x})' = (1, \mathrm{x})\big)\,[f/\mathrm{x}] \end{array}$$

  Substitution means replacing x *by* f*, and replacing* x′ *by* f′*. This results in:*

  $$\begin{array}{l} \mathcal{S}_c \models \big(\epsilon = \mathbf{e} \wedge (\mathbf{s}, \mathrm{t}, \mathrm{u})' = (1, \mathrm{t}, \mathrm{u})\big) \\ \rightarrow \\ \big(\epsilon = \mathbf{e} \wedge (\mathbf{s}, f)' = (\mathbf{s}, f)\big) \end{array}$$

  This is valid because $(\mathrm{t}, \mathrm{u})' = (\mathrm{t}, \mathrm{u}) \Rightarrow f' = f$.

- $$\begin{array}{l} \mathcal{S}_c \models \big(\epsilon = \mathbf{i} \wedge (\mathrm{t}, \mathrm{u}) = (1, 0) \wedge (\mathbf{s}, \mathrm{t}, \mathrm{u})' = (\mathbf{s}, 2, 1)\big) \\ \rightarrow \\ \mathbf{stut}_a\,[f/\mathrm{x}] \end{array}$$

  Because $\mathbf{stut}_a \triangleq$

  $$\begin{array}{ll} & \epsilon = \lambda \\ \vee & \big(\epsilon = \mathbf{i} \wedge (\mathbf{s}, \mathrm{x})' = (\mathbf{s}, \mathrm{x})\big) \\ \vee & \big(\epsilon = \mathbf{e} \wedge (\mathbf{s}, \mathrm{x})' = (\mathbf{s}, \mathrm{x})\big) \end{array}$$

it suffices to prove:

$$\mathcal{S}_c \models \Big(\epsilon = \mathbf{i} \wedge (\mathrm{t}, \mathrm{u}) = (1, 0) \wedge (\mathbf{s}, \mathrm{t}, \mathrm{u})' = (\mathbf{s}, 2, 1)\Big) \\ \rightarrow \\ \Big(\epsilon = \mathbf{i} \wedge (\mathbf{s}, \mathrm{x})' = (\mathbf{s}, \mathrm{x})\Big)\,[f/\mathrm{x}]$$

Substitution means replacing x *by* t *because* $\mathrm{t} = 1 \wedge \mathrm{u} = 0$*, and replacing* x′ *by* $\mathrm{t}' - \mathrm{u}'$ *because* $\mathrm{t}' = 2 \wedge \mathrm{u}' = 1$*. This results in:*

$$\mathcal{S}_c \models \Big(\epsilon = \mathbf{i} \wedge (\mathrm{t}, \mathrm{u}) = (1, 0) \wedge (\mathbf{s}, \mathrm{t}, \mathrm{u})' = (\mathbf{s}, 2, 1)\Big) \\ \rightarrow \\ \Big(\epsilon = \mathbf{i} \wedge (\mathbf{s}, \mathrm{t} - \mathrm{u})' = (\mathbf{s}, \mathrm{t})\Big)$$

This is valid.

- $$\mathcal{S}_c \models \Big(\epsilon = \mathbf{i} \wedge (\mathbf{s}, \mathrm{u}) = (1, 2) \wedge (\mathbf{s}, \mathrm{t}, \mathrm{u})' = (0, \mathrm{t}, \mathrm{u})\Big) \\ \rightarrow \\ \Big(\epsilon = \mathbf{i} \wedge (\mathbf{s}, \mathrm{x}) = (1, 2) \wedge (\mathbf{s}, \mathrm{x})' = (0, \mathrm{x})\Big)\,[f/\mathrm{x}]$$

  Substitution means replacing x *by* u *because* $\mathrm{u} = 2 \wedge \mathrm{t} = 2$*, and replacing* x′ *by* u′ *because* $\mathrm{u}' = 2 \wedge \mathrm{t}' = 2$*. This results in:*

  $$\mathcal{S}_c \models \Big(\epsilon = \mathbf{i} \wedge (\mathbf{s}, \mathrm{u}) = (1, 2) \wedge (\mathbf{s}, \mathrm{t}, \mathrm{u})' = (0, \mathrm{t}, \mathrm{u})\Big) \\ \rightarrow \\ \Big(\epsilon = \mathbf{i} \wedge (\mathbf{s}, \mathrm{u}) = (1, 2) \wedge (\mathbf{s}, \mathrm{u})' = (\mathbf{s}, \mathrm{u})\Big)$$

  This is valid.

- $\mathcal{S}_c \models \mathbf{stut}_c \rightarrow \mathbf{stut}_a\,[f/\mathrm{x}]$

  Definition of $\mathbf{stut}_a$ *and* $\mathbf{stut}_c$ *results in*

  $$\begin{aligned} \mathcal{S}_c \models \quad & \epsilon = \lambda \\ & \vee \Big(\epsilon = \mathbf{i} \wedge (\mathbf{s}, \mathrm{t}, \mathrm{u})' = (\mathbf{s}, \mathrm{t}, \mathrm{u})\Big) \\ & \vee \Big(\epsilon = \mathbf{e} \wedge (\mathbf{s}, \mathrm{t}, \mathrm{u})' = (\mathbf{s}, \mathrm{t}, \mathrm{u})\Big) \\ & \rightarrow \\ & \epsilon = \lambda \\ & \vee \Big(\epsilon = \mathbf{i} \wedge (\mathbf{s}, \mathrm{x})' = (\mathbf{s}, \mathrm{x})\Big)\,[f/\mathrm{x}] \\ & \vee \Big(\epsilon = \mathbf{e} \wedge (\mathbf{s}, \mathrm{x})' = (\mathbf{s}, \mathrm{x})\Big)\,[f/\mathrm{x}] \end{aligned}$$

  This is valid.

- $\mathcal{S}_c \models \mathbf{true}\,[f/\mathrm{x}]$

  This is valid.

So $\mathcal{S}_{c1} \| \mathcal{S}_{c2}$ **ref** $\mathcal{S}_a$.

2.5 Relative Refinement and Composition of Reactive System Specifications

In this section the concept of *relative* refinement and composition in the development of systems is explained. Ordinary refinement stipulates that the set of histories generated by the concrete system is included in the set of histories generated by the abstract system. Relative refinement means that this inclusion almost holds, i.e., if one leaves some of the histories generated at the concrete level out of account this inclusion holds. Histories generated by the abstract system can also be left out because a concrete system could be an abstract system in a next refinement step. Ordinary composition means that the histories of two components are merged into the histories of the composed system. Relative composition means that one leaves certain histories out of this merge, i.e., the merge is performed on smaller sets of histories generated by the components. In the first two subsections we consider the sets that extract the good computations as arbitrary, i.e., it can be a safety set, liveness set or neither of them. In the third subsection a condition similar to machine closedness is imposed on a relative system, i.e., the relative system can then be split into a safety part and a liveness part. Using this fact a proof rule for relative refinement is constructed in the last subsection based on rule given in Section 2.4. Again we formulate these concepts first in terms of sets of histories and then in DTL.

2.5.1 Semantic Relative Refinement and Composition of Specifications

Definition 39 (Relative refinement of systems)
Given concrete system $\mathcal{S}_c \triangleq (B_c, H_c)$ and aset W_c of allowed histories for $\mathcal{S}_c$ ($W_c \subseteq \mathcal{H}$ constraining B_c) and abstract system $\mathcal{S}_a \triangleq (B_a, H_a)$ together with a set W_a of allowed histories for $\mathcal{S}_a$ ($W_a \subseteq \mathcal{H}$ constraining B_a). Let $G_c \triangleq H_c \cap W_c$ and $G_a \triangleq H_a \cap W_a$. Then $\mathcal{S}_c$ **relatively refines** *$\mathcal{S}_a$ with respect to (W_c, W_a), denoted by $\mathcal{S}_c\ {}_{W_c}\mathbf{ref}^{W_a}\ \mathcal{S}_a$, iff $\mathfrak{O}(B_c) = \mathfrak{O}(B_a)$ and $\mathcal{O}_{\mathrm{X}_c}(G_c) \subseteq \mathcal{O}_{\mathrm{X}_a}(G_a)$.*

Relativizing can also be used for composition, i.e., if during composition one gets unwanted histories these are removed, using a set that characterizes the allowed histories.

Definition 40 (Relative composition of two systems)
Given systems $\mathcal{S}_i = (B_i, H_i)$ where $B_i = ((\mathrm{In}_i, \mathrm{Out}_i), (\mathrm{V}_i, \mathrm{X}_i))$ and ($i = 1, 2$) such that $\mathrm{X}_1 \cap \mathrm{X}_2 = \emptyset$ and given sets $W_i \subseteq \mathcal{H}$ constraining B_i. Let $\overline{W}$ denote (W_1, W_2). Then the **relative composed system** *$\mathcal{S}$ with respect to $\overline{W}$, denoted $\mathcal{S}_1 \,|_{\overline{W}}|\, \mathcal{S}_2$, is defined as (B, H) with $B \triangleq ((\mathrm{In}_1 \setminus \mathrm{Out}_2 \cup \mathrm{In}_2 \setminus \mathrm{Out}_1, \mathrm{Out}_1 \setminus \mathrm{In}_2 \cup \mathrm{Out}_2 \setminus \mathrm{In}_1), (\mathrm{V}_1 \cup \mathrm{V}_2, \mathrm{X}_1 \cup \mathrm{X}_2))$, and $H \triangleq H_1 \overline{W} H_2 \triangleq (H_1 \cap W_1) \otimes (H_2 \cap W_2)$.*

The following is a compositional relative refinement theorem.

Theorem 7 (Compositional relative refinement)
Given concrete systems $\mathcal{S}_i = (B_i, H_i)$ ($i = 1, 2$) and given set W_c constraining B_{12} (the

basis of $\mathcal{S}_1 \parallel \mathcal{S}_2$). And given abstract systems $\mathcal{S}_j = (B_j, H_j)$ ($j = 3, 4$) and given set W_a constraining B_{34} (the basis of $\mathcal{S}_3 \parallel \mathcal{S}_4$). Then the following holds:

$$\begin{array}{ll} (H_1 \otimes H_2) \cap (W_{c1} \otimes W_{c2}) \subseteq (H_1 \cap W_{c1}) \bigotimes (H_2 \cap W_{c2}) & \\ W_c \subseteq W_{c1} \otimes W_{c2} & \\ W_{a3} \otimes W_{a4} \subseteq W_a & W_{ci} \text{ constraining } B_i \ (i{=}1{,}2) \\ \mathcal{S}_1 \ {}_{W_{c1}}\mathbf{ref}^{\,W_{a3}} \ \mathcal{S}_3 & W_{aj} \text{ constraining } B_j \ (j{=}3{,}4) \\ \mathcal{S}_2 \ {}_{W_{c2}}\mathbf{ref}^{\,W_{a4}} \ \mathcal{S}_4 & \\ \hline \mathcal{S}_1 \parallel \mathcal{S}_2 \ {}_{W_c}\mathbf{ref}^{\,W_a} \ \mathcal{S}_3 \parallel \mathcal{S}_4 & \end{array}$$

If the extra requirements W don't constrain the ϵ-variables then the following lemma can be used to prove the first premise of above theorem.

Lemma 9
Given systems $\mathcal{S}_i = (B_i, H_i)$ and sets W_i constraining B_i ($i = 1, 2$) with no restrictions on the event variables. Then the following holds:

$$(H_1 \cap W_1) \bigotimes (H_2 \cap W_2) = H_1 \bigotimes H_2 \cap W_1 \bigotimes W_2$$

In case the abstract requirement W_a can't be decomposed into component requirements the following rule can be used.

Lemma 10
Given concrete systems $\mathcal{S}_i = (B_i, H_i)$ ($i = 1, 2$) and given set W_c constraining B_{12}. And given abstract systems $\mathcal{S}_j = (B_j, H_j)$ ($j = 3, 4$) and given set W_a constraining B_{34} without restricting the ϵ variables. Then the following holds:

$$\begin{array}{ll} H_1 \otimes H_2 \cap W_{c1} \otimes W_{c2} \subseteq (H_1 \cap W_{c1}) \bigotimes (H_2 \cap W_{c2}) & \\ W_c \subseteq W_{c1} \otimes W_{c2} & \\ \mathcal{S}_1 \ {}_{W_{c1}}\mathbf{ref}^{\,W_a} \ \mathcal{S}_3 & W_{ci} \text{ constraining } B_i \ (i{=}1{,}2) \\ \mathcal{S}_2 \ {}_{W_{c2}}\mathbf{ref}^{\,W_a} \ \mathcal{S}_4 & \\ \hline \mathcal{S}_1 \parallel \mathcal{S}_2 \ {}_{W_c}\mathbf{ref}^{\,W_a} \ \mathcal{S}_3 \parallel \mathcal{S}_4 & \end{array}$$

The following lemma is useful for proving the second premise of the theorem.

Lemma 11
Given sets W_i ($i = 1, 2$) not restricting the ϵ variables then

$$W_1 \bigotimes W_2 = W_1 \cap W_2.$$

2.5.2 Relative Refinement and Composition of DTL Specifications

Theorem 8 (Relative refinement of DTL machine specifications)
Given concrete machine specification $\mathcal{S}_c \triangleq (B_c, \mathrm{I}_c \wedge \Box \mathrm{T}_c \wedge \mathrm{L}_c)$ and DTL formula W_c over B_c and abstract machine specification $\mathcal{S}_a \triangleq (B_a, \mathrm{I}_a \wedge \Box \mathrm{T}_a \wedge \mathrm{L}_a)$ and DTL formula W_a over B_a. Let $\mathrm{G}_c \triangleq \mathrm{I}_c \wedge \Box \mathrm{T}_c \wedge \mathrm{L}_c \wedge \mathrm{W}_c$ and $\mathrm{G}_a \triangleq \mathrm{I}_a \wedge \Box \mathrm{T}_a \wedge \mathrm{L}_a \wedge \mathrm{W}_a$. Then $\mathcal{S}_c \ {}_{Hist(\mathrm{W}_c)}\mathbf{ref}^{\,Hist(\mathrm{W}_a)} \ \mathcal{S}_a$ iff

$$\mathfrak{D}(B_c) = \mathfrak{D}(B_a) \text{ and}$$
$$\models (\exists \mathrm{X}_c \,.\, (\mathrm{G}_c)) \rightarrow (\exists \mathrm{X}_a \,.\, (\mathrm{G}_a))$$

Definition 41 (Relative composition of two DTL machine specifications)
Given machine system specifications $(B_i, \mathrm{I}_i \wedge \Box\mathrm{T}_i \wedge \mathrm{L}_i)$ *where* $B_i \triangleq ((\mathrm{In}_i, \mathrm{Out}_i), (\mathrm{V}_i, \mathrm{X}_i))$, *and given DTL formulae* W_i *over* B_i *for* $i = 1, 2$. *Then the* **relative composed** *machine specification* $\mathcal{S}$ *w.r.t.* $\overline{\mathrm{W}}$ *is defined as* (B, H) *where* $B \triangleq ((\mathrm{In}_1 \setminus \mathrm{Out}_2 \cup \mathrm{In}_2 \setminus \mathrm{Out}_1, \mathrm{Out}_1 \setminus \mathrm{In}_2 \cup \mathrm{Out}_2 \setminus \mathrm{In}_1), (\mathrm{V}_1 \cup \mathrm{V}_2, \mathrm{X}_1 \cup \mathrm{X}_2))$ *and* $\mathrm{H} \triangleq \exists \epsilon_1, \epsilon_2. ({}_{B_1^A} \odot_{B_2^A} (\epsilon, \epsilon_1, \epsilon_2) \wedge (\mathrm{I}_1 \wedge \Box\mathrm{T}_1 \wedge \mathrm{L}_1 \wedge \mathrm{W}_1)[\epsilon_1/\epsilon] \wedge (\mathrm{I}_2 \wedge \Box\mathrm{T}_2 \wedge \mathrm{L}_2 \wedge \mathrm{W}_2)[\epsilon_2/\epsilon])$.

Theorem 9 (Relative composition corresponds to semantic merge)
Given machine system specifications $(B_i, \mathrm{I}_i \wedge \Box\mathrm{T}_i \wedge \mathrm{L}_i)$ *where* $B_i \triangleq ((\mathrm{In}_i, \mathrm{Out}_i), (\mathrm{V}_i, \mathrm{X}_i))$, *and given DTL formulae* W_i *over* B_i *for* $i = 1, 2$ *and let* $\overline{W} \triangleq (Hist(\mathrm{W}_c), Hist(\mathrm{W}_a))$ *and given the relative composed system as in Def. 41, i.e.,* (B, H) *where* $B \triangleq ((\mathrm{In}_1 \setminus \mathrm{Out}_2 \cup \mathrm{In}_2 \setminus \mathrm{Out}_1, \mathrm{Out}_1 \setminus \mathrm{In}_2 \cup \mathrm{Out}_2 \setminus \mathrm{In}_1), (\mathrm{V}_1 \cup \mathrm{V}_2, \mathrm{X}_1 \cup \mathrm{X}_2))$ *and* $\mathrm{H} \triangleq \exists \epsilon_1, \epsilon_2. ({}_{B_1^A} \odot_{B_2^A} (\epsilon, \epsilon_1, \epsilon_2) \wedge (\mathrm{I}_1 \wedge \Box\mathrm{T}_1 \wedge \mathrm{L}_1 \wedge \mathrm{W}_1)[\epsilon_1/\epsilon] \wedge (\mathrm{I}_2 \wedge \Box\mathrm{T}_2 \wedge \mathrm{L}_2 \wedge \mathrm{W}_2)[\epsilon_2/\epsilon])$ *then*

$$Hist(\mathrm{I}_1 \wedge \Box\mathrm{T}_1 \wedge \mathrm{L}_1) \, \textcircled{\scriptsize $\overline{W}$} \, Hist(\mathrm{I}_2 \wedge \Box\mathrm{T}_2 \wedge \mathrm{L}_2) = Hist(\mathrm{H})$$

2.5.3 Proving Semantic Relative Refinement of Specifications

The above sections explain the purpose of the restricting set W. In order to prove relative refinement we must know how this set W looks like. Is it a safety set, a liveness set or neither of them? A result of [AS85] states that every set of histories can be represented as the intersection of a safety and a liveness set. Now lemma 1 expresses that for a machine M_1, $Comp(M_1)$ is a safety set. So we will represent W as a machine M_1 and an external set L_1 s.t. W is machine closed, i.e., $cl(Comp(M_1) \cap L_1) = Comp(M_1)$. We also require that $(B, Comp(M) \cap Comp(M_1) \cap L \cap L_1)$ is machine closed, i.e., $cl(Comp(M) \cap Comp(M_1) \cap L \cap L_1) = Comp(M) \cap Comp(M_1)$, because this is the system that is used in the relative refinement relation. We want to use the refinement mappings of Def. 38 to prove relative refinement of systems. This means that $Comp(M) \cap Comp(M_1)$ should be represented as a machine M_2 such that $Comp(M_2) = Comp(M) \cap Comp(M_1)$. The following lemma expresses that this M_2 can be constructed from M and M_1.

Lemma 12
Given machines $M \triangleq (B, I, T)$ *and* $M_1 \triangleq (B, I_1, T_1)$. *Define machine* M_2 *as* (B, I_2, T_2) *where* I_2 *and* T_2 *are as follows:*

- $I_2 \triangleq I \cap I_1$, *and*
- $T_2 \triangleq T \cap T_1$.

Then $Comp(M_2) = Comp(M) \cap Comp(M_1)$.

Now the technique of refinement mappings from Section 2.4 can be applied to prove relative refinement of systems. This is expressed in the following definition.

Definition 42 (Relative refinement mapping between machine specifications)
Given concrete machine specification $\mathcal{S}_c \triangleq (B_c, Comp(M_c) \cap L_c)$ *and set* $W_c = Comp(M_{c1}) \cap L_{c1}$, *and given abstract machine specification* $\mathcal{S}_a \triangleq (B_a, Comp(M_a) \cap L_a)$ *and set* $W_a = Comp(M_{a1}) \cap L_{a1}$. *A* **relative refinement mapping** *from machine specification* $\mathcal{S}_c$ *to machine specification* $\mathcal{S}_a$ *is a mapping* $f : \Sigma \to \Sigma$ *s.t.*

- *For all* $\sigma \in \Sigma$, $\sigma|^1_{\mathrm{V}_c} = f(\sigma)|^1_{\mathrm{V}_c}$.
-
  - *For all* $\sigma_c \in I_c \cap I_{c1}$, *exist* $\sigma_a \in I_a \cap I_{a1}$ *s.t.* $\sigma_a = f(\sigma_c)$.
  - *For all* $\langle d, \sigma_{c1}, \sigma_{c2}\rangle \in T_c \cap T_{c1}$, $\langle d, f(\sigma_{c1}), f(\sigma_{c2})\rangle \in T_a \cap T_{a1}$ *or* $(f(\sigma_{c1}) = f(\sigma_{c2}) \wedge d(\epsilon) \in \{\lambda, \mathbf{i}, \mathbf{e}\}$.
  - *For all* $h_c \in Comp(M_c) \cap Comp(M_{c1} \cap L_c$ *there exist a* $h_a \in L_a \cap L_{a1}$ *s.t. for all* $t \in \mathbb{R}^{\geq 0}$, $\langle \psi_c(t), \theta_c(t)\rangle = \langle \psi_a(t), \theta(t)_a\rangle$ *and* $f(\theta_c(t)) = \theta_a(t)$.

The following lemma expresses that relative refinement mappings are indeed sufficient for proving relative refinement of machine specifications.

Lemma 13
Given concrete machine specification $\mathcal{S}_c \triangleq (B_c, Comp(M_c) \cap L_c)$ *and set* $W_c = Comp(M_{c1})$ $\cap L_{c1}$, *and given abstract machine specification* $\mathcal{S}_a \triangleq (B_a, Comp(M_a) \cap L_a)$ *and set* $W_a = Comp(M_{a1}) \cap L_{a1}$ *s.t.* $\mathfrak{O}(B_c) = \mathfrak{O}(B_a)$. *If there exists a relative refinement mapping from* $\mathcal{S}_c$ *to* $\mathcal{S}_a$ *then* $\mathcal{S}_c \;{}_{W_c}\mathbf{ref}^{W_a}\, \mathcal{S}_a$.

2.5.4 Proving Relative Refinement of DTL Specifications

Using the results of the previous section and Section 2.4 it is not surprising that following rule can be applied to prove relative refinement of systems.

Rule 3 (Proof rule for relative refinement)
Given concrete machine specification $\mathcal{S}_c \triangleq (B_c, \mathrm{I}_c \wedge \Box \mathrm{T}_c \wedge \mathrm{L}_c)$ *and* $\mathrm{W}_c \triangleq \mathrm{I}_{c1} \wedge \Box \mathrm{T}_{c1} \wedge \mathrm{L}_{c1}$ *and abstract machine specification* $\mathcal{S}_a \triangleq (B_a, \mathrm{I}_a \wedge \Box \mathrm{T}_a \wedge \mathrm{L}_a)$ *and* $\mathrm{W}_a \triangleq \mathrm{I}_{a1} \wedge \Box \mathrm{T}_{a1} \wedge \mathrm{L}_{a1}$ *s.t.* $\mathfrak{O}(B_c) = \mathfrak{O}(B_a)$. *Let* f *be a relative refinement mapping from* $\mathcal{S}_c$ *to* $\mathcal{S}_a$ *then*

$$
\begin{array}{l}
\mathcal{S}_c \cap Hist(W_c) \models (\mathrm{I}_c \wedge \mathrm{I}_{c1}) \rightarrow (\mathrm{I}_a \wedge \mathrm{I}_{a1})\,[f/\mathrm{X}_a] \\
\mathcal{S}_c \cap Hist(W_c) \models (T_c \wedge T_{c1}) \rightarrow (T_a \wedge T_{a1})\,[f/\mathrm{X}_a] \\
\mathcal{S}_c \cap Hist(W_c) \models (L_a \cap L_{a1})\,[f/\mathrm{X}_a] \\
\hline
\models (\exists \mathrm{X}_c\,.\,(\mathrm{I}_c \wedge \Box \mathrm{T}_c \wedge \mathrm{L}_c \wedge W_c)) \rightarrow (\exists \mathrm{X}_a\,.\,(\mathrm{I}_a \wedge \Box \mathrm{T}_a \wedge \mathrm{L}_a \wedge W_a))
\end{array}
$$

Chapter 3

Readers/Writers Example

3.1 Introduction

The relative refinement technique will now be used to formalize Dijkstra's development strategy for the readers/writers problem. The readers/writers problem, described intuitively, is as follows: given N readers and M writers, a reader performs, cyclically, non-critical action `NCS` and critical action `READ`, and a writer performs, again cyclically, non-critical action `NCS` and critical action `WRITE`. These readers and writers must be synchronized in such a way that if a writer performs the `WRITE` action it is the only process that performs a critical action, i.e. mutual exclusion is required (`ME`). Furthermore, it is necessary that any request to execute the critical action is eventually granted, i.e. eventual access should hold (`EA`). It is this synchronizer that has to be developed. But before we give the development we formulate an abstract specification for the problem.

The abstract specification of Dijkstra consists of a program, implementing the above readers and writers, and the requirements `ME` and `EA`. In our formalism this will be represented by system $\mathcal{S}_0$ and requirement W_0. The development process has four steps: in the first step Dijkstra gives an implementation by a program that produces undesirable deadlocked computations. In our formalism the first implementation is represented by system $\mathcal{S}_1$ and a requirement W_1 which removes the deadlocked computations. We will prove that $\mathcal{S}_1$ relatively refines $\mathcal{S}_0$ with respect to $(\mathrm{W}_1, \mathrm{W}_0)$. In the second step Dijkstra uses the split binary semaphore technique to delete the deadlocked computations from the first implementation; he obtains by this technique a second implementation that introduces as undesirable computations new deadlocked ones. In our formalism the second implementation is represented by the system $\mathcal{S}_2$ and the requirement W_2 that removes the newly introduced deadlocked computations. We will prove that $\mathcal{S}_2$ relatively refines $\mathcal{S}_1$ with respect to $(\mathrm{W}_2, \mathrm{W}_1)$. These deadlocked computations are deleted in the third step resulting in a third implementation that contains as undesirable computations unnecessarily blocking ones. These computations are not deadlocking computations but only computations that are inefficient because they suspend a reader or writer unnecessarily. In our formalism the third implementation will be represented by the system $\mathcal{S}_3$ and the requirement W_3 that removes the unnecessarily blocking computations. It is proved that $\mathcal{S}_3$ relatively refines $\mathcal{S}_2$ with respect to $(\mathrm{W}_3, \mathrm{W}_2)$. In the fourth step, these unnecessarily blocking computations are deleted and also the resulting implementation is cleaned up. In our formalism the fourth implementation will be represented by system $\mathcal{S}_4$ and it is proved that $\mathcal{S}_4$ relatively refines $\mathcal{S}_3$ with respect to $(\mathbf{true}, \mathrm{W}_3)$, i.e., in the fourth step no further requirements are imposed.

3.2 The abstract specification

Here Dijkstra's strategy [Dij79] is followed and it is shown how the informal approach used there can be formalized.
Dijkstra rewrites the informal specification as follows: as a first step, he describes readers and writers by programs (he assumes that the semantics of these programs is intuitively clear):

$$\texttt{reader}_i^0: \quad \mathbf{do}\ \texttt{true} \rightarrow \texttt{NCS;READ}\ \ \mathbf{od}$$

$$\texttt{writer}_j^0: \quad \mathbf{do}\ \texttt{true} \rightarrow \texttt{NCS;WRITE}\ \mathbf{od}$$

He then combines these programs into one parallel program $\texttt{Syn}^0$. $\texttt{Syn}^0$ denotes the abstract specification and is defined as follows:

$$\texttt{Syn}^0 \ : \ \|_{i=1}^{N}\ \texttt{reader}_i^0 \ \|\ \|_{j=1}^{M}\ \texttt{writer}_j^0 \ ,$$

Where $\|_{i=1}^{N}\ \texttt{reader}_i^0$ is a notation for the N-fold parallel composition of $\texttt{reader}_i^0$. Finally he formulates an informal requirement to exclude from $\texttt{Syn}^0$ the unwanted sequences. This requirement is the same as in the introduction: $\texttt{ME}$ and $\texttt{EA}$. The complete abstract specification is thus $\texttt{Syn}^0$ plus this requirement.

Each $\texttt{reader}_i^0$ and $\texttt{writer}_j^0$ is represented respectively by DTL machine specification $\mathcal{S}_{r_i^0}$ and $\mathcal{S}_{w_j^0}$. We will incorporate the requirement $\texttt{EA}$ as a liveness requirement in each machine specification. The parallel composition of all the separate machine specifications $\mathcal{S}_0 \triangleq \|_{i=1}^{N}$ $\mathcal{S}_{r_i^0}$ $\|\|\|_{j=1}^{M}$ $\mathcal{S}_{w_j^0}$ then corresponds to $\texttt{Syn}^0$ plus $\texttt{EA}$. $\texttt{ME}$ will be incorporated as an extra requirement on $\mathcal{S}_0$. The following sections will give in detail the machine specifications $\mathcal{S}_{r_i^0}$ and $\mathcal{S}_{w_j^0}$, and the extra requirement W_0.

3.2.1 Specification $\mathcal{S}_{r_i^0}$

The formal specification $\mathcal{S}_{r_i^0} = (B_{r_i^0}, \mathrm{H}_{r_i^0})$ where $\mathrm{H}_{r_i^0} \triangleq \mathrm{I}_{r_i^0} \wedge \Box \mathrm{T}_{r_i^0} \wedge \mathrm{L}_{r_i^0}$ and $B_{r_i^0}$, $\mathrm{I}_{r_i^0}$, $\mathrm{T}_{r_i^0}$ and $\mathrm{L}_{r_i^0}$ are as follows:

1. **Basis** $B_{r_i^0} \triangleq ((\mathrm{In}_{r_i^0}, \mathrm{Out}_{r_i^0}), (\mathrm{V}_{r_i^0}, \mathrm{X}_{r_i^0}))$

$$\begin{aligned}
\mathrm{Out}_{r_i^0} &\triangleq \emptyset, \\
\mathrm{In}_{r_i^0} &\triangleq \emptyset, \\
\mathrm{V}_{r_i^0} &\triangleq \{\mathrm{s}_{r_i}\}, \\
\mathrm{X}_{r_i^0} &\triangleq \emptyset
\end{aligned}$$

- $\mathbf{s}_{r_i} = 0$: reader$_i^0$ is non critical.
- $\mathbf{s}_{r_i} = 1$: reader$_i^0$ is critical.

2. **Initial States:**

$$\mathrm{I}_{r_i^0} \triangleq \mathbf{s}_{r_i} = 0$$

Reader$_i^0$ starts in the non critical state.

3. **Transitions:**
$\mathrm{T}_{r_i^0} \triangleq$

$\tau_{r_{i,1}^0}$ $\quad \big(\epsilon = \mathbf{i} \wedge \mathbf{s}_{r_i} = 0 \wedge \mathbf{s}'_{r_i} = 1\big)$

Reader$_i^0$ becomes critical.

$\tau_{r_{i,2}^0}$ $\quad \vee \ \big(\epsilon = \mathbf{i} \wedge \mathbf{s}_{r_i} = 1 \wedge \mathbf{s}'_{r_i} = 0\big)$

Reader$_i^0$ becomes critical.

$\tau_{r_{i,0}^0}$ $\quad \vee \ \mathbf{stut}_{r_i^0}$

These transitions are illustrated in figure 3.1

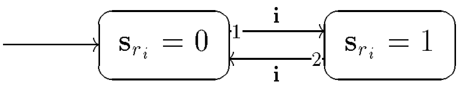

Figure 3.1: Transitions of reader$_i^0$.

4. **Liveness**
As discussed above $\mathrm{L}_{r_i^0}$ should express the `EA` requirement, i.e., all the transitions are weakly fair.
Let $\mathrm{WF}_{r_i^0} \triangleq \{\tau_{r_{i,k}^0} \mid k \in \{1,2\}\}$ and $\mathrm{SF}_{r_i^1} \triangleq \emptyset$ then

$$\mathrm{L}_{r_i^0} \triangleq \bigwedge_{\tau \in \mathrm{WF}_{r_i^0}} (\Diamond\Box En(\tau) \rightarrow \Box\Diamond\tau) \wedge \bigwedge_{\tau \in \mathrm{SF}_{r_i^0}} (\Box\Diamond En(\tau) \rightarrow \Box\Diamond\tau)$$

3.2.2 Specification $\mathcal{S}_{w_j^0}$

The formal specification $\mathcal{S}_{w_j^0} = (B_{w_j^0}, \mathrm{H}_{w_j^0})$ where $\mathrm{H}_{w_j^0} \triangleq \mathrm{I}_{w_j^0} \wedge \Box\mathrm{T}_{w_j^0} \wedge \mathrm{L}_{w_j^0}$ and $B_{w_j^0}$, $\mathrm{I}_{w_j^0}$, $\mathrm{T}_{w_j^0}$ and $\mathrm{L}_{w_j^0}$ are as follows:

1. **Basis** $B_{w_j^0} \triangleq ((\mathrm{In}_{w_j^0}, \mathrm{Out}_{w_j^0}), (\mathrm{V}_{w_j^0}, \mathrm{X}_{w_j^0}))$

$$\begin{array}{lcl} \mathrm{Out}_{w_j^0} & \triangleq & \emptyset, \\ \mathrm{In}_{w_j^0} & \triangleq & \emptyset, \\ \mathrm{V}_{w_j^0} & \triangleq & \{\mathbf{s}_{w_j}\}, \\ \mathrm{X}_{w_j^0} & \triangleq & \emptyset \end{array}$$

   - $\mathbf{s}_{w_j} = 0$: writer$_j^0$ is non critical.
   - $\mathbf{s}_{w_j} = 1$: writer$_j^0$ is critical.

2. **Initial States:**

$$\mathrm{I}_{w_j^0} \triangleq \mathbf{s}_{w_j} = 0$$

   Writer$_j^0$ starts in the non critical state.

3. **Transitions:**
   $\mathrm{T}_{w_j^0} \triangleq$

   $\tau_{w_{j,1}^0}$ $\quad \left(\epsilon = \mathbf{i} \wedge \mathbf{s}_{w_j} = 0 \wedge \mathbf{s}'_{w_j} = 1\right)$
   Writer$_j^0$ becomes critical.

   $\tau_{w_{j,2}^0}$ $\quad \vee \left(\epsilon = \mathbf{i} \wedge \mathbf{s}_{w_j} = 1 \wedge \mathbf{s}'_{w_j} = 0\right)$
   Writer$_j^0$ becomes non critical.

   $\tau_{w_{j,0}^0}$ $\quad \vee\ \mathbf{stut}_{w_j^0}$

   These transitions are illustrated in figure 3.2

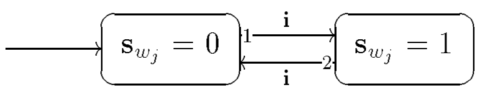

Figure 3.2: Transitions of writer$_i^0$.

4. **Liveness**
   As discussed above $\mathrm{L}_{w_j^0}$ should express the `EA` requirement, i.e., all the transitions are weakly fair.
   Let $\mathrm{WF}_{w_j^0} \triangleq \{\tau_{w_{j,k}^0} \mid k \in \{1, 2\}\}$ and $\mathrm{SF}_{w_j^1} \triangleq \emptyset$ then

$$\mathrm{L}_{w_j^0} \triangleq \bigwedge_{\tau \in \mathrm{WF}_{w_j^0}} (\Diamond\Box En(\tau) \to \Box\Diamond\tau) \wedge \bigwedge_{\tau \in \mathrm{SF}_{w_j^0}} (\Box\Diamond En(\tau) \to \Box\Diamond\tau)$$

3.2.3 Requirement W_0

The extra condition on the composed system should express the mutual exclusion property ME. A reader (writer) is critical if $\mathtt{s}_{r_i} = 1$ ($\mathtt{s}_{w_j} = 1$. Let $\sharp(i : 1 \leq i \leq N : \mathtt{s}_{r_i} = 1)$ denote the number of components such that $\mathtt{s}_{r_i} = 1$. The condition is then as follows:

$$\begin{aligned} \mathrm{W}_0 \triangleq \Box \quad & (\sharp(j : 1 \leq j \leq M : \mathtt{s}_{w_j} = 1) = 0 \vee \\ & (\sharp(i : 1 \leq i \leq N : \mathtt{s}_{r_i} = 1) = 0 \wedge \sharp(j : 1 \leq j \leq M : \mathtt{s}_{w_j} = 1) = 1) \end{aligned}$$

As seen in Section 2.5 W_0 should be defined as a machine and a liveness condition in order to apply the proof rule for relative refinement. This can be done quite easily. The liveness condition is **true**. Define p as $\sharp(j : 1 \leq j \leq M : \mathtt{s}_{w_j} = 1) = 0 \vee (\sharp(i : 1 \leq i \leq N : \mathtt{s}_{r_i} = 1) = 0 \wedge \sharp(j : 1 \leq j \leq M : \mathtt{s}_{w_j} = 1) = 1)$ and p' as $\sharp(j : 1 \leq j \leq M : \mathtt{s}'_{w_j} = 1) = 0 \vee (\sharp(i : 1 \leq i \leq N : \mathtt{s}'_{r_i} = 1) = 0 \wedge \sharp(j : 1 \leq j \leq M : \mathtt{s}'_{w_j} = 1) = 1)$. Then $p \wedge \Box((p \wedge p') \vee \mathbf{stut}_0)$ is the machine in DTL corresponding to W_0.

3.3 The first development step

Dijkstra's next step is to translate the informally stated requirement into formal program form, i.e. to transform reader_i^0 and writer_j^0 in such a way that they satisfy the mutual-exclusion requirement ME. We discuss this translation informally.

He introduces shared variables `aw` and `ar` and binary semaphore `x`. Shared variable `ar` represents the number of readers which may execute their `READ`, and `aw` represents the number of writers which may execute their `WRITE`. A reader increases `ar` by 1 if it allowed to execute its `READ` and decreases `ar` by 1 if it is finished with executing its `READ`. Since `ar` will be changed and accessed by several readers, Dijkstra protects the operation of increasing and decreasing `ar` by semaphore operations P and V on binary semaphore x to ensure that only one reader changes `ar` at a time, i.e. mutual exclusion. The synchronization requirement is brought into reader_i by guarding the increasing operation of `ar` with condition `aw=0`, i.e., the number of writers that may execute their `WRITE` equals zero. The same can be done for writer_j. The initial values of the shared variables are 0 and the initial value of semaphore `x` is 1. This results in the following programs:

```
reader_i^1:
     do true → NCS;
               P(x);(*) if aw=0 →ar:=ar+1 fi;V(x);
               READ;
               P(x);ar:=ar-1;V(x)
     od
writer_j^1:
     do true → NCS;
               P(x);(+) if aw=0 ∧ ar=0→aw:=aw+1 fi;V(x);
               WRITE;
               P(x);aw:=aw-1;V(x)
     od
```

$\mathtt{Syn}^1 \; : \; \|_{i=1}^{N} \; \mathtt{reader}_i^1 \; \| \; \|_{j=1}^{M} \; \mathtt{writer}_j^1$

This first approximation can deadlock. A deadlocked sequence is for instance:

> A writer starts in the initial state and then executes `NCS;P(x);(+)`, as result of that the value of `aw` changes in 1. A reader then executes `NCS;P(x);(*)` and blocks in the `if-fi` clause of `(*)` because `aw=1` and the semantics of this `if-fi` is such that when no guard is fulfilled it blocks. Then no reader or writer can then execute `(*)` or `(+)` because `x=0` and `x` holds this value forever. The requirement is thus that these deadlocked sequences are not generated.

Now $\texttt{Syn}^1$ will be specified in Stark's formalism. Like the abstract specification each reader_i^1 and writer_j^1 is represented by a separate machine specification $\mathcal{S}_{r_i^1}$ and $\mathcal{S}_{w_j^1}$. The composed system $\mathcal{S}_1 \triangleq \|_{i=1}^{N} \mathcal{S}_{r_i^1} \;\|\|_{j=1}^{M} \mathcal{S}_{w_j^1}$ and corresponds with $\texttt{Syn}^1$. For $\mathcal{S}_1$ the extra requirement W_1 for excluding deadlocked computations is formulated. In the following subsections we give DTL machine specifications $\mathcal{S}_{r_i^1}$ and $\mathcal{S}_{w_j^1}$, and the extra requirement W_1.

3.3.1 Specification $\mathcal{S}_{r_i^1}$

The formal specification $\mathcal{S}_{r_i^1} \triangleq (B_{r_i^1}, \mathrm{H}_{r_i^1})$ where $\mathrm{H}_{r_i^1} \triangleq \mathrm{I}_{r_i^1} \wedge \Box \mathrm{T}_{r_i^1} \wedge \mathrm{L}_{r_i^1}$ and $B_{r_i^1}$, $\mathrm{I}_{r_i^1}$, $\mathrm{T}_{r_i^1}$ and $\mathrm{L}_{r_i^1}$ are as follows:

1. **Basis** $B_{r_i^1} = ((\mathrm{In}_{r_i^1}, \mathrm{Out}_{r_i^1}), (\mathrm{V}_{r_i^1}, \mathrm{X}_{r_i^1}))$

$$\begin{array}{lcl}
\mathrm{In}_{r_i^1} & \triangleq & \emptyset, \\
\mathrm{Out}_{r_i^1} & \triangleq & \emptyset, \\
\mathrm{V}_{r_i^1} & \triangleq & \{\mathbf{x}, \mathbf{ar}, \mathbf{aw}, \mathrm{s}_{r_i}\}, \\
\mathrm{X}_{r_i^1} & \triangleq & \{\ell_{r_i^1}\}
\end{array}$$

- $\ell_{r_i^1} = 0$: reader_i^1 is non critical.
- $\ell_{r_i^1} = 1$: reader_i^1 has passed its first P-operation.
- $\ell_{r_i^1} = 2$: reader_i^1 has increased **ar** by 1.
- $\ell_{r_i^1} = 3$: reader_i^1 is critical.
- $\ell_{r_i^1} = 4$: reader_i^1 has passed its second P-operation.
- $\ell_{r_i^1} = 5$: reader_i^1 has decreased **ar** by 1.

Let $\Psi_1 \triangleq (\mathbf{x}, \mathbf{ar}, \mathbf{aw}, \mathrm{s}_{r_i}, \ell_{r_i^1})$ and $\Psi_1' \triangleq (\mathbf{x}', \mathbf{ar}', \mathbf{aw}', \mathrm{s}_{r_i}', \ell_{r_i^1}')$.

2. **Initial States:**

$$\mathrm{I}_{r_i^1} \triangleq \Psi_1 = (1, 0, 0, 0, 0)$$

3. **Transitions:**
$\mathrm{T}_{r_i^1} \triangleq$

$\tau_{r^1_{i,1}}$ $\quad \Big(\epsilon = \mathbf{i} \wedge \ell_{r^1_i} = 0 \wedge \mathbf{x} = 1 \wedge \Psi_1' = \Psi_1 \big[0, 1/\mathbf{x}, \ell_{r^1_i}\big]\Big)$

Reader^1_i executes the first P-action.

$\tau_{r^1_{i,2}}$ $\quad \vee \Big(\epsilon = \mathbf{i} \wedge \ell_{r^1_i} = 1 \wedge \mathbf{aw} = 0 \wedge \Psi_1' = \Psi_1 \big[\mathbf{ar} + 1, 2/\mathbf{ar}, \ell_{r^1_i}\big]\Big)$

Reader^1_i can increase the number of active readers by if the number of active writers is zero.

$\tau_{r^1_{i,3}}$ $\quad \vee \Big(\epsilon = \mathbf{i} \wedge \ell_{r^1_i} = 2 \wedge \Psi_1' = \Psi_1 \big[1, 1, 3/\mathbf{s}_{r_i}, \mathbf{x}, \ell_{r^1_i}\big]\Big)$

Reader^1_i becomes critical.

$\tau_{r^1_{i,4}}$ $\quad \vee \Big(\epsilon = \mathbf{i} \wedge \ell_{r^1_i} = 3 \wedge \mathbf{x} = 1 \wedge \Psi_1' = \Psi_1 \big[0, 4/\mathbf{x}, \ell_{r^1_i}\big]\Big)$

Reader^1_i executes its second P-action.

$\tau_{r^1_{i,5}}$ $\quad \vee \Big(\epsilon = \mathbf{i} \wedge \ell_{r^1_i} = 4 \wedge \Psi_1' = \Psi_1 \big[\mathbf{ar} - 1, 5/\mathbf{ar}, \ell_{r^1_i}\big]\Big)$

Reader^1_i decreases the number of active readers by one.

$\tau_{r^1_{i,6}}$ $\quad \vee \Big(\epsilon = \mathbf{i} \wedge \ell_{r^1_i} = 5 \wedge \Psi_1' = \Psi_1 \big[0, 1, 0/\mathbf{s}_{r_i}, \mathbf{x}, \ell_{r^1_i}\big]\Big)$

Reader^1_i becomes non critical.

$\tau_{r^1_{i,7}}$ $\quad \vee \Big(\epsilon = \mathbf{e} \wedge \mathbf{x} = 1 \wedge \Psi_1' = \Psi_1 [0/\mathbf{x}]\Big)$

The environment executes a P-operation on $\mathbf{x}$.

$\tau_{r^1_{i,8}}$ $\quad \vee \Big(\epsilon = \mathbf{e} \wedge \ell_{r^1_i} \in \{0, 3\} \wedge \mathbf{x} = 0 \wedge \Psi_1' = \Psi_1 [1/\mathbf{x}]\Big)$

The environment executes a V-operation on $\mathbf{x}$.

$\tau_{r^1_{i,0}}$ $\quad \vee\ \mathbf{stut}_{r^1_i}$

These transitions are illustrated in figure 3.3

4. **Liveness:**
   $\mathrm{L}_{r^1_i}$ expresses that the P- and V-operations on the semaphore $\mathbf{x}$ are strongly fair and all the other transitions are weakly fair.
   Let $\mathrm{WF}_{r^1_i} \triangleq \{\tau_{r^1_{i,k}} \mid k \in \{2, 5\}\}$ and $\mathrm{SF}_{r^1_i} \triangleq \{\tau_{r^1_{i,k}} \mid k \in \{1, 3, 4, 6, 7, 8\}\}$ then

$$\mathrm{L}_{r^1_i} \triangleq \bigwedge_{\tau \in \mathrm{WF}_{r^1_i}} (\Diamond\Box En(\tau) \rightarrow \Box\Diamond\tau) \wedge \bigwedge_{\tau \in \mathrm{SF}_{r^1_i}} (\Box\Diamond En(\tau) \rightarrow \Box\Diamond\tau)$$

3.3.2 Specification $\mathcal{S}_{w^1_j}$

The formal specification $\mathcal{S}_{w^1_j} \triangleq (B_{w^1_j}, \mathrm{H}_{w^1_j})$ where $\mathrm{H}_{w^1_j} \triangleq \mathrm{I}_{w^1_j} \wedge \Box\mathrm{T}_{w^1_j} \wedge \mathrm{L}_{w^1_j}$ and $B_{w^1_j}$, $\mathrm{I}_{w^1_j}$, $\mathrm{T}_{w^1_j}$ and $\mathrm{L}_{w^1_j}$ are as follows:

1. **Basis** $B_{w^1_j} = ((\mathrm{In}_{w^1_j}, \mathrm{Out}_{w^1_j}), (\mathrm{V}_{w^1_j}, \mathrm{X}_{w^1_j}))$

$$\begin{aligned}
\mathrm{In}_{w^1_j} &\triangleq \emptyset, \\
\mathrm{Out}_{w^1_j} &\triangleq \emptyset, \\
\mathrm{V}_{w^1_j} &\triangleq \{\mathbf{x}, \mathbf{ar}, \mathbf{aw}, \mathbf{s}_{w_j}\}, \\
\mathrm{X}_{w^1_j} &\triangleq \{\ell_{w^1_j}\}
\end{aligned}$$

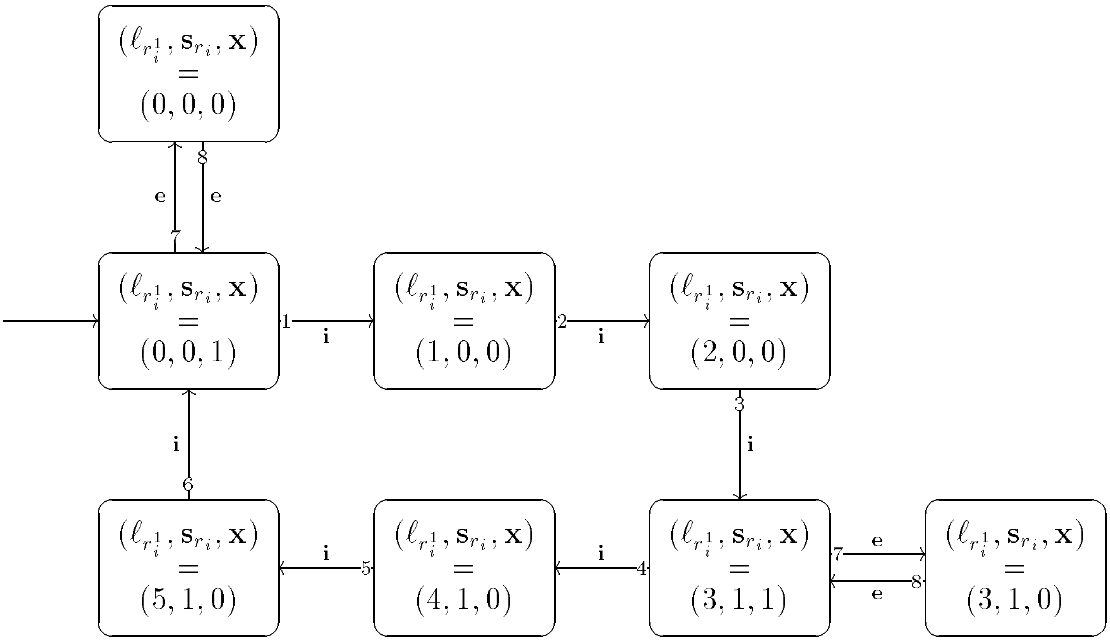

Figure 3.3: Transitions of reader$_i^1$.

- $\ell_{w_j^1} = 0$: writer$_j^1$ is non critical.
- $\ell_{w_j^1} = 1$: writer$_j^1$ has passed its first P-operation.
- $\ell_{w_j^1} = 2$: writer$_j^1$ has increased **aw** by 1.
- $\ell_{w_j^1} = 3$: writer$_j^1$ is critical.
- $\ell_{w_j^1} = 4$: writer$_j^1$ has passed its second P-operation.
- $\ell_{w_j^1} = 5$: writer$_j^1$ has decreased **aw** by 1.

Let $\Psi_1 \triangleq (\mathbf{x}, \mathbf{ar}, \mathbf{aw}, \mathrm{s}_{w_j}, \ell_{w_j^1})$ and $\Psi_1' \triangleq (\mathbf{x}', \mathbf{ar}', \mathbf{aw}', \mathrm{s}'_{w_j}, \ell'_{w_j^1})$.

2. **Initial States:**

   $$\mathrm{I}_{w_j^1} \triangleq \Psi_1 = (1, 0, 0, 0)$$

3. **Transitions:**
   $\mathrm{T}_{w_j^1} \triangleq$

$\tau_{w_{j,1}^1}$ $\quad \Big(\epsilon = \mathbf{i} \wedge \ell_{w_j^1} = 0 \wedge \mathbf{x} = 1 \wedge \Psi_1' = \Psi_1\left[0, 1/\mathbf{x}, \ell_{w_j^1}\right]\Big)$

Writer$_j^1$ executes the first P-action.

$\tau_{w_{j,2}^1}$ $\quad \vee \Big(\epsilon = \mathbf{i} \wedge \ell_{w_j^1} = 1 \wedge \mathbf{ar} = 0 \wedge \mathbf{aw} = 0 \wedge \Psi_1' = \Psi_1\left[\mathbf{aw} + 1, 2/\mathbf{aw}, \ell_{w_j^1}\right]\Big)$

Writer$_j^1$ can increase the numbers of active writers if the number of active writers and readers is zero.

$\tau_{w^1_{j,3}} \quad \vee \ \left(\epsilon = \mathbf{i} \wedge \ell_{w^1_j} = 2 \wedge \Psi_1' = \Psi_1 \left[1, 1, 3/\mathbf{s}_{w_j}, \mathbf{x}, \ell_{w^1_j}\right]\right)$

Writer^1_j becomes critical.

$\tau_{w^1_{j,4}} \quad \vee \ \left(\epsilon = \mathbf{i} \wedge \ell_{w^1_j} = 3 \wedge \mathbf{x} = 1 \wedge \Psi_1' = \Psi_1 \left[0, 4/\mathbf{x}, \ell_{w^1_j}\right]\right)$

Writer^1_j executes the second P-action.

$\tau_{w^1_{j,5}} \quad \vee \ \left(\epsilon = \mathbf{i} \wedge \ell_{w^1_j} = 4 \wedge \Psi_1' = \Psi_1 \left[\mathbf{aw} - 1, 5/\mathbf{aw}, \ell_{w^1_j}\right]\right)$

Writer^1_j decreases the number of active writers by one.

$\tau_{w^1_{j,6}} \quad \vee \ \left(\epsilon = \mathbf{i} \wedge \ell_{w^1_j} = 5 \wedge \Psi_1' = \Psi_1 \left[0, 1, 0/\mathbf{s}_{w_j}, \mathbf{x}, \ell_{w^1_j}\right]\right)$

Writer j becomes non critical.

$\tau_{w^1_{j,7}} \quad \vee \ \left(\epsilon = \mathbf{e} \wedge \mathbf{x} = 1 \wedge \Psi_1' = \Psi_1 \left[0/\mathbf{x}\right]\right)$

The environment executes a P-operation on $\mathbf{x}$.

$\tau_{w^1_{j,8}} \quad \vee \ \left(\epsilon = \mathbf{e} \wedge \ell_{w^1_j} \in \{0, 3\} \wedge \mathbf{x} = 0 \wedge \Psi_1' = \Psi_1 \left[1/\mathbf{x}\right]\right)$

The environment executes a V-operation on $\mathbf{x}$.

$\tau_{w^1_{j,0}} \quad \vee \ \mathbf{stut}_{w^1_j}$

These transitions are illustrated in figure 3.4

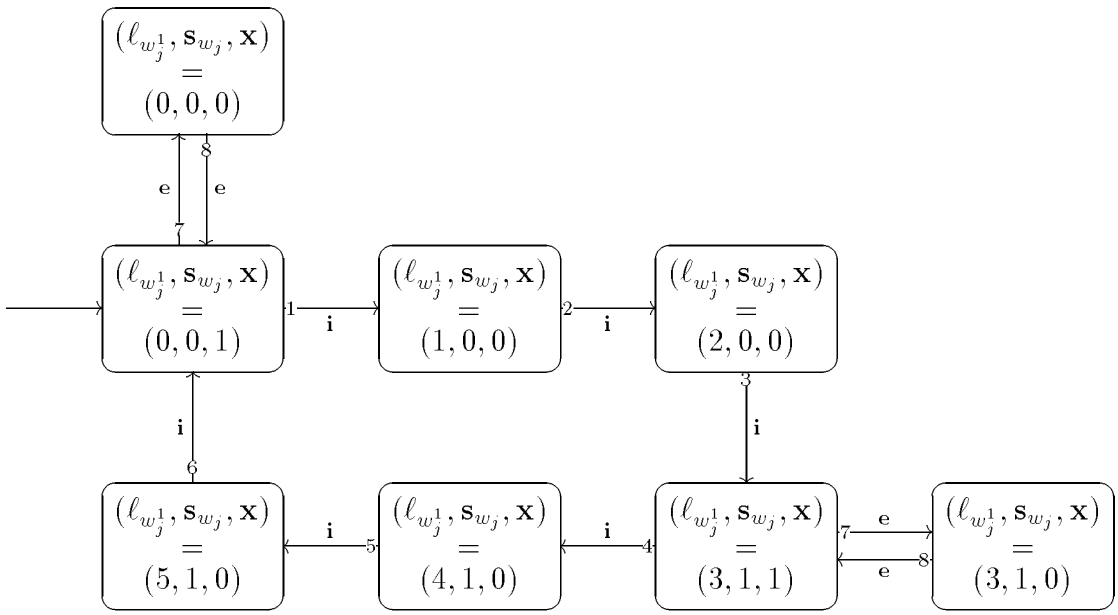

Figure 3.4: Transitions of writer^1_j.

4. **Liveness**
   $L_{w^1_j}$ expresses that the P- and V-operations on the semaphore $\mathbf{x}$ are strongly fair and all the other transitions are weakly fair.

Let $\mathrm{WF}_{w_j^1} \triangleq \{\tau_{w_{j,k}^1} \mid k \in \{2,5\}\}$ and $\mathrm{SF}_{w_j^1} \triangleq \{\tau_{w_{j,k}^1} \mid k \in \{1,3,4,6,7,8\}\}$ then

$$\mathrm{L}_{w_j^1} \triangleq \bigwedge_{\tau \in \mathrm{WF}_{w_j^1}} (\Diamond\Box En(\tau) \rightarrow \Box\Diamond\tau) \wedge \bigwedge_{\tau \in \mathrm{SF}_{w_j^1}} (\Box\Diamond En(\tau) \rightarrow \Box\Diamond\tau)$$

3.3.3 Requirement W_1

The condition should express that the described deadlocked sequences don't occur, i.e., it when **ar** is increased by 1 then $\mathbf{aw} = 0$ and when **aw** is increased by 1 then $\mathbf{aw} = 0$ and $\mathbf{ar} = 0$. Formally:

$$\mathrm{W}_1 \triangleq \Box\left(\left(\bigwedge_{i=1}^{N} \ell_{r_i^1} = 1 \rightarrow \mathbf{aw} = 0\right) \wedge \left(\bigwedge_{j=1}^{M} \ell_{w_j^1} = 1 \rightarrow (\mathbf{ar} = 0 \wedge \mathbf{aw} = 0)\right)\right)$$

This corresponds to the following machine: Let

$$\begin{array}{lcl} p_{ri} & \triangleq & \ell_{r_i^1} = 1 \rightarrow \mathbf{aw} = 0 \\ p'_{ri} & \triangleq & \ell'_{r_i^1} = 1 \rightarrow \mathbf{aw}' = 0 \\ p_{wj} & \triangleq & \ell_{w_j^1} = 1 \rightarrow (\mathbf{ar} = 0 \wedge \mathbf{aw} = 0) \\ p'_{wj} & \triangleq & \ell'_{w_j^1} = 1 \rightarrow (\mathbf{ar}' = 0 \wedge \mathbf{aw}' = 0) \end{array}$$

then W_1 is the conjunction of the machines $p_{ri} \wedge \Box((p_{ri} \wedge p'_{ri}) \vee stut)$ and $p_{wj} \wedge \Box((p_{wj} \wedge p'_{wj}) \vee stut)$ for $1 \leq i \leq N$ and $1 \leq j \leq M$.

3.3.4 $\mathcal{S}_1$ relatively refines $\mathcal{S}_0$

Since the semaphore **x** and the shared variables **ar** and **aw** are used only by the subcomponents of $\mathcal{S}_1$, we should prove $\mathcal{S}_1 \upharpoonright \{\mathbf{x}, \mathbf{ar}, \mathbf{aw}\}$ relatively refines $\mathcal{S}_0$ instead of $\mathcal{S}_1$ relatively refines $\mathcal{S}_0$. According to definition 35, 36 and theorem 8 $\mathcal{S}_1 \upharpoonright \{\mathbf{x}, \mathbf{ar}, \mathbf{aw}\}$ relatively refines $\mathcal{S}_0$ with respect to $(\mathrm{W}_1, \mathrm{W}_0)$ iff the following holds:

$\mathfrak{O}(B_1) = \mathfrak{O}(B_0)$ and
$\models (\exists \mathrm{X}_1 . (\mathrm{G}_1 \wedge (\epsilon = \mathbf{e} \Rightarrow (\mathrm{x}, \mathrm{ar}, \mathrm{aw})' = (\mathrm{x}, \mathrm{ar}, \mathrm{aw}))) \rightarrow (\exists \mathrm{X}_0 . (\mathrm{G}_0))$

where X_1 are the local variables from $\mathcal{S}_1$, i.e., $\mathrm{X}_1 \triangleq \{\ell_{r_i^1} \mid i = 1, \ldots, N\} \cup \{\ell_{w_j^1} \mid j = 1, \ldots, M\} \cup \{\mathrm{x}, \mathrm{aw}, \mathrm{ar}\}$ and G_1 is the composition of $\mathcal{S}_{r_i^1}$ $(i = 1, \ldots, N)$ and $\mathcal{S}_{w_j^1}$ $(j = 1, \ldots, M)$ and W_1,
let $\bar{\epsilon}_1 \triangleq \epsilon_{1,1}, \ldots, \epsilon_{1,N}, \epsilon_{1,N+1}, \ldots, \epsilon_{1,N+M}$, and
let $\bar{B}_1^A \triangleq B_{r_1^1}^A, \ldots, B_{r_N^1}^A, B_{w_1^1}^A, \ldots, B_{w_M^1}^A$
then $\mathrm{G}_1 \triangleq$

$$\left(\exists \bar{\epsilon}_1 . \odot_{\bar{B}_1^A}(\epsilon, \bar{\epsilon}_1) \wedge \bigwedge_{i=1}^{N} \mathrm{H}_{r_i^1}[\epsilon_{1,i}/\epsilon] \wedge \bigwedge_{j=1}^{M} \mathrm{H}_{w_j^1}[\epsilon_{1,N+j}/\epsilon]\right) \wedge \mathrm{W}_1$$

X_0 are the local variables from $\mathcal{S}_0$, i.e., $\mathrm{X}_0 \triangleq \emptyset$ and G_0 is the composition of $\mathcal{S}_{r_i^0}$ $(i = 1, \ldots, N)$ and $\mathcal{S}_{w_j^0}$ $(j = 1, \ldots, M)$ and W_0,

let $\bar{\epsilon}_0 \triangleq e_{1,1}, \ldots, \epsilon_{0,N}, \epsilon_{0,N+1}, \ldots, \epsilon_{0,N+M}$, and
let $\bar{B}_0^A \triangleq B^A_{r_1^0}, \ldots, B^A_{r_N^0}, B^A_{w_1^0}, \ldots, B^A_{w_M^0}$
then $\mathrm{G}_0 \triangleq$

$$\left(\exists \bar{\epsilon}_0 . \odot_{\bar{B}_0^A}(\epsilon, \bar{\epsilon}_0) \wedge \bigwedge_{i=1}^N \mathrm{H}_{r_i^0}[\epsilon_{0,i}/\epsilon] \wedge \bigwedge_{j=1}^M \mathrm{H}_{w_j^0}[\epsilon_{0,N+j}/\epsilon]\right) \wedge \mathrm{W}_0$$

Since W_0 can't be decomposed into sub-requirements but doesn't constrain the ϵ variables and W_1 can be decomposed into sub-requirements $\mathrm{W}_{r_i^1} \triangleq \Box(\ell_{r_i^1} = 1 \rightarrow \mathbf{aw} = 0)$ for reader$_i^1$ and $\mathrm{W}_{w_i^1} \triangleq \Box(\ell_{w_j^1} = 1 \rightarrow (\mathbf{aw} = 0 \wedge \mathbf{ar} = 0)$, and doesn't constrain the ϵ variables Lemma 9, 10 and 11 can be used for the proof, i.e., following proof rule can be used

$$\begin{array}{ll}
W_1 \subseteq \bigcap_{i=1}^N W_{r_i^1} \cap \bigcap_{j=1}^M W_{w_j^1} & \\
\mathcal{S}_{r_i^1} \ {}_{W_{r_i^1}}\mathbf{ref}^{W_0}\ \mathcal{S}_{r_i^0} & W_{r_i^1} \text{ constraining } B_{r_i^1} \\
\mathcal{S}_{w_j^1} \ {}_{W_{w_j^1}}\mathbf{ref}^{W_0}\ \mathcal{S}_{w_j^0} & W_{w_j^1} \text{ constraining } B_{w_j^1} \\
\hline
\mathcal{S}_1 \ {}_{W_1}\mathbf{ref}^{W_0}\ \mathcal{S}_0 &
\end{array}$$

This means we have to prove for $i = 1, \ldots, N$ and $j = 1, \ldots, M$:

$$\begin{array}{ll}
(1) & \left(\exists \ell_{r_i^1} . (\mathrm{H}_{r_i^1} \wedge \mathrm{W}_{r_i^1})\right) \rightarrow \mathrm{H}_{r_i^0} \wedge \mathrm{W}_0 \\
(2) & \left(\exists \ell_{w_j^1} . (\mathrm{H}_{w_j^1} \wedge \mathrm{W}_{w_j^1})\right) \rightarrow \mathrm{H}_{w_j^0} \wedge \mathrm{W}_0 \\
(3) & \mathrm{W}_1 \rightarrow (\mathrm{W}_{r_i^1} \wedge \mathrm{W}_{w_j^1})
\end{array}$$

ad (1) Rule 3 will be used to prove (1). This means one has to prove

$$\begin{array}{ll}
(a) & \mathcal{S}_1 \cap Hist(\mathrm{W}_1) \models (\mathrm{I}_{r_i^1} \wedge p_{ri}) \rightarrow \mathrm{I}_{r_i^0} \wedge p \\
(b) & \mathcal{S}_1 \cap Hist(\mathrm{W}_1) \models \mathrm{T}_{r_i^1} \wedge ((p_{ri} \wedge p'_{ri}) \vee \mathbf{stut}_{r_i^1}) \rightarrow \mathrm{T}_{r_i^0} \wedge ((p \wedge p') \vee \mathbf{stut}_0) \\
(c) & \mathcal{S}_1 \cap Hist(\mathrm{W}_1) \models \mathrm{L}_{r_i^0}
\end{array}$$

(a) **Proof 1**

$$\begin{array}{ll}
 & \mathrm{I}_{r_i^1} \wedge p_{ri} \\
= & \quad \% \quad Def.\ \mathrm{I}_{r_i^1}, p_{ri} \\
 & (\mathrm{x}, \mathrm{ar}, \mathrm{aw}, \mathbf{s}_{r_i}, \ell_{r_i^1}) = (1,0,0,0,0) \wedge (\ell_{r_i^1} \rightarrow \mathrm{aw} = 0) \\
\rightarrow & \quad \% \quad 0 \leq \sharp(j : 1 \leq j \leq M : \mathbf{s}_{w_j} = 1) \leq \mathrm{aw} \\
 & \qquad\ 0 \leq \sharp(i : 1 \leq j \leq M : \mathbf{s}_{r_i} = 1) \leq \mathrm{ar} \\
 & \mathbf{s}_{r_i} = 0 \\
 & \wedge(\sharp(j : 1 \leq j \leq M : \mathbf{s}_{w_j} = 1) = 0 \\
 & \ \vee(\sharp(j : 1 \leq j \leq M : \mathbf{s}_{w_j} = 1) = 1 \wedge \sharp(i : 1 \leq j \leq M : \mathbf{s}_{r_i} = 1) = 0)) \\
= & \quad \% \quad Def.\ \mathrm{I}_{r_i^0}, p \\
 & \mathrm{I}_{r_i^0} \wedge p
\end{array}$$

(b) **Proof 2**
Since $\mathrm{T}_{r_i^1}$ *is of the form* $\mathbf{stut}_{r_i^1} \vee \bigvee_\tau(\epsilon = \mathbf{a}_\tau \wedge trans_\tau)$ *then* $\mathrm{T}_{r_i^1} \wedge ((p_{ri} \wedge p'_{ri}) \vee \mathbf{stut}_{r_i^1})$ *is equal to* $\mathbf{stut}_{r_i^1} \vee \bigvee_\tau(\epsilon = \mathbf{a}_\tau \wedge trans_\tau \wedge p_{ri} \wedge p'_{ri})$. $\mathrm{T}_{r_i^0}$ *is of the form* $\mathbf{stut}_{r_i^0} \vee \bigvee_\tau(\epsilon = \mathbf{a}_\tau \wedge trans_\tau)$ *so* $\mathrm{T}_{r_i^0} \wedge ((p \wedge p') \vee \mathbf{stut}_0)$ *is equal to* $\mathbf{stut}_{r_i^0} \vee \bigvee_\tau(\epsilon = \mathbf{a}_\tau \wedge trans_\tau \wedge p \wedge p')$.

– $$\begin{array}{ll} & \tau_{r^1_{i,1}} \wedge p_{ri} \wedge p'_{ri} \\ = & \Big(\epsilon = \mathbf{i} \wedge \ell_{r^1_i} = 0 \wedge p_{ri} \wedge \mathrm{x} = 1 \wedge p'_{ri} \wedge \Psi'_1 = \Psi_1 \big[0, 1/\mathrm{x}, \ell_{r^1_i}\big]\Big) \\ \rightarrow & \mathbf{stut}_{r^0_i} \end{array}$$
since $\mathbf{s}_{r_i}$ *doesn't change.*

– $$\begin{array}{ll} & \tau_{r^1_{i,2}} \wedge p_{ri} \wedge p'_{ri} \\ = & \Big(\epsilon = \mathbf{i} \wedge \ell_{r^1_i} = 1 \wedge p_{ri} \wedge \mathbf{aw} = 0 \wedge p'_{ri} \wedge \Psi'_1 = \Psi_1 \big[\mathbf{ar}{+}1, 2/\mathbf{ar}, \ell_{r^1_i}\big]\Big) \\ \rightarrow & \mathbf{stut}_{r^0_i} \end{array}$$
since $\mathbf{s}_{r_i}$ *doesn't change.*

– $$\begin{array}{ll} & \tau_{r^1_{i,3}} \wedge p_{ri} \wedge p'_{ri} \\ = & \Big(\epsilon = \mathbf{i} \wedge \ell_{r^1_i} = 2 \wedge p_{ri} \wedge p'_{ri} \wedge \Psi'_1 = \Psi_1 \big[1, 1, 3/\mathbf{s}_{r_i}, \mathbf{x}, \ell_{r^1_i}\big]\Big) \\ \rightarrow & \Big(\epsilon = \mathbf{i} \wedge \mathbf{s}_{r_i} = 0 \wedge p \wedge p' \wedge \mathbf{s}'_{r_i} = 1\Big) \\ = & \tau_{r^0_{i,1}} \wedge p \wedge p' \end{array}$$
because $\ell_{r^1_i} = 1 \rightarrow \mathrm{aw} = 0$ *and* $0 \leq \sharp(j : 1 \leq j \leq M : \mathbf{s}_{w_j} = 1) \leq \mathrm{aw}$ *and* $0 \leq \sharp(i : 1 \leq i \leq N : \mathbf{s}_{r_i} = 1) \leq \mathrm{ar}$.

– $$\begin{array}{ll} & \tau_{r^1_{i,4}} \wedge p_{ri} \wedge p'_{ri} \\ = & \Big(\epsilon = \mathbf{i} \wedge \ell_{r^1_i} = 3 \wedge \mathbf{x} = 1 \wedge p_{ri} \wedge p'_{ri} \wedge \Psi'_1 = \Psi_1 \big[0, 4/\mathbf{x}, \ell_{r^1_i}\big]\Big) \\ \rightarrow & \mathbf{stut}_{r^0_i} \end{array}$$
since $\mathbf{s}_{r_i}$ *doesn't change.*

– $$\begin{array}{ll} & \tau_{r^1_{i,5}} \wedge p_{ri} \wedge p'_{ri} \\ = & \Big(\epsilon = \mathbf{i} \wedge \ell_{r^1_i} = 4 \wedge p_{ri} \wedge p'_{ri} \wedge \Psi'_1 = \Psi_1 \big[\mathbf{ar} - 1, 5/\mathbf{ar}, \ell_{r^1_i}\big]\Big) \\ \rightarrow & \mathbf{stut}_{r^0_i} \end{array}$$
since $\mathbf{s}_{r_i}$ *doesn't change.*

– $$\begin{array}{ll} & \tau_{r^1_{i,6}} \wedge p_{ri} \wedge p'_{ri} \\ & \Big(\epsilon = \mathbf{i} \wedge \ell_{r^1_i} = 5 \wedge p_{ri} \wedge p'_{ri} \wedge \Psi'_1 = \Psi_1 \big[0, 1, 0/\mathbf{s}_{r_i}, \mathbf{x}, \ell_{r^1_i}\big]\Big) \\ \rightarrow & \Big(\epsilon = \mathbf{i} \wedge \mathbf{s}_{r_i} = 1 \wedge p \wedge p' \wedge \mathbf{s}'_{r_i} = 0\Big) \\ = & \tau_{r^0_{i,2}} \wedge p \wedge p' \end{array}$$
because $0 \leq \sharp(j : 1 \leq j \leq M : \mathbf{s}_{w_j} = 1) \leq \mathrm{aw}$ *and* $0 \leq \sharp(i : 1 \leq i \leq N : \mathbf{s}_{r_i} = 1) \leq \mathrm{ar}$.

– $$\begin{array}{ll} & \tau_{r^1_{i,7}} \wedge p_{ri} \wedge p'_{ri} \\ = & \Big(\epsilon = \mathbf{e} \wedge \mathbf{x} = 1 \wedge p_{ri} \wedge p'_{ri} \wedge \Psi'_1 = \Psi_1 [0/\mathbf{x}]\Big) \\ \rightarrow & \mathbf{stut}_{r^0_i} \end{array}$$
since $\mathbf{s}_{r_i}$ *doesn't change.*

– $$\begin{array}{ll} & \tau_{r^1_{i,8}} \wedge p_{ri} \wedge p'_{ri} \\ = & \Big(\epsilon = \mathbf{e} \wedge \ell_{r^1_i} \in \{0, 3\} \wedge \mathbf{x} = 0 \wedge p_{ri} \wedge p'_{ri} \wedge \Psi'_1 = \Psi_1 [1/\mathbf{x}]\Big) \\ \rightarrow & \mathbf{stut}_{r^0_i} \end{array}$$
since $\mathbf{s}_{r_i}$ *doesn't change.*

– $\mathbf{stut}_{r^1_i} \rightarrow \mathbf{stut}_{r^0_i}$
since $\mathbf{s}_{r_i}$ *doesn't change.*

(c) $\quad \mathrm{L}_{r_i^0}$
$= \ (\Diamond\Box En(\tau_{r_{i,1}^0}) \to \Box\Diamond\tau_{r_{i,1}^0}) \wedge (\Diamond\Box En(\tau_{r_{i,2}^0}) \to \Box\Diamond\tau_{r_{i,2}^0})$
$= \ (\Diamond\Box(\epsilon = \mathbf{i} \wedge \mathtt{s}_{r_i} = 0) \to \Box\Diamond\big(\big(\epsilon = \mathbf{i} \wedge \mathtt{s}_{r_i} = 0 \wedge \mathtt{s}'_{r_i} = 1\big)\big)$

From the fact that (see Figure 3.3) transitions $\tau_{r_{i,1}^1}$ and $\tau_{r_{i,3}^1}$ are strongly fair and $\tau_{r_{i,2}^1}$ is weakly fair follows that $(\Diamond\Box En(\tau_{r_{i,1}^0}) \to \Box\Diamond\tau_{r_{i,1}^0})$, i.e., $\tau_{r_{i,1}^0}$ is weakly fair. From the fact that (see Figure 3.3) transitions $\tau_{r_{i,4}^1}$ and $\tau_{r_{i,6}^1}$ are strongly fair and $\tau_{r_{i,5}^1}$ is weakly fair follows that $(\Diamond\Box En(\tau_{r_{i,2}^0}) \to \Box\Diamond\tau_{r_{i,2}^0})$, i.e., $\tau_{r_{i,2}^0}$ is weakly fair.

ad (2) Analogue to the proof of (1).

ad (3) This is trivial because $\mathrm{W}_1 \leftrightarrow (\bigwedge_{i=1}^{N} \mathrm{W}_{r_i^1} \wedge \bigwedge_{j=1}^{M} \mathrm{W}_{w_j^1})$.

3.4 The second development step

As seen in section 3.3 the first implementation can generate deadlocked sequences. In this step we change the components of the first implementation in such a way that deadlock inside a PV-section is not possible anymore. This is the same as is done by Dijkstra: he massages reader$_i^1$ and writer$_j^1$ into reader$_j^2$ and writer$_j^2$ so that no deadlocked sequences inside a PV-section are generated any more.

One such deadlocked sequence generated by the first implementation is as follows: suppose reader$_i^1$ has gained the access-right for the shared variables (first PV-segment) and suppose **aw** $= 1$ (a writer is executing `WRITE`). Then reader$_i^1$ can never increase **ar** by 1, i.e., reader$_i^1$ has deadlocked.

Dijkstra uses the split binary semaphore technique to prevent programs from becoming deadlocked inside a PV-section. The idea is that we must prevent programs from getting the access-right (get into a PV-section) for the shared variables if we know that they can not give it back (get deadlocked inside a PV-section). For reader$_i^1$ this means: never let it enter the first PV-section if `aw` does not equal zero. For writer$_j^1$ this means: never let it enter the first PV-section if `aw` or `ar` does not equal zero. Reader$_i^1$ and writer$_j^1$ never block in their second PV-section.
How does one prevent that reader$_i^1$ gets deadlocked inside a PV-section? This is done as follows: reader$_i^1$ chooses, when it gives the access-right back, who can have it thereafter. reader$_i^1$ executes therefore the following piece of program as replacement for `V(mx)`:

```
CHOOSE: if true → V(m) [] aw=0 → V(r) [] aw=0 ∧ ar=0 → V(w) fi
```

We have to split semaphore `mx` in three pieces. If `aw` equals zero then a reader is allowed to enter its first PV-section, i.e., this PV-section is not guarded by `P(mx)` but by `P(r)`. We do this substitution for all PV-sections of reader$_i^1$ and writer$_j^1$. So we have replaced `mx` by three other binary semaphores.
What is the initial value of these semaphores? If they all have initial value 1 then more than one program can have access-right to the shared variables, i.e., only one has initial

value 1. Semaphore `r` can not have initial value 1 because if no reader wants to execute `READ` then no writer can execute `WRITE`. The same holds for semaphore `w`. Thus `m` has initial value 1. But then no reader or writer can enter the first PV-section. The solution of this problem is that we insert a PV-section (`P(m);CHOOSE`) at front of the first one. This is in short what Dijkstra does to prevent that reader$_i^1$ and writer$_j^1$ get deadlocked inside a PV-section. The result of this transformation is:

```
reader_i^2:
          do true → NCS;
                    P(m);CHOOSE;
                    P(r);ar:=ar+1;CHOOSE;
                    READ;
                    P(m);ar:=ar-1;CHOOSE
          od
writer_j^2:
          do true → NCS;
                    P(m);CHOOSE;
                    P(w);aw:=aw+1;CHOOSE;
                    WRITE;
                    P(m);aw:=aw-1;CHOOSE
          od
```

$\mathtt{Syn}^2 \;:\; \|_{i=1}^{N}\ \mathtt{reader}_i^2 \;\|\; \|_{j=1}^{M}\ \mathtt{writer}_j^2$

$\mathtt{Syn}^2$ generates no sequences that can deadlock inside a PV-section. But $\mathtt{Syn}^2$ can generate sequences that can deadlock outside these sections, e.g. initially a reader$_i^2$ can choose for a `V(w)` operation, and get blocked by a `P(r)` operation. Then no other reader or writer can enter the first PV-section because semaphore `m` equals zero.

In the following sections the DTL machine specifications $\mathcal{S}_{r_i^2}$ (corresponding to program reader$_i^2$) and $\mathcal{S}_{w_j^2}$ (corresponding to program writer$_j^2$), and the extra requirement W_2, excluding computations that deadlock outside PV-sections, are given.

3.4.1 Specification $\mathcal{S}_{r_i^2}$

The formal specification $\mathcal{S}_{r_i^2} \triangleq (B_{r_i^2}, \mathrm{H}_{r_i^2})$ where $\mathrm{H}_{r_i^2} \triangleq \mathrm{I}_{r_i^2} \wedge \Box\mathrm{T}_{r_i^2} \wedge \mathrm{L}_{r_i^2}$ and $B_{r_i^2}$, $\mathrm{I}_{r_i^2}$, $\mathrm{T}_{r_i^2}$ and $\mathrm{L}_{r_i^2}$ are as follows:

1. **Basis** $B_{r_i^2} = ((\mathrm{In}_{r_i^2}, \mathrm{Out}_{r_i^2}), (\mathrm{V}_{r_i^2}, \mathrm{X}_{r_i^2}))$

$$
\begin{aligned}
\mathrm{In}_{r_i^2} &\triangleq \emptyset, \\
\mathrm{Out}_{r_i^2} &\triangleq \emptyset, \\
\mathrm{V}_{r_i^2} &\triangleq \{\mathbf{m}, \mathbf{r}, \mathbf{w}, \mathbf{ar}, \mathbf{aw}, \mathrm{s}_{r_i}\}, \\
\mathrm{X}_{r_i^2} &\triangleq \{\ell_{r_i^2}\}
\end{aligned}
$$

- $\ell_{r_i^2} = 0$: reader$_i^2$ is non critical.

- $\ell_{r_i^2} = 6$: reader$_i^2$ has executed first P-action on $\mathbf{m}$.
- $\ell_{r_i^2} = 7$: reader$_i^2$ has executed first `CHOOSE`.
- $\ell_{r_i^2} = 1$: reader$_i^2$ has executed P-action on $\mathbf{r}$.
- $\ell_{r_i^2} = 2$: reader$_i^2$ has increased $\mathbf{ar}$ by 1.
- $\ell_{r_i^2} = 3$: reader$_i^2$ is critical.
- $\ell_{r_i^2} = 4$: reader$_i^2$ has executed second P-action on $\mathbf{m}$.
- $\ell_{r_i^2} = 5$: reader$_i^2$ has decreased $\mathbf{ar}$ by 1.

Let $\Psi_2 \triangleq (\mathbf{m}, \mathbf{r}, \mathbf{w}, \mathbf{ar}, \mathbf{aw}, \mathrm{s}_{r_i}, \ell_{r_i^2})$ and $\Psi_2' \triangleq (\mathbf{m}', \mathbf{r}', \mathbf{w}', \mathbf{ar}', \mathbf{aw}', \mathrm{s}_{r_i}', \ell_{r_i^2}')$.

2. **Initial States:**

$$\mathrm{I}_{r_i^2} \triangleq \Psi_2 = (1, 0, 0, 0, 0, 0, 0)$$

3. **Transitions:**

Let $CHO(X) \triangleq \begin{array}{l} \vee \;\; \Psi_2' = \Psi_2 \left[1, X/\mathbf{m}, \ell_{r_i^2}\right] \\ \vee \;\; (\mathbf{aw} = 0 \wedge \Psi_2' = \Psi_2 \left[1, X/\mathbf{r}, \ell_{r_i^2}\right]) \\ \vee \;\; (\mathbf{aw} = 0 \wedge \mathbf{ar} = 0 \wedge \Psi_2' = \Psi_2 \left[1, X/\mathbf{w}, \ell_{r_i^2}\right]) \end{array}$

$\mathrm{T}_{r_i^2} \triangleq$

$\tau_{r_{i,1}^2}$ $\quad \left(\epsilon = \mathbf{i} \wedge (\ell_{r_i^2}, \mathbf{m}) = (0, 1) \wedge \Psi_2' = \Psi_2 \left[0, 6/\mathbf{m}, \ell_{r_i^2}\right]\right)$

Reader$_i^2$ executes its first P-action on $\mathbf{m}$.

$\tau_{r_{i,2}^2}$ $\quad \vee \; \left(\epsilon = \mathbf{i} \wedge \ell_{r_i^2} = 6 \wedge CHO(7)\right)$

Reader$_i^2$ executes the first `CHOOSE`.

$\tau_{r_{i,3}^2}$ $\quad \vee \; \left(\epsilon = \mathbf{i} \wedge (\ell_{r_i^2}, \mathbf{r}) = (7, 1) \wedge \Psi_2' = \Psi_2 \left[0, 1/\mathbf{r}, \ell_{r_i^2}\right]\right)$

Reader$_i^2$ executes P-action on $\mathbf{r}$.

$\tau_{r_{i,4}^2}$ $\quad \vee \; \left(\epsilon = \mathbf{i} \wedge \ell_{r_i^2} = 1 \wedge \Psi_2' = \Psi_2 \left[\mathbf{ar} + 1, 2/\mathbf{ar}, \ell_{r_i^2}\right]\right)$

Reader$_i^2$ increases the number of active readers by one.

$\tau_{r_{i,5}^2}$ $\quad \vee \; \left(\epsilon = \mathbf{i} \wedge \ell_{r_i^2} = 2 \wedge CHO(3) \wedge \Psi_2' = \Psi_2 \left[1/\mathrm{s}_{r_i}\right]\right)$

Reader$_i^2$ becomes critical.

$\tau_{r_{i,6}^2}$ $\quad \vee \; \left(\epsilon = \mathbf{i} \wedge (\ell_{r_i^2}, \mathbf{m}) = (3, 1) \wedge \Psi_2' = \Psi_2 \left[0, 4/\mathbf{m}, \ell_{r_i^2}\right]\right)$

Reader$_i^2$ executes the second P-action on $\mathbf{m}$.

$\tau_{r_{i,7}^2}$ $\quad \vee \; \left(\epsilon = \mathbf{i} \wedge \ell_{r_i^2} = 4 \wedge \Psi_2' = \Psi_2 \left[\mathbf{ar} - 1, 5/\mathbf{ar}, \ell_{r_i^2}\right]\right)$

Reader$_i^2$ decreases the number of active readers by one.

$\tau_{r_{i,8}^2}$ $\quad \vee \; \left(\epsilon = \mathbf{i} \wedge \ell_{r_i^2} = 5 \wedge CHO(0) \wedge \Psi_2' = \Psi_2 \left[0/\mathrm{s}_{r_i}\right]\right)$

Reader$_i^2$ becomes non critical.

$\tau_{r^2_{i,9}} \quad \vee \ \left(\epsilon = \mathbf{e} \wedge \mathbf{m} = 1 \wedge \Psi_2' = \Psi_2\,[0/\mathbf{m}]\right)$
The environment executes a P-operation on $\mathbf{m}$.

$\tau_{r^2_{i,10}} \quad \vee \ \left(\epsilon = \mathbf{e} \wedge \mathbf{r} = 1 \wedge \Psi_2' = \Psi_2\,[0/\mathbf{r}]\right)$
The environment executes a P-operation on $\mathbf{r}$.

$\tau_{r^2_{i,11}} \quad \vee \ \left(\epsilon = \mathbf{e} \wedge \mathbf{w} = 1 \wedge \Psi_2' = \Psi_2\,[0/\mathbf{w}]\right)$
The environment executes a P-operation on $\mathbf{w}$.

$\tau_{r^2_{i,12}} \quad \vee \ \left(\epsilon = \mathbf{e} \wedge \ell_{r^2_i} \in \{0,7,3\} \wedge \mathbf{m} = 0 \wedge \Psi_2' = \Psi_2\,[1/\mathbf{m}]\right)$
The environment executes a V-operation on $\mathbf{m}$.

$\tau_{r^2_{i,13}} \quad \vee \ \left(\epsilon = \mathbf{e} \wedge \ell_{r^2_i} \in \{0,7,3\} \wedge \mathbf{r} = 0 \wedge \Psi_2' = \Psi_2\,[1/\mathbf{r}]\right)$
The environment executes a V-operation on $\mathbf{r}$.

$\tau_{r^2_{i,14}} \quad \vee \ \left(\epsilon = \mathbf{e} \wedge \ell_{r^2_i} \in \{0,7,3\} \wedge \mathbf{w} = 0 \wedge \Psi_2' = \Psi_2\,[1/\mathbf{w}]\right)$
The environment executes a V-operation on $\mathbf{w}$.

$\tau_{r^2_{i,0}} \quad \vee \ \mathbf{stut}_{r^2_i}$

These transitions are illustrated in figure 3.5

4. **Liveness**
$\mathrm{L}_{r^2_i}$ expresses that the P- and V-operations on the semaphores $\mathbf{m}$, $\mathbf{r}$ and $\mathbf{w}$ are strongly fair and all the other transitions are weakly fair.
Let $\mathrm{WF}_{r^2_i} \triangleq \{\tau_{r^2_{i,k}} \mid k \in \{4,7\}\}$ and
$\mathrm{SF}_{r^2_i} \triangleq \{\tau_{r^2_{i,k}} \mid k \in \{1,2,3,5,6,8,9,10,11,12,13,14\}\}$ then

$$\mathrm{L}_{r^2_i} \triangleq \bigwedge_{\tau \in \mathrm{WF}_{r^2_i}} (\Diamond\Box En(\tau) \rightarrow \Box\Diamond\tau) \wedge \bigwedge_{\tau \in \mathrm{SF}_{r^2_i}} (\Box\Diamond En(\tau) \rightarrow \Box\Diamond\tau)$$

3.4.2 Specification $\mathcal{S}_{w^2_j}$

The formal specification $\mathcal{S}_{w^2_j} \triangleq (B_{w^2_j}, \mathrm{H}_{w^2_j})$ where $\mathrm{H}_{w^2_j} \triangleq \mathrm{I}_{w^2_j} \wedge \Box\mathrm{T}_{w^2_j} \wedge \mathrm{L}_{w^2_j}$ and $B_{w^2_j}$, $\mathrm{I}_{w^2_j}$, $\mathrm{T}_{w^2_j}$ and $\mathrm{L}_{w^2_j}$ are as follows:

1. **Basis** $B_{w^2_j} = ((\mathrm{In}_{w^2_j}, \mathrm{Out}_{w^2_j}), (\mathrm{V}_{w^2_j}, \mathrm{X}_{w^2_j}))$

$$\begin{array}{lcl} \mathrm{In}_{w^2_j} & \triangleq & \emptyset, \\ \mathrm{Out}_{w^2_j} & \triangleq & \emptyset, \\ \mathrm{V}_{w^2_j} & \triangleq & \{\mathbf{m}, \mathbf{r}, \mathbf{w}, \mathbf{ar}, \mathbf{aw}, \mathbf{s}_{w_j}\}, \\ \mathrm{X}_{w^2_j} & \triangleq & \{\ell_{w^2_j}\} \end{array}$$

- $\ell_{w^2_j} = 0$: writer^2_j is non critical.
- $\ell_{w^2_j} = 6$: writer^2_j has executed first P-action on $\mathbf{m}$.

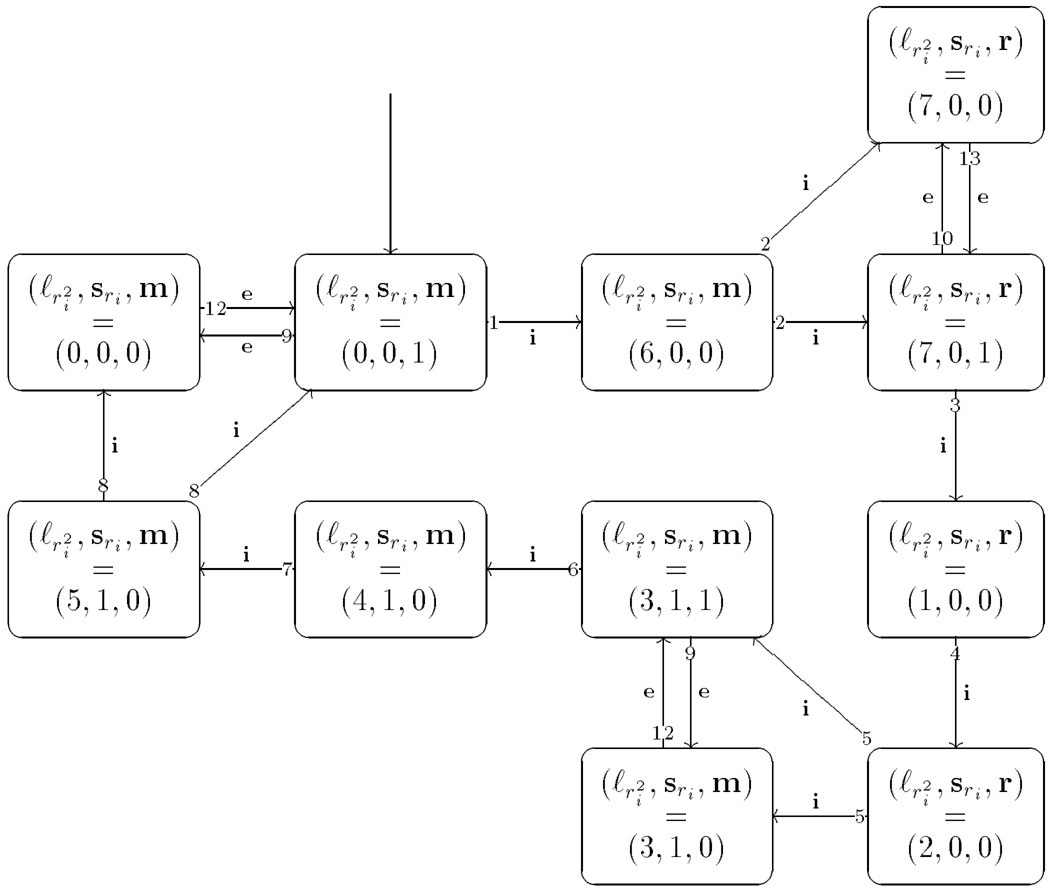

Figure 3.5: Transitions of reader$_i^2$.

- $\ell_{w_j^2} = 7$: writer$_i^2$ has executed first `CHOOSE`.
- $\ell_{w_j^2} = 1$: writer$_i^2$ has executed P-action on $\mathbf{w}$.
- $\ell_{w_j^2} = 2$: writer$_i^2$ has increased $\mathbf{aw}$ by 1.
- $\ell_{w_j^2} = 3$: writer$_i^2$ is critical.
- $\ell_{w_j^2} = 4$: writer$_i^2$ has executed second P-action on $\mathbf{m}$.
- $\ell_{w_j^2} = 5$: writer$_i^2$ has decreased $\mathbf{aw}$ by 1.

Let $\Psi_2 \triangleq (\mathbf{m}, \mathbf{r}, \mathbf{w}, \mathbf{ar}, \mathbf{aw}, \mathrm{s}_{w_j}, \ell_{w_j^2})$ and $\Psi_2' \triangleq (\mathbf{m}', \mathbf{r}', \mathbf{w}', \mathbf{ar}', \mathbf{aw}', \mathrm{s}_{w_j}', \ell_{w_j^2}')$.

2. **Initial States:**

$$\mathrm{I}_{w_j^2} \triangleq \Psi_2 = (1,0,0,0,0,0,0)$$

3. **Transitions:**

Let $CHO(X) \triangleq$ $\vee$ $\Psi'_2 = \Psi_2\left[1, X/\mathbf{m}, \ell_{w_j^2}\right]$
$\vee$ $(\mathbf{aw} = 0 \wedge \Psi'_2 = \Psi_2\left[1, X/\mathbf{r}, \ell_{w_j^2}\right])$
$\vee$ $(\mathbf{aw} = 0 \wedge \mathbf{ar} = 0 \wedge \Psi'_2 = \Psi_2\left[1, X/\mathbf{w}, \ell_{w_j^2}\right])$

$\mathrm{T}_{w_j^2} \triangleq$

$\tau_{w^2_{j,1}}$ $\left(\epsilon = \mathbf{i} \wedge (\ell_{w_j^2}, \mathbf{m}) = (0,1) \wedge \Psi'_2 = \Psi_2\left[0, 6/\mathbf{m}, \ell_{w_j^2}\right]\right)$
Writer$_j^2$ executes its first P-action on $\mathbf{m}$.

$\tau_{w^2_{j,2}}$ $\vee$ $\left(\epsilon = \mathbf{i} \wedge \ell_{w_j^2} = 6 \wedge CHO(7)\right)$
Writer$_j^2$ executes the first `CHOOSE`.

$\tau_{w^2_{j,3}}$ $\vee$ $\left(\epsilon = \mathbf{i} \wedge (\ell_{w_j^2}, \mathbf{w}) = (7,1) \wedge \Psi'_2 = \Psi_2\left[0, 1/\mathbf{w}, \ell_{w_j^2}\right]\right)$
Writer$_j^2$ executes P-action on $\mathbf{w}$.

$\tau_{w^2_{j,4}}$ $\vee$ $\left(\epsilon = \mathbf{i} \wedge \ell_{w_j^2} = 1 \wedge \Psi'_2 = \Psi_2\left[\mathbf{aw} + 1, 2/\mathbf{aw}, \ell_{w_j^2}\right]\right)$
Writer$_j^2$ increases the number of active writers by one.

$\tau_{w^2_{j,5}}$ $\vee$ $\left(\epsilon = \mathbf{i} \wedge \ell_{w_j^2} = 2 \wedge CHO(3) \wedge \Psi'_2 = \Psi_2\left[1/\mathbf{s}_{w_j}\right]\right)$
Writer$_j^2$ becomes critical.

$\tau_{w^2_{j,6}}$ $\vee$ $\left(\epsilon = \mathbf{i} \wedge (\ell_{w_j^2}, \mathbf{m}) = (3,1) \wedge \Psi'_2 = \Psi_2\left[0, 4/\mathbf{m}, \ell_{w_j^2}\right]\right)$
Writer$_j^2$ executes the second P-action on $\mathbf{m}$.

$\tau_{w^2_{j,7}}$ $\vee$ $\left(\epsilon = \mathbf{i} \wedge \ell_{w_j^2} = 4 \wedge \Psi'_2 = \Psi_2\left[\mathbf{aw} - 1, 5/\mathbf{aw}, \ell_{w_j^2}\right]\right)$
Writer$_j^2$ decreases the number of active writers by one.

$\tau_{w^2_{j,8}}$ $\vee$ $\left(\epsilon = \mathbf{i} \wedge \ell_{w_j^2} = 5 \wedge CHO(0) \wedge \Psi'_2 = \Psi_2\left[0/\mathbf{s}_{w_j}\right]\right)$
Writer$_j^2$ becomes non critical.

$\tau_{w^2_{j,9}}$ $\vee$ $\left(\epsilon = \mathbf{e} \wedge \mathbf{m} = 1 \wedge \Psi'_2 = \Psi_2\left[0/\mathbf{m}\right]\right)$
The environment executes a P-operation on $\mathbf{m}$.

$\tau_{w^2_{j,10}}$ $\vee$ $\left(\epsilon = \mathbf{e} \wedge \mathbf{r} = 1 \wedge \Psi'_2 = \Psi_2\left[0/\mathbf{r}\right]\right)$
The environment executes a P-operation on $\mathbf{r}$.

$\tau_{w^2_{j,11}}$ $\vee$ $\left(\epsilon = \mathbf{e} \wedge \mathbf{w} = 1 \wedge \Psi'_2 = \Psi_2\left[0/\mathbf{w}\right]\right)$
The environment executes a P-operation on $\mathbf{w}$.

$\tau_{w^2_{j,12}}$ $\vee$ $\left(\epsilon = \mathbf{e} \wedge \ell_{w_j^2} \in \{0,7,3\} \wedge \mathbf{m} = 0 \wedge \Psi'_2 = \Psi_2\left[1/\mathbf{m}\right]\right)$
The environment executes a V-operation on $\mathbf{m}$.

$\tau_{w^2_{j,13}}$ $\vee$ $\left(\epsilon = \mathbf{e} \wedge \ell_{w_j^2} \in \{0,7,3\} \wedge \mathbf{r} = 0 \wedge \Psi'_2 = \Psi_2\left[1/\mathbf{r}\right]\right)$
The environment executes a V-operation on $\mathbf{r}$.

$\tau_{w^2_{j,14}}$ $\vee$ $\left(\epsilon = \mathbf{e} \wedge \ell_{w_j^2} \in \{0,7,3\} \wedge \mathbf{w} = 0 \wedge \Psi'_2 = \Psi_2\left[1/\mathbf{w}\right]\right)$
The environment executes a V-operation on $\mathbf{w}$.

$\tau_{w^2_{j,0}} \quad \vee\ \mathbf{stut}_{w^2_j}$

These transitions are illustrated in figure 3.6

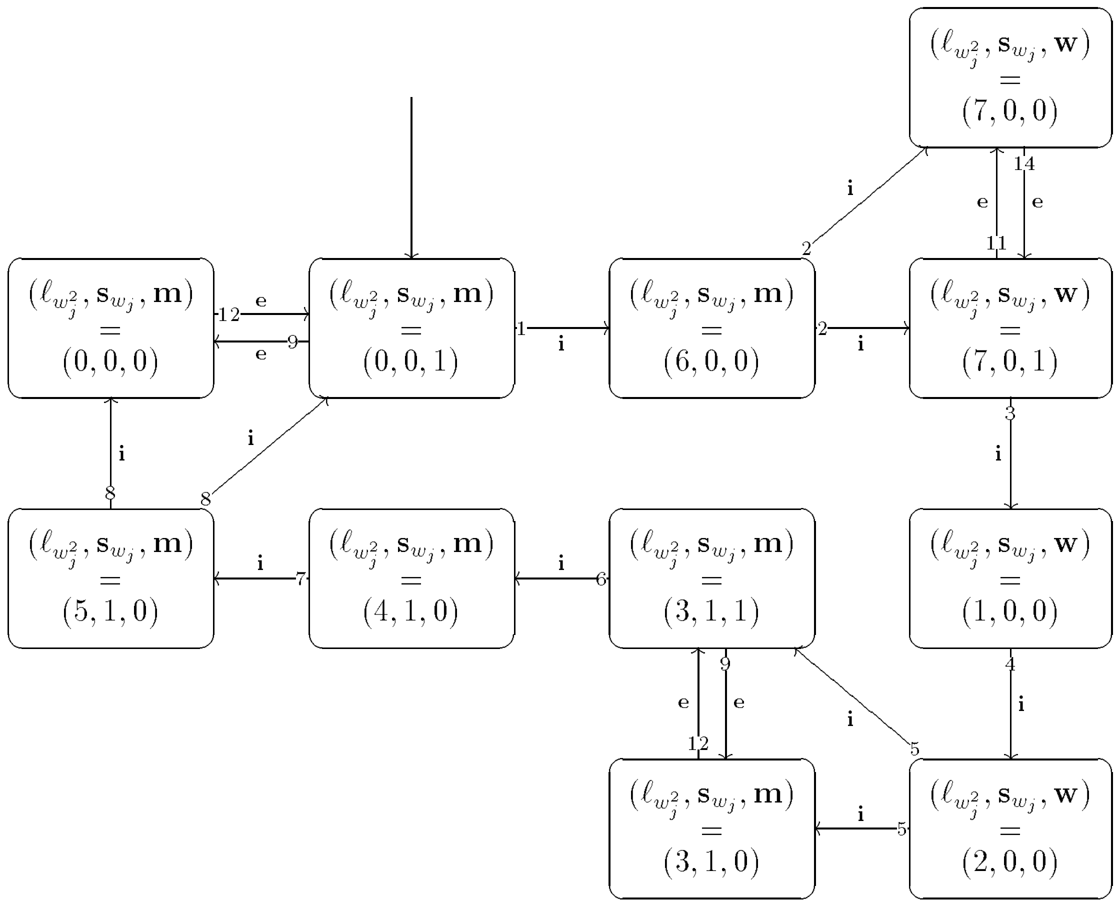

Figure 3.6: Transitions of writer^2_j.

4. **Liveness:**
   $\mathrm{L}_{w^2_j}$ expresses that the P- and V-operations on the semaphores $\mathbf{m}$, $\mathbf{r}$ and $\mathbf{w}$ are strongly fair and all the other transitions are weakly fair.
   Let $\mathrm{WF}_{w^2_j} \triangleq \{\tau_{w^2_{j,k}} \mid k \in \{4,7\}\}$ and
   $\mathrm{SF}_{w^2_i} \triangleq \{\tau_{w^2_{j,k}} \mid k \in \{1,2,3,5,6,8,9,10,11,12,13,14\}\}$ then

$$\mathrm{L}_{w^2_j} \triangleq \bigwedge_{\tau \in \mathrm{WF}_{w^2_j}} (\Diamond\Box En(\tau) \rightarrow \Box\Diamond\tau) \wedge \bigwedge_{\tau \in \mathrm{SF}_{w^2_j}} (\Box\Diamond En(\tau) \rightarrow \Box\Diamond\tau)$$

3.4.3 Requirement W_2

W_2 should express that reader^2_i and writer^2_j executes `CHOOSE` in such a way that no deadlocked computations are generated, i.e.,

- a `V(m)` is executed if the number of readers and writers that are bound to execute a `P(m)` is greater than zero,
- a `V(r)` is executed if the number of readers that are bound to execute a `P(r)` is greater than zero,
- a `V(w)` is executed if the number of writers that are bound to execute a `P(w)` is greater than zero.

Let q be defined as

$$\begin{array}{ll} & (\mathbf{m} = 1 \wedge \sharp(k : 1 \leq k \leq N : \ell_{r_k^2} \in \{0,1,2,3,4,5\}) + \\ & \quad \sharp(n : 1 \leq n \leq M : \ell_{w_n^2} \in \{0,1,2,3,4,5\}) > 0) \\ \vee & (\mathbf{r} = 1 \wedge \mathbf{aw} = 0 \wedge \sharp(k : 1 \leq k \leq N : \ell_{r_k^2} \in \{6,7\}) > 0) \\ \vee & (\mathbf{w} = 1 \wedge \mathbf{aw} = 0 \wedge \mathbf{ar} = 0 \wedge \sharp(n : 1 \leq n \leq M : \ell_{w_n^2} \in \{6,7\}) > 0) \end{array}$$

Then W_2 is as follows

$$\mathrm{W}_2 \triangleq \Box\left((\bigwedge_{i=1}^{N} \ell_{r_i^2} \in \{0,7,3\} \rightarrow q) \wedge (\bigwedge_{j=1}^{M} \ell_{w_j^2} \in \{0,7,3\} \rightarrow q) \right)$$

The same construction as in the previous development step is used to write this down as a machine. Let $p_2 \triangleq (\bigwedge_{i=1}^{N} \ell_{r_i^2} \in \{0,7,3\} \rightarrow q) \wedge (\bigwedge_{j=1}^{M} \ell_{w_j^2} \in \{0,7,3\} \rightarrow q)$ then $\mathrm{W}_2 = p_2 \wedge \Box((p_2 \wedge p_2') \vee \mathbf{stut}_2)$. Again the liveness part of W_2 equals **true**.

3.4.4 $\mathcal{S}_2$ relatively refines $\mathcal{S}_1$

Since the semaphore **x** and the shared variables **ar** and **aw** are used only by the subcomponents of $\mathcal{S}_1$ and the semaphores **m**, **w** and **r** and the shared variables **ar** and **aw** only by the subcomponents of $\mathcal{S}_2$, we should prove $\mathcal{S}_2 \restriction \{\mathbf{m},\mathbf{w},\mathbf{r},\mathbf{ar},\mathbf{aw}\}$ relatively refines $\mathcal{S}_1 \restriction \{\mathbf{x},\mathbf{ar},\mathbf{aw}\}$. According to definition 35, 36 and theorem 8 $\mathcal{S}_2 \restriction \{\mathbf{m},\mathbf{r},\mathbf{w},\mathbf{ar},\mathbf{aw}\}$ relatively refines $\mathcal{S}_1 \restriction \{\mathbf{x},\mathbf{ar},\mathbf{aw}\}$ with respect to $(\mathrm{W}_2, \mathrm{W}_1)$ iff the following holds:

$$\begin{array}{l} \mathfrak{D}(B_2) = \mathfrak{D}(B_1) \text{ and} \\ \models (\exists \mathrm{X}_2 \,.\, (\mathrm{G}_2 \wedge (\epsilon = \mathbf{e} \Rightarrow (\mathrm{m},\mathbf{r},\mathbf{w},\mathrm{ar},\mathrm{aw})' = (\mathrm{m},\mathbf{r},\mathbf{w},\mathrm{ar},\mathrm{aw})))) \\ \;\rightarrow \\ \;(\exists \mathrm{X}_1 \,.\, (\mathrm{G}_1 \wedge (\epsilon = \mathbf{e} \Rightarrow (\mathrm{x},\mathrm{ar},\mathrm{aw})' = (\mathrm{x},\mathrm{ar},\mathrm{aw})))) \end{array}$$

where X_2 are the local variables from $\mathcal{S}_2$, i.e., $\mathrm{X}_2 \triangleq \{\ell_{r_i^2} \mid i = 1,\ldots,N\} \cup \{\ell_{w_j^2} \mid j = 1,\ldots,M\} \cup \{\mathrm{m},\mathbf{r},\mathbf{w},\mathrm{aw},\mathrm{ar}\}$ and G_2 is the composition of $\mathcal{S}_{r_i^2}$ $(i = 1,\ldots,N)$ and $\mathcal{S}_{w_j^2}$ $(j = 1,\ldots,M)$ and W_2,
let $\bar{\epsilon}_2 \triangleq e_{2,1},\ldots,\epsilon_{2,N},\epsilon_{2,N+1},\ldots,\epsilon_{2,N+M}$, and
let $\bar{B}_2^A \triangleq B^A_{r_1^2},\ldots,B^A_{r_N^2},B^A_{w_1^2},\ldots,B^A_{w_M^2}$
then $\mathrm{G}_2 \triangleq$

$$\left(\exists \bar{\epsilon}_2 .\, \odot_{\bar{B}_2^A}(\epsilon,\bar{\epsilon}_2) \wedge \bigwedge_{i=1}^{N} \mathrm{H}_{r_i^2}[\epsilon_{2,i}/\epsilon] \wedge \bigwedge_{j=1}^{M} \mathrm{H}_{w_j^2}[\epsilon_{2,N+j}/\epsilon]\right) \wedge \mathrm{W}_2$$

X_1 are the local variables from $\mathcal{S}_1$, i.e., $X_1 \triangleq \{\ell_{r_i^1} \mid i = 1,\dots,N\} \cup \{\ell_{w_j^1} \mid j = 1,\dots,M\} \cup \{\mathbf{x},\mathbf{ar},\mathbf{aw}\}$ and G_1 is the composition of $\mathcal{S}_{r_i^1}$ $(i = 1,\dots,N)$ and $\mathcal{S}_{w_j^1}$ $(j = 1,\dots,M)$ and W_1,
let $\bar{\epsilon}_1 \triangleq \epsilon_{1,1},\dots,\epsilon_{1,N},\epsilon_{1,N+1},\dots,\epsilon_{1,N+M}$, and
let $\bar{B}_1^A \triangleq B_{r_1^1}^A,\dots,B_{r_N^1}^A,B_{w_1^1}^A,\dots,B_{w_M^1}^A$
then $G_1 \triangleq$

$$\left(\exists\bar{\epsilon}_1.\odot_{\bar{B}_1^A}(\epsilon,\bar{\epsilon}_1)\wedge\bigwedge_{i=1}^N \mathrm{H}_{r_i^1}[\epsilon_{1,i}/\epsilon]\wedge\bigwedge_{j=1}^M \mathrm{H}_{w_j^1}[\epsilon_{1,N+j}/\epsilon]\right)\wedge \mathrm{W}_1$$

As seen in the previous development step W_1 is ϵ-free and can be decomposed into sub-requirements $W_{r_i^1}$ and $W_{w_j^1}$ $(i = 1,\dots,N$ and $j = 1,\dots,M)$. W_2 however can't be decomposed into sub-requirements but it is ϵ-free. Now Lemma 9, 10 and 11 can be used for the proof, i.e., following proof rule can be used

$$\begin{array}{ll}
\bigotimes_{i=1}^N H_{r_i^1}\otimes\bigotimes_{j=1}^M H_{w_j^1}\bigcap W_2\subseteq & \\
\quad\bigotimes_{i=1}^N (H_{r_i^1}\cap W_2)\otimes\bigotimes_{j=1}^M (H_{w_j^1}\cap W_2) & \\
\bigcap_{i=1}^N W_{r_i^1}\cap\bigcap_{j=1}^M W_{w_j^1}\subseteq W_1 & W_{r_i^1}\text{ constraining }B_{r_i^1} \\
\mathcal{S}_{r_i^2}\ {}_{W_2}\mathbf{ref}^{W_{r_i^1}}\ \mathcal{S}_{r_i^1} & W_{w_j^1}\text{ constraining }B_{w_j^1} \\
\mathcal{S}_{w_j^2}\ {}_{W_2}\mathbf{ref}^{W_{w_j^1}}\ \mathcal{S}_{w_j^1} & \\
\hline
\mathcal{S}_2\ {}_{W_2}\mathbf{ref}^{W_1}\ \mathcal{S}_1 &
\end{array}$$

This means we have to prove for $i = 1,\dots,N$ and $j = 1,\dots,M$:

(1) $\left(\exists X_{r_i^2}.(\mathrm{H}_{r_i^2}\wedge \mathrm{W}_2)\right)\rightarrow\left(\exists X_{r_i^1}.(\mathrm{H}_{r_i^1}\wedge \mathrm{W}_{r_i^1})\right)$

(2) $\left(\exists X_{w_j^2}.(\mathrm{H}_{w_j^2}\wedge \mathrm{W}_2)\right)\rightarrow\left(\exists X_{w_j^1}.(\mathrm{H}_{w_j^1}\wedge \mathrm{W}_{w_j^1})\right)$

(3) $(\mathrm{W}_{r_i^1}\wedge \mathrm{W}_{w_j^1})\rightarrow \mathrm{W}_1$

(4) $(\exists\bar{\epsilon}_2.\odot_{\bar{B}_2^A}(\epsilon,\bar{\epsilon}_2)\wedge\bigwedge_{i=1}^N \mathrm{H}_{r_i^2}[\epsilon_{2,i}/\epsilon]\wedge\bigwedge_{j=1}^M \mathrm{H}_{w_j^2}[\epsilon_{2,N+j}/\epsilon])\wedge \mathrm{W}_2$
$\rightarrow$
$(\exists\bar{\epsilon}_2.\odot_{\bar{B}_2^A}(\epsilon,\bar{\epsilon}_2)\wedge\bigwedge_{i=1}^N(\mathrm{H}_{r_i^2}\wedge \mathrm{W}_2)[\epsilon_{2,i}/\epsilon]\wedge\bigwedge_{j=1}^M(\mathrm{H}_{w_j^2}\wedge \mathrm{W}_2)[\epsilon_{2,N+j}/\epsilon])$

ad (1) Rule 3 will be used to prove (1). This means one has to prove (a), (b) and (c) below, for $\bar{f}$ the refinement mapping from $\mathcal{S}_2$ to $\mathcal{S}_1$, defined as: $\bar{f} = f_{\mathrm{x}}, f_{\ell_{r_i^1}}, f_{\mathrm{ar}}, f_{\mathrm{aw}}$ where $f_{\ell_{r_i^1}}$ is defined as

$$\begin{array}{l}
if \\
\quad\begin{array}{lll}
\ell_{r_i^2}=6 & then & \ell_{r_i^2}-6 \\
\ell_{r_i^2}=7 & then & \ell_{r_i^2}-7 \\
\ell_{r_i^2}\neq 6\wedge\ell_{r_i^2}\neq 7 & then & \ell_{r_i^2}
\end{array} \\
fi
\end{array}$$

and f_{x} is defined as

$$\begin{array}{l}
if \\
\quad\begin{array}{lll}
\ell_{r_i^2}=6 & then & \mathrm{m}-1 \\
\ell_{r_i^2}\neq 6 & then & \mathrm{m}+\mathrm{r}+\mathrm{w}
\end{array} \\
fi
\end{array}$$

, i.e., the first PV-section is stuttering and semaphore x is split into semaphores m, r and w. Note: the refinement mappings for aw and ar are equal to the identity mapping, so we can leave them out.

$$
\begin{array}{lll}
(a) & \mathcal{S}_2 \cap Hist(\mathrm{W}_2) \models & (\mathrm{I}_{r_i^2} \wedge p_2) \rightarrow (\mathrm{I}_{r_i^1} \wedge p_{ri}) \left[\bar{f}/\mathrm{X}_1\right] \\
(b) & \mathcal{S}_2 \cap Hist(\mathrm{W}_2) \models & \mathrm{T}_{r_i^2} \wedge ((p_2 \wedge p_2') \vee \mathbf{stut}_2) \\
 & & \rightarrow (\mathrm{T}_{r_i^1} \wedge ((p_{ri} \wedge p_{ri}') \vee \mathbf{stut}_{r_i^1})) \left[\bar{f}/\mathrm{X}_1\right] \\
(c) & \mathcal{S}_2 \cap Hist(\mathrm{W}_2) \models & \mathrm{L}_{r_i^1} \left[\bar{f}/\mathrm{X}_1\right]
\end{array}
$$

(a) **Proof 3**

$$
\begin{array}{ll}
 & \mathrm{I}_{r_i^2} \wedge p_2 \\
= & \quad \% \quad Def.\ \mathrm{I}_{r_i^2} \\
 & (\mathrm{m}, \mathrm{r}, \mathrm{w}, \mathrm{ar}, \mathrm{aw}, \mathbf{s}_{r_i}, \ell_{r_i^2}) = (1,0,0,0,0,0,0) \\
\rightarrow & \quad \% \quad Def.\ f_{\mathrm{x}}, f_{\ell_{r_i^1}} \\
 & ((\mathrm{x}, \mathrm{ar}, \mathrm{aw}, \mathbf{s}_{r_i}, \ell_{r_i^1}) = (1,0,0,0,0) \wedge \ell_{r_i^1} = 1 \rightarrow \mathrm{aw} = 0) \left[\bar{f}/\mathrm{X}_1\right] \\
= & \quad \% \quad Def.\ \mathrm{I}_{r_i^1}, p_{ri} \\
 & (\mathrm{I}_{r_i^1} \wedge p_{ri}) \left[\bar{f}/\mathrm{X}_1\right]
\end{array}
$$

(b) **Proof 4**

Since $\mathrm{T}_{r_i^2}$ *is of the form* $\mathbf{stut}_{r_i^2} \vee \bigvee_\tau(\epsilon = \mathbf{a}_\tau \wedge trans_\tau)$ *then* $\mathrm{T}_{r_i^2} \wedge ((p_2 \wedge p_2') \vee \mathbf{stut}_2)$ *is equal to* $\mathbf{stut}_{r_i^2} \vee \bigvee_\tau(\epsilon = \mathbf{a}_\tau \wedge trans_\tau \wedge p_2 \wedge p_2')$. $\mathrm{T}_{r_i^1}$ *is of the form* $\mathbf{stut}_{r_i^1} \vee \bigvee_\tau(\epsilon = \mathbf{a}_\tau \wedge trans_\tau)$ *so* $\mathrm{T}_{r_i^1} \wedge ((p_{ri} \wedge p_{ri}') \vee \mathbf{stut}_{r_i^1})$ *is equal to* $\mathbf{stut}_{r_i^1} \vee \bigvee_\tau(\epsilon = \mathbf{a}_\tau \wedge trans_\tau \wedge p_{ri} \wedge p_{ri}')$.

- $$
\begin{array}{ll}
 & \tau_{r_{i,1}^2} \wedge p_2 \wedge p_2' \\
= & \left(\epsilon = \mathbf{i} \wedge (\ell_{r_i^2}, \mathrm{m}) = (0,1) \wedge p_2 \wedge p_2' \wedge \Psi_2' = \Psi_2 \left[0, 6/\mathrm{m}, \ell_{r_i^2}\right]\right) \\
\rightarrow & \left(\epsilon = \mathbf{i} \wedge \Psi_1' = \Psi_1\right) \left[\bar{f}/\mathrm{X}_1\right] \\
\rightarrow & \mathbf{stut}_{r_i^1} \left[\bar{f}/\mathrm{X}_1\right]
\end{array}
$$

  The first P-operation of reader$_i^2$ *is an stuttering step in reader*$_i^1$.

- $$
\begin{array}{ll}
 & \tau_{r_{i,2}^2} \wedge p_2 \wedge p_2' \\
= & \left(\epsilon = \mathbf{i} \wedge \ell_{r_i^2} = 6 \wedge p_2 \wedge p_2' \wedge CHO(7)\right) \\
\rightarrow & \left(\epsilon = \mathbf{i} \wedge \Psi_1' = \Psi_1\right) \left[\bar{f}/\mathrm{X}_1\right] \\
\rightarrow & \mathbf{stut}_{r_i^1} \left[\bar{f}/\mathrm{X}_1\right]
\end{array}
$$

  The first V-operation of reader$_i^2$ *is an stuttering step in reader*$_i^1$.

- $$
\begin{array}{ll}
 & \tau_{r_{i,3}^2} \wedge p_2 \wedge p_2' \\
= & \left(\epsilon = \mathbf{i} \wedge (\ell_{r_i^2}, \mathrm{r}) = (7,1) \wedge p_2 \wedge p_2' \wedge \Psi_2' = \Psi_2 \left[0, 1/\mathrm{r}, \ell_{r_i^2}\right]\right) \\
\rightarrow & \left(\epsilon = \mathbf{i} \wedge \ell_{r_i^1} = 0 \wedge \mathrm{x} = 1 \wedge p_{ri} \wedge p_{ri}' \wedge \Psi_1' = \Psi_1 \left[0, 1/\mathrm{x}, \ell_{r_i^1}\right]\right) \left[\bar{f}/\mathrm{X}_1\right] \\
= & (\tau_{r_{i,1}^1} \wedge p_{ri} \wedge p_{ri}') \left[\bar{f}/\mathrm{X}_1\right]
\end{array}
$$

  The second P-operation of reader$_i^2$ *corresponds to the first P-operation of reader*$_i^1$.

– $$\begin{array}{ll} & \tau_{r^2_{i,4}} \wedge p_2 \wedge p_2' \\ = & \left(\epsilon = \mathbf{i} \wedge \ell_{r^2_i} = 1 \wedge p_2 \wedge p_2' \wedge \Psi_2' = \Psi_2 \left[\mathrm{ar}+1, 2/\mathrm{ar}, \ell_{r^2_i}\right]\right) \\ \rightarrow & \left(\epsilon = \mathbf{i} \wedge (\ell_{r^1_i}, \mathrm{aw}) = (1,0) \wedge p_{ri} \wedge p_{ri}' \wedge \Psi_1' = \Psi_1 \left[\mathrm{ar}+1, 2/\mathrm{ar}, \ell_{r^1_i}\right]\right) \\ & \left[\bar{f}/\mathrm{X}_1\right] \\ = & (\tau_{r^1_{i,2}} \wedge p_{ri} \wedge p_{ri}') \left[\bar{f}/\mathrm{X}_1\right] \end{array}$$

The ar *increment step of reader*^2_i *corresponds to the* ar *increment step of reader*^1_i *.*

– $$\begin{array}{ll} & \tau_{r^2_{i,5}} \wedge p_2 \wedge p_2' \\ = & \left(\epsilon = \mathbf{i} \wedge \ell_{r^2_i} = 2 \wedge p_2 \wedge p_2' \wedge CHO(3) \wedge \Psi_2' = \Psi_2 \left[1/\mathbf{s}_{r_i}\right]\right) \\ \rightarrow & \left(\epsilon = \mathbf{i} \wedge \ell_{r^1_i} = 2 \wedge p_{ri} \wedge p_{ri}' \wedge \Psi_1' = \Psi_1 \left[1, 1, 3/\mathbf{s}_{r_i}, \mathrm{x}, \ell_{r^1_i}\right]\right) \left[\bar{f}/\mathrm{X}_1\right] \\ = & (\tau_{r^1_{i,3}} \wedge p_{ri} \wedge p_{ri}') \left[\bar{f}/\mathrm{X}_1\right] \end{array}$$

If reader^2_i *becomes critical then reader*^1_i *becomes critical.*

– $$\begin{array}{ll} & \tau_{r^2_{i,6}} \wedge p_2 \wedge p_2' \\ = & \left(\epsilon = \mathbf{i} \wedge (\ell_{r^2_i}, \mathrm{m}) = (3,1) \wedge p_2 \wedge p_2' \wedge \Psi_2' = \Psi_2 \left[0, 4/\mathrm{m}, \ell_{r^2_i}\right]\right) \\ \rightarrow & \left(\epsilon = \mathbf{i} \wedge \ell_{r^1_i} = 3 \wedge \mathrm{x} = 1 \wedge p_{ri} \wedge p_{ri}' \wedge \Psi_1' = \Psi_1 \left[0, 4/\mathrm{x}, \ell_{r^1_i}\right]\right) \left[\bar{f}/\mathrm{X}_1\right] \\ = & (\tau_{r^1_{i,4}} \wedge p_{ri} \wedge p_{ri}') \left[\bar{f}/\mathrm{X}_1\right] \end{array}$$

The third P-operation of reader^2_i *corresponds to the second P-operation of reader*^1_i*.*

– $$\begin{array}{ll} & \tau_{r^2_{i,7}} \wedge p_2 \wedge p_2' \\ = & \left(\epsilon = \mathbf{i} \wedge \ell_{r^2_i} = 4 \wedge p_2 \wedge p_2' \wedge \Psi_2' = \Psi_2 \left[\mathrm{ar}-1, 5/\mathrm{ar}, \ell_{r^2_i}\right]\right) \\ \rightarrow & \left(\epsilon = \mathbf{i} \wedge \ell_{r^1_i} = 4 \wedge p_{ri} \wedge p_{ri}' \wedge \Psi_1' = \Psi_1 \left[\mathrm{ar}-1, 5/\mathrm{ar}, \ell_{r^1_i}\right]\right) \left[\bar{f}/\mathrm{X}_1\right] \\ = & (\tau_{r^1_{i,5}} \wedge p_{ri} \wedge p_{ri}') \left[\bar{f}/\mathrm{X}_1\right] \end{array}$$

The ar *decrement step of reader*^2_i *corresponds to the* ar *decrement step of reader*^1_i*.*

– $$\begin{array}{ll} & \tau_{r^2_{i,8}} \wedge p_2 \wedge p_2' \\ = & \left(\epsilon = \mathbf{i} \wedge \ell_{r^2_i} = 5 \wedge p_2 \wedge p_2' \wedge CHO(0) \wedge \Psi_2' = \Psi_2 \left[0/\mathbf{s}_{r_i}\right]\right) \\ \rightarrow & \left(\epsilon = \mathbf{i} \wedge \ell_{r^1_i} = 5 \wedge p_{ri} \wedge p_{ri}' \wedge \Psi_1' = \Psi_1 \left[0, 1, 0/\mathbf{s}_{r_i}, \mathrm{x}, \ell_{r^1_i}\right]\right) \left[\bar{f}/\mathrm{X}_1\right] \\ = & (\tau_{r^1_{i,6}} \wedge p_{ri} \wedge p_{ri}') \left[\bar{f}/\mathrm{X}_1\right] \end{array}$$

If reader^2_i *becomes non-critical then reader*^1_i *becomes non-critical.*

– $$\begin{array}{ll} & \tau_{r^2_{i,9}} \wedge p_2 \wedge p_2' \\ = & \left(\epsilon = \mathbf{e} \wedge \mathrm{m} = 1 \wedge p_2 \wedge p_2' \wedge \Psi_2' = \Psi_2 \left[0/\mathrm{m}\right]\right) \\ \rightarrow & \left(\epsilon = \mathbf{e} \wedge \mathrm{x} = 1 \wedge p_{ri} \wedge p_{ri}' \wedge \Psi_1' = \Psi_1 \left[0/\mathrm{x}\right]\right) \left[\bar{f}/\mathrm{X}_1\right] \\ = & (\tau_{r^1_{i,7}} \wedge p_{ri} \wedge p_{ri}') \left[\bar{f}/\mathrm{X}_1\right] \end{array}$$

If the environment of reader^2_i *executes a P-operation then the environment of reader*^1_i *also executes a P-operation.*

- $$\begin{array}{ll} & \tau_{r^2_{i,10}} \wedge p_2 \wedge p'_2 \\ = & \big(\epsilon = \mathbf{e} \wedge \mathrm{r} = 1 \wedge p_2 \wedge p'_2 \wedge \Psi'_2 = \Psi_2\,[0/\mathrm{r}]\big) \\ \rightarrow & \big(\epsilon = \mathbf{e} \wedge \mathrm{x} = 1 \wedge p_{ri} \wedge p'_{ri} \wedge \Psi'_1 = \Psi_1\,[0/\mathrm{x}]\big)\,\big[\bar{f}/\mathrm{X}_1\big] \\ = & (\tau_{r^1_{i,7}} \wedge p_{ri} \wedge p'_{ri})\,\big[\bar{f}/\mathrm{X}_1\big] \end{array}$$

  If the environment of reader$_i^2$ executes a P-operation then the environment of reader$_i^1$ also executes a P-operation.

- $$\begin{array}{ll} & \tau_{r^2_{i,11}} \wedge p_2 \wedge p'_2 \\ = & \big(\epsilon = \mathbf{e} \wedge \mathrm{w} = 1 \wedge p_2 \wedge p'_2 \wedge \Psi'_2 = \Psi_2\,[0/\mathrm{w}]\big) \\ \rightarrow & \big(\epsilon = \mathbf{e} \wedge \mathrm{x} = 1 \wedge p_{ri} \wedge p'_{ri} \wedge \Psi'_1 = \Psi_1\,[0/\mathrm{x}]\big)\,\big[\bar{f}/\mathrm{X}_1\big] \\ = & (\tau_{r^1_{i,7}} \wedge p_{ri} \wedge p'_{ri})\,\big[\bar{f}/\mathrm{X}_1\big] \end{array}$$

  If the environment of reader$_i^2$ executes a P-operation then the environment of reader$_i^1$ also executes a P-operation.

- $$\begin{array}{ll} & \tau_{r^2_{i,12}} \wedge p_2 \wedge p'_2 \\ = & \big(\epsilon = \mathbf{e} \wedge \ell_{r^2_i} \in \{0,7,3\} \wedge \mathrm{m} = 0 \wedge p_2 \wedge p'_2 \wedge \Psi'_2 = \Psi_2\,[1/\mathrm{m}]\big) \\ \rightarrow & \big(\epsilon = \mathbf{e} \wedge \ell_{r^1_i} \in \{0,3\} \wedge \mathrm{x} = 0 \wedge p_{ri} \wedge p'_{ri} \wedge \Psi'_1 = \Psi_1\,[1/\mathrm{x}]\big)\,\big[\bar{f}/\mathrm{X}_1\big] \\ = & (\tau_{r^1_{i,8}} \wedge p_{ri} \wedge p'_{ri})\,\big[\bar{f}/\mathrm{X}_1\big] \end{array}$$

  If the environment of reader$_i^2$ executes a V-operation then the environment of reader$_i^1$ also executes a V-operation.

- $$\begin{array}{ll} & \tau_{r^2_{i,13}} \wedge p_2 \wedge p'_2 \\ = & \big(\epsilon = \mathbf{e} \wedge \ell_{r^2_i} \in \{0,7,3\} \wedge \mathrm{r} = 0 \wedge p_2 \wedge p'_2 \wedge \Psi'_2 = \Psi_2\,[1/\mathrm{r}]\big) \\ \rightarrow & \big(\epsilon = \mathbf{e} \wedge \ell_{r^1_i} \in \{0,3\} \wedge \mathrm{x} = 0 \wedge p_{ri} \wedge p'_{ri} \wedge \Psi'_1 = \Psi_1\,[1/\mathrm{x}]\big)\,\big[\bar{f}/\mathrm{X}_1\big] \\ = & (\tau_{r^1_{i,8}} \wedge p_{ri} \wedge p'_{ri})\,\big[\bar{f}/\mathrm{X}_1\big] \end{array}$$

  If the environment of reader$_i^2$ executes a V-operation then the environment of reader$_i^1$ also executes a V-operation.

- $$\begin{array}{ll} & \tau_{r^2_{i,14}} \wedge p_2 \wedge p'_2 \\ = & \big(\epsilon = \mathbf{e} \wedge \ell_{r^2_i} \in \{0,7,3\} \wedge \mathrm{w} = 0 \wedge p_2 \wedge p'_2 \wedge \Psi'_2 = \Psi_2\,[1/\mathrm{w}]\big) \\ \rightarrow & \big(\epsilon = \mathbf{e} \wedge \ell_{r^1_i} \in \{0,3\} \wedge \mathrm{x} = 0 \wedge p_{ri} \wedge p'_{ri} \wedge \Psi'_1 = \Psi_1\,[1/\mathrm{x}]\big)\,\big[\bar{f}/\mathrm{X}_1\big] \\ = & (\tau_{r^1_{i,8}} \wedge p_{ri} \wedge p'_{ri})\,\big[\bar{f}/\mathrm{X}_1\big] \end{array}$$

  If the environment of reader$_i^2$ executes a V-operation then the environment of reader$_i^1$ also executes a V-operation.

- $\mathbf{stut}_{r^2_i} \rightarrow \mathbf{stut}_{r^1_i}\,\big[\bar{f}/\mathrm{X}_1\big]$

  since $\mathbf{s}_{r_i}$ *doesn't change.*

(c) Let $\mathrm{WF}_{r^2_i} \triangleq \{\tau_{r^2_{i,k}} \mid k \in \{4,7\}\}$ and
$\mathrm{SF}_{r^2_i} \triangleq \{\tau_{r^2_{i,k}} \mid k \in \{1,2,3,5,6,8,9,10,11,12,13,14\}\}$ then

$$\mathrm{L}_{r^2_i} \triangleq \bigwedge_{\tau \in \mathrm{WF}_{r^2_i}} (\Diamond\Box En(\tau) \rightarrow \Box\Diamond\tau) \wedge \bigwedge_{\tau \in \mathrm{SF}_{r^2_i}} (\Box\Diamond En(\tau) \rightarrow \Box\Diamond\tau)$$

Let $\mathrm{WF}_{r_i^1} \triangleq \{\tau_{r_{i,k}^1} \mid k \in \{2,5\}\}$ and $\mathrm{SF}_{r_i^1} \triangleq \{\tau_{r_{i,k}^1} \mid k \in \{1,3,4,6,7,8\}\}$ then

$$\mathrm{L}_{r_i^1} \triangleq \bigwedge_{\tau \in \mathrm{WF}_{r_i^1}} (\Diamond\Box En(\tau) \to \Box\Diamond\tau) \wedge \bigwedge_{\tau \in \mathrm{SF}_{r_i^1}} (\Box\Diamond En(\tau) \to \Box\Diamond\tau)$$

The following holds:

$$\mathcal{S}_2 \cap Hist(\mathrm{W}_2) \models \mathrm{L}_{r_i^2} \to \mathrm{L}_{r_i^1}\left[\bar{f}/\mathrm{X}_1\right]$$

since $\tau_{r_{i,2}^1}$ is relatively refined by $\tau_{r_{i,4}^2}$, $\tau_{r_{i,5}^1}$ is relatively refined by $\tau_{r_{i,7}^2}$, and $\tau_{r_{i,1}^1}$ is relatively refined by $\tau_{r_{i,1}^2}$, $\tau_{r_{i,2}^2}$ and $\tau_{r_{i,3}^2}$, and $\tau_{r_{i,3}^1}$ is relatively refined by $\tau_{r_{i,5}^2}$, and $\tau_{r_{i,4}^1}$ is relatively refined by $\tau_{r_{i,6}^2}$, and $\tau_{r_{i,6}^1}$ is relatively refined by $\tau_{r_{i,8}^2}$, and $\tau_{r_{i,7}^1}$ is relatively refined by $\tau_{r_{i,9}^2}$, $\tau_{r_{i,10}^2}$ and $\tau_{r_{i,11}^2}$, and $\tau_{r_{i,8}^1}$ is relatively refined by $\tau_{r_{i,12}^2}$, $\tau_{r_{i,13}^2}$ and $\tau_{r_{i,14}^2}$. So

$$\mathcal{S}_2 \cap Hist(\mathrm{W}_2) \models \mathrm{L}_{r_i^1}\left[\bar{f}/\mathrm{X}_1\right]$$

ad (2) Analogue to the proof of (1).

ad (3) This is trivial because $\mathrm{W}_1 \leftrightarrow (\bigwedge_{i=1}^{N} \mathrm{W}_{r_i^1} \wedge \bigwedge_{j=1}^{M} \mathrm{W}_{w_j^1})$.

ad (4) The following holds because W_2 doesn't contain ϵ_2 variables, i.e., it can be put within the existential quantification, and furthermore $\mathrm{W}_2 = \mathrm{W}_2\,[\epsilon_{2,i}/\epsilon] = W_2\,[\epsilon_{2,N+j}/\epsilon]$ ($i = 1,\ldots,N$ and $j = 1,\ldots,M$) because W_2 doesn't constrain the ϵ variable.

$$(\exists\bar{\epsilon}_2.\ \odot_{B_2^A}(\epsilon,\bar{\epsilon}_2) \wedge \textstyle\bigwedge_{i=1}^{N} \mathrm{H}_{r_i^2}\,[\epsilon_{2,i}/\epsilon] \wedge \bigwedge_{j=1}^{M} \mathrm{H}_{w_j^2}\,[\epsilon_{2,N+j}/\epsilon]) \wedge \mathrm{W}_2$$
$$\to$$
$$(\exists\bar{\epsilon}_2.\ \odot_{B_2^A}(\epsilon,\bar{\epsilon}_2) \wedge \textstyle\bigwedge_{i=1}^{N}(\mathrm{H}_{r_i^2} \wedge \mathrm{W}_2)\,[\epsilon_{2,i}/\epsilon] \wedge \bigwedge_{j=1}^{M}(\mathrm{H}_{w_j^2} \wedge \mathrm{W}_2)\,[\epsilon_{2,N+j}/\epsilon])$$

3.5 The third development step

Dijkstra's solution to the problem of the newly introduced deadlocked sequences is as follows: record in a shared variable bX the number of components that can generate a P-operation on a semaphore X as their first coming P-operation. A component that executed a P-operation on X decreases bX by one. The component "knows" what its next P-operation is, so it increases the corresponding shared variable by one. The guards in the `CHOOSE` segment are changed so that the correct V-branch is chosen. The initial value of bm is $N+M$ because initially all processes have `P(m)` as their first coming P-operation. The initial value of br and bw is then of course 0. Like in the second step the initial value of m is 1 and that of ar, aw, r and w 0. The result of this transformation is as follows:

```
reader_i^3:
        do true → NCS;
                  P(m);bm:=bm-1;br:=br+1;CHOOSE;
                  P(r);br:=br-1;ar:=ar+1;bm:=bm+1;CHOOSE;
                  READ;
```

```
                    P(m);bm:=bm-1;ar:=ar-1;bm:=bm+1;CHOOSE
        od
```

writer$_j^3$:

```
        do true → NCS;
                    P(m);bm:=bm-1;bw:=bw+1;CHOOSE;
                    P(w);bw:=bw-1;aw:=aw+1;bm:=bm+1;CHOOSE;
                    WRITE;
                    P(m);bm:=bm-1;aw:=aw-1;bm:=bm+1;CHOOSE
        od
```

with CHOOSE:
```
if bm>0 →V(m)
[] aw=0 ∧ br>0 →V(r)
[] aw=0 ∧ ar=0 ∧ bw>0 →V(w)
fi
```

$\texttt{Syn}^3 \;:\; \|_{i=1}^{N}\ \texttt{reader}_i^3 \ \|\ \|_{j=1}^{M}\ \texttt{writer}_j^3$

Syn^3 still generates sequences that Dijkstra does not allow. These sequences are generated because CHOOSE is still non-deterministic. Suppose a $\texttt{reader}_i^3$ can choose between a V(m) and a V(r) operation. Choosing V(m) causes that another reader$_k^3$ (writer$_l^3$) can signal that it has finished executing READ (WRITE) or wants to execute READ (WRITE). A V(r) causes that a reader$_k^3$ can execute READ. Choosing V(m) thus unnecessarily blocks a reader$_k^3$. So it is not a deadlocked sequence but only an inefficient sequence. The informal requirement of Syn^3 is that no unnecessary blocking sequences are allowed.

In the following sections the DTL machine specifications $\mathcal{S}_{r_i^3}$ (corresponding to program reader$_i^3$) and $\mathcal{S}_{w_j^3}$ (corresponding to program writer$_j^3$), and the extra requirement W_3, excluding inefficient computations, are given.

3.5.1 Specification $\mathcal{S}_{r_i^3}$

The formal specification $\mathcal{S}_{r_i^3} \triangleq (B_{r_i^3}, \mathrm{H}_{r_i^3})$ where $\mathrm{H}_{r_i^3} \triangleq \mathrm{I}_{r_i^3} \wedge \Box\mathrm{T}_{r_i^3} \wedge \mathrm{L}_{r_i^3}$ and $B_{r_i^3}$, $\mathrm{I}_{r_i^3}$, $\mathrm{T}_{r_i^3}$ and $\mathrm{L}_{r_i^3}$ are as follows:

1. **Basis** $B_{r_i^3} = ((\mathrm{In}_{r_i^3}, \mathrm{Out}_{r_i^3}), (\mathrm{V}_{r_i^3}, \mathrm{X}_{r_i^3}))$

$$
\begin{aligned}
\mathrm{In}_{r_i^3} &\triangleq \emptyset,\\
\mathrm{Out}_{r_i^3} &\triangleq \emptyset,\\
\mathrm{V}_{r_i^3} &\triangleq \{\mathbf{m}, \mathbf{bm}, \mathbf{r}, \mathbf{br}, \mathbf{w}, \mathbf{bw}, \mathbf{ar}, \mathbf{aw}, \mathrm{s}_{r_i}\},\\
\mathrm{X}_{r_i^3} &\triangleq \{\ell_{r_i^3}\}
\end{aligned}
$$

- $\ell_{r_i^3} = 0$: reader$_i^3$ is non critical.
- $\ell_{r_i^3} = 6$: reader$_i^3$ executed first P-action on $\mathbf{m}$.

- $\ell_{r_i^3} = 8$: reader$_i^3$ updated **bm** and **br**.
- $\ell_{r_i^3} = 7$: reader$_i^3$ executed first `CHOOSE`.
- $\ell_{r_i^3} = 1$: reader$_i^3$ executed P-action on **r**.
- $\ell_{r_i^3} = 2$: reader$_i^3$ updated **br**, **ar** and **bm**.
- $\ell_{r_i^3} = 3$: reader$_i^3$ is critical.
- $\ell_{r_i^3} = 4$: reader$_i^3$ executed second P-action on **m**.
- $\ell_{r_i^3} = 5$: reader$_i^3$ updated **ar**.

Let $\Psi_3 \triangleq (\mathbf{m}, \mathbf{bm}, \mathbf{r}, \mathbf{br}, \mathbf{w}, \mathbf{bw}, \mathbf{ar}, \mathbf{aw}, \mathbf{s}_{r_i}, \ell_{r_i^3})$ and
$\Psi_3' \triangleq (\mathbf{m}', \mathbf{bm}', \mathbf{r}', \mathbf{br}', \mathbf{w}', \mathbf{bw}', \mathbf{ar}', \mathbf{aw}', \mathbf{s}_{r_i}', \ell_{r_i^3}')$.

2. **Initial States**

$$\mathrm{I}_{r_i^3} \triangleq \Psi_3 = (1, N + M, 0, 0, 0, 0, 0, 0, 0, 0)$$

3. **Transitions:**

Let $CHO(X) \triangleq \begin{array}{ll} \vee & (\mathbf{bm} > 0 \wedge \Psi_3' = \Psi_3\left[1, X/\mathbf{m}, \ell_{r_i^3}\right]) \\ \vee & (\mathbf{aw} = 0 \wedge \mathbf{br} > 0 \wedge \Psi_3' = \Psi_3\left[1, X/\mathbf{r}, \ell_{r_i^3}\right]) \\ \vee & (\mathbf{aw} = 0 \wedge \mathbf{ar} = 0 \wedge \mathbf{bw} > 0 \wedge \Psi_3' = \Psi_3\left[1, X/\mathbf{w}, \ell_{r_i^3}\right]) \end{array}$

$\mathrm{T}_{r_i^3} \triangleq$

$\tau_{r_{i,1}^3}$ $\quad \left(\epsilon = \mathbf{i} \wedge (\ell_{r_i^3}, \mathbf{m}) = (0,1) \wedge \Psi_3' = \Psi_3\left[0, 6/\mathbf{m}, \ell_{r_i^3}\right]\right)$

Reader$_i^3$ executes first P-action on **m**.

$\tau_{r_{i,2}^3}$ $\quad \vee \left(\epsilon = \mathbf{i} \wedge \ell_{r_i^3} = 6 \wedge \Psi_3' = \Psi_3\left[\mathbf{bm} - 1, \mathbf{br} + 1, 8/\mathbf{bm}, \mathbf{br}, \ell_{r_i^3}\right]\right)$

Reader$_i^3$ updates **bm** and **br**.

$\tau_{r_{i,3}^3}$ $\quad \vee \left(\epsilon = \mathbf{i} \wedge \ell_{r_i^3} = 8 \wedge CHO(7)\right)$

Reader$_i^3$ executes first `CHOOSE`.

$\tau_{r_{i,4}^3}$ $\quad \vee \left(\epsilon = \mathbf{i} \wedge (\ell_{r_i^3}, \mathbf{r}) = (7,1) \wedge \Psi_3' = \Psi_3\left[0, 1/\mathbf{r}, \ell_{r_i^3}\right]\right)$

Reader$_i^3$ executes its P-action on **r**.

$\tau_{r_{i,5}^3}$ $\quad \vee \left(\epsilon = \mathbf{i} \wedge \ell_{r_i^3} = 1 \wedge \Psi_3' = \Psi_3\left[\mathbf{br} - 1, \mathbf{ar} + 1, \mathbf{bm} + 1, 2/\mathbf{br}, \mathbf{ar}, \mathbf{bm}, \ell_{r_i^3}\right]\right)$

Reader$_i^3$ updates **br**, **ar** and **bm**.

$\tau_{r_{i,6}^3}$ $\quad \vee \left(\epsilon = \mathbf{i} \wedge \ell_{r_i^3} = 2 \wedge CHO(3) \wedge \Psi_3' = \Psi_3\left[1/\mathbf{s}_{r_i}\right]\right)$

Reader$_i^3$ becomes critical.

$\tau_{r_{i,7}^3}$ $\quad \vee \left(\epsilon = \mathbf{i} \wedge (\ell_{r_i^3}, \mathbf{m}) = (3,1) \wedge \Psi_3' = \Psi_3\left[0, 4/\mathbf{m}, \ell_{r_i^3}\right]\right)$

Reader$_i^3$ executes second P-action on **m**.

$\tau_{r_{i,8}^3}$ $\quad \vee \left(\epsilon = \mathbf{i} \wedge \ell_{r_i^3} = 4 \wedge \Psi_3' = \Psi_3\left[\mathbf{ar} - 1, 5/\mathbf{ar}, \ell_{r_i^3}\right]\right)$

Reader$_i^3$ updates **ar**.

$\tau_{r^3_{i,9}}$ $\quad\vee\ \big(\epsilon = \mathbf{i} \wedge \ell_{r^3_i} = 5 \wedge CHO(0) \wedge \Psi_3' = \Psi_3\,[0/\mathbf{s}_{r_i}]\big)$

Reader^3_i becomes non critical.

$\tau_{r^3_{i,10}}$ $\quad\vee\ \big(\epsilon = \mathbf{e} \wedge \mathbf{m} = 1 \wedge \Psi_3' = \Psi_3\,[0/\mathbf{m}]\big)$

The environment executes a P-operation on **m**.

$\tau_{r^3_{i,11}}$ $\quad\vee\ \big(\epsilon = \mathbf{e} \wedge \mathbf{r} = 1 \wedge \Psi_3' = \Psi_3\,[0/\mathbf{r}]\big)$

The environment executes a P-operation on **r**.

$\tau_{r^3_{i,12}}$ $\quad\vee\ \big(\epsilon = \mathbf{e} \wedge \mathbf{w} = 1 \wedge \Psi_3' = \Psi_3\,[0/\mathbf{w}]\big)$

The environment executes a P-operation on **w**.

$\tau_{r^3_{i,13}}$ $\quad\vee\ \big(\epsilon = \mathbf{e} \wedge \ell_{r^3_i} \in \{0,7,3\} \wedge \mathbf{m} = 0 \wedge \Psi_3' = \Psi_3\,[1/\mathbf{m}]\big)$

The environment executes a V-operation on **m**.

$\tau_{r^3_{i,14}}$ $\quad\vee\ \big(\epsilon = \mathbf{e} \wedge \ell_{r^3_i} \in \{0,7,3\} \wedge \mathbf{r} = 0 \wedge \Psi_3' = \Psi_3\,[1/\mathbf{r}]\big)$

The environment executes a V-operation on **r**.

$\tau_{r^3_{i,15}}$ $\quad\vee\ \big(\epsilon = \mathbf{e} \wedge \ell_{r^3_i} \in \{0,7,3\} \wedge \mathbf{w} = 0 \wedge \Psi_3' = \Psi_3\,[1/\mathbf{w}]\big)$

The environment executes a P-operation on **w**.

$\tau_{r^3_{i,0}}$ $\quad\vee\ \mathbf{stut}_{r^3_i}$

These transitions are illustrated in figure 3.7

4. **Liveness:**
$\mathrm{L}_{r^3_i}$ expresses that the P- and V-operations on the semaphores **m**, **r** and **w** are strongly fair and all the other transitions are weakly fair.
Let $\mathrm{WF}_{r^3_i} \triangleq \{\tau_{r^3_{i,k}} \mid k \in \{2,5,8\}\}$ and
$\mathrm{SF}_{r^3_i} \triangleq \{\tau_{r^3_{i,k}} \mid k \in \{1,3,4,6,7,9,10,11,12,13,14,15\}\}$ then

$$\mathrm{L}_{r^3_i} \triangleq \bigwedge_{\tau\in \mathrm{WF}_{r^3_i}} (\Diamond\Box En(\tau) \rightarrow \Box\Diamond\tau) \wedge \bigwedge_{\tau\in \mathrm{SF}_{r^3_i}} (\Box\Diamond En(\tau) \rightarrow \Box\Diamond\tau)$$

3.5.2 Specification $\mathcal{S}_{w^3_j}$

The formal specification $\mathcal{S}_{w^3_j} \triangleq (B_{w^3_j}, \mathrm{H}_{w^3_j})$ where $\mathrm{H}_{w^3_j} \triangleq \mathrm{I}_{w^3_j} \wedge \Box\mathrm{T}_{w^3_j} \wedge \mathrm{L}_{w^3_j}$ and $B_{w^3_j}$, $\mathrm{I}_{w^3_j}$, $\mathrm{T}_{w^3_j}$ and $\mathrm{L}_{w^3_j}$ are as follows:

1. **Basis** $B_{w^3_j} = ((\mathrm{In}_{w^3_j}, \mathrm{Out}_{w^3_j}), (\mathrm{V}_{w^3_j}, \mathrm{X}_{w^3_j}))$

$$\begin{aligned}
\mathrm{In}_{w^3_j} &\triangleq \emptyset,\\
\mathrm{Out}_{w^3_j} &\triangleq \emptyset,\\
\mathrm{V}_{w^3_j} &\triangleq \{\mathbf{m}, \mathbf{bm}, \mathbf{r}, \mathbf{br}, \mathbf{w}, \mathbf{bw}, \mathbf{ar}, \mathbf{aw}, \mathbf{s}_{w_j}\},\\
\mathrm{X}_{w^3_j} &\triangleq \{\ell_{w^3_j}\}
\end{aligned}$$

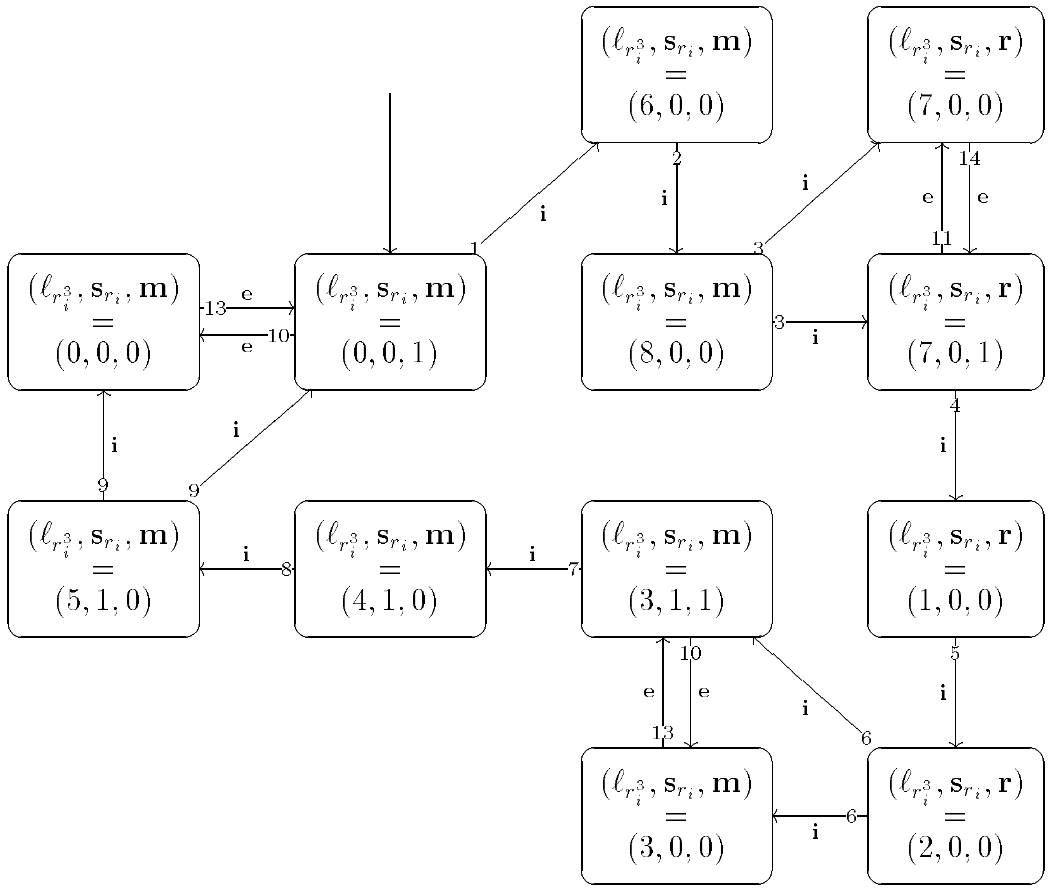

Figure 3.7: Transitions of reader$_i^3$.

- $\ell_{w_j^3} = 0$: writer$_j^3$ is non critical.
- $\ell_{w_j^3} = 6$: writer$_j^3$ executed first P-action on $\mathbf{m}$.
- $\ell_{w_j^3} = 8$: writer$_j^3$ updated $\mathbf{bm}$ and $\mathbf{bw}$.
- $\ell_{w_j^3} = 7$: writer$_j^3$ executed first `CHOOSE`.
- $\ell_{w_j^3} = 1$: writer$_j^3$ executed P-action on $\mathbf{w}$.
- $\ell_{w_j^3} = 2$: writer$_j^3$ updated $\mathbf{bw}$, $\mathbf{aw}$ and $\mathbf{bm}$.
- $\ell_{w_j^3} = 3$: writer$_j^3$ is critical.
- $\ell_{w_j^3} = 4$: writer$_j^3$ executed second P-action on $\mathbf{m}$.
- $\ell_{w_j^3} = 5$: writer$_j^3$ updated $\mathbf{aw}$.

Let $\Psi_3 \triangleq (\mathbf{m}, \mathbf{bm}, \mathbf{r}, \mathbf{br}, \mathbf{w}, \mathbf{bw}, \mathbf{ar}, \mathbf{aw}, \mathrm{s}_{w_j}, \ell_{w_j^3})$ and
$\Psi_3' \triangleq (\mathbf{m}', \mathbf{bm}', \mathbf{r}', \mathbf{br}', \mathbf{w}', \mathbf{bw}', \mathbf{ar}', \mathbf{aw}', \mathrm{s}'_{w_j}, \ell'_{w_j^3})$.

2. **Initial States**

$$\mathrm{I}_{w_j^3} \triangleq \Psi_3 = (1, N+M, 0,0,0,0,0,0,0,0)$$

3. **Transitions:**
Let $CHO(X) \triangleq \begin{array}{l} \vee \ \ (\mathbf{bm} > 0 \wedge \Psi_3' = \Psi_3 \left[1, X/\mathbf{m}, \ell_{w_j^3}\right]) \\ \vee \ \ (\mathbf{aw} = 0 \wedge \mathbf{br} > 0 \wedge \Psi_3' = \Psi_3 \left[1, X/\mathbf{r}, \ell_{w_j^3}\right]) \\ \vee \ \ (\mathbf{aw} = 0 \wedge \mathbf{ar} = 0 \wedge \mathbf{bw} > 0 \wedge \Psi_3' = \Psi_3 \left[1, X/\mathbf{w}, \ell_{w_j^3}\right]) \end{array}$

$\mathrm{T}_{w_j^3} \triangleq$

$\tau_{w_{i,1}^3}$ $\left(\epsilon = \mathbf{i} \wedge (\ell_{w_j^3}, \mathbf{m}) = (0,1) \wedge \Psi_3' = \Psi_3 \left[0, 6/\mathbf{m}, \ell_{w_j^3}\right]\right)$
Writer$_j^3$ executes first P-action on $\mathbf{m}$.

$\tau_{w_{i,2}^3}$ $\vee \left(\epsilon = \mathbf{i} \wedge \ell_{w_j^3} = 6 \wedge \Psi_3' = \Psi_3 \left[\mathbf{bm} - 1, \mathbf{bw} + 1, 8/\mathbf{bm}, \mathbf{bw}, \ell_{w_j^3}\right]\right)$
Writer$_j^3$ updates $\mathbf{bm}$ and $\mathbf{bw}$.

$\tau_{w_{i,2}^3}$ $\vee \left(\epsilon = \mathbf{i} \wedge \ell_{w_j^3} = 8 \wedge CHO(7)\right)$
Writer$_j^3$ executes first `CHOOSE`.

$\tau_{w_{i,4}^3}$ $\vee \left(\epsilon = \mathbf{i} \wedge (\ell_{w_j^3}, \mathbf{w}) = (7,1) \wedge \Psi_3' = \Psi_3 \left[0, 1/\mathbf{w}, \ell_{w_j^3}\right]\right)$
Writer$_j^3$ executes its P-action on $\mathbf{w}$.

$\tau_{w_{i,5}^3}$ $\vee \left(\epsilon = \mathbf{i} \wedge \ell_{w_j^3} = 1 \wedge \Psi_3' = \Psi_3 \left[\mathbf{bw} - 1, \mathbf{aw}+1, \mathbf{bm}+1, 2/\mathbf{bw}, \mathbf{aw}, \mathbf{bm}, \ell_{w_j^3}\right]\right)$
Writer$_j^3$ updates $\mathbf{bw}$, $\mathbf{aw}$ and $\mathbf{bm}$.

$\tau_{w_{i,6}^3}$ $\vee \left(\epsilon = \mathbf{i} \wedge \ell_{w_j^3} = 2 \wedge CHO(3) \wedge \Psi_3' = \Psi_3 \left[1/\mathbf{s}_{w_j}\right]\right)$
Writer$_j^3$ becomes critical.

$\tau_{w_{i,7}^3}$ $\vee \left(\epsilon = \mathbf{i} \wedge (\ell_{w_j^3}, \mathbf{m}) = (3,1) \wedge \Psi_3' = \Psi_3 \left[0, 4/\mathbf{m}, \ell_{w_j^3}\right]\right)$
Writer$_j^3$ executes second P-action on $\mathbf{m}$.

$\tau_{w_{i,8}^3}$ $\vee \left(\epsilon = \mathbf{i} \wedge \ell_{w_j^3} = 4 \wedge \Psi_3' = \Psi_3 \left[\mathbf{aw} - 1, 5/\mathbf{aw}, \ell_{w_j^3}\right]\right)$
Writer$_j^3$ updates $\mathbf{aw}$.

$\tau_{w_{i,9}^3}$ $\vee \left(\epsilon = \mathbf{i} \wedge \ell_{w_j^3} = 5 \wedge CHO(0) \wedge \Psi_3' = \Psi_3 \left[0/\mathbf{s}_{w_j}\right]\right)$
Writer$_j^3$ becomes non critical.

$\tau_{w_{i,10}^3}$ $\vee \left(\epsilon = \mathbf{e} \wedge \mathbf{m} = 1 \wedge \Psi_3' = \Psi_3 \left[0/\mathbf{m}\right]\right)$
The environment executes a P-operation on $\mathbf{m}$.

$\tau_{w_{i,11}^3}$ $\vee \left(\epsilon = \mathbf{e} \wedge \mathbf{r} = 1 \wedge \Psi_3' = \Psi_3 \left[0/\mathbf{r}\right]\right)$
The environment executes a P-operation on $\mathbf{r}$.

$\tau_{w_{i,12}^3}$ $\vee \left(\epsilon = \mathbf{e} \wedge \mathbf{w} = 1 \wedge \Psi_3' = \Psi_3 \left[0/\mathbf{w}\right]\right)$
The environment executes a P-operation on $\mathbf{w}$.

$\tau_{w^3_{i,13}}$ $\quad\vee\ \big(\epsilon = \mathbf{e} \wedge \ell_{w^3_j} \in \{0, 7, 3\} \wedge \mathbf{m} = 0 \wedge \Psi_3' = \Psi_3\,[1/\mathbf{m}]\big)$

The environment executes a V-operation on $\mathbf{m}$.

$\tau_{w^3_{i,14}}$ $\quad\vee\ \big(\epsilon = \mathbf{e} \wedge \ell_{w^3_j} \in \{0, 7, 3\} \wedge \mathbf{r} = 0 \wedge \Psi_3' = \Psi_3\,[1/\mathbf{r}]\big)$

The environment executes a V-operation on $\mathbf{r}$.

$\tau_{w^3_{i,15}}$ $\quad\vee\ \big(\epsilon = \mathbf{e} \wedge \ell_{w^3_j} \in \{0, 7, 3\} \wedge \mathbf{w} = 0 \wedge \Psi_3' = \Psi_3\,[1/\mathbf{w}]\big)$

The environment executes a P-operation on $\mathbf{w}$.

$\tau_{w^3_{i,0}}$ $\quad\vee\ \mathbf{stut}_{w^3_j}$

These transitions are illustrated in figure 3.8

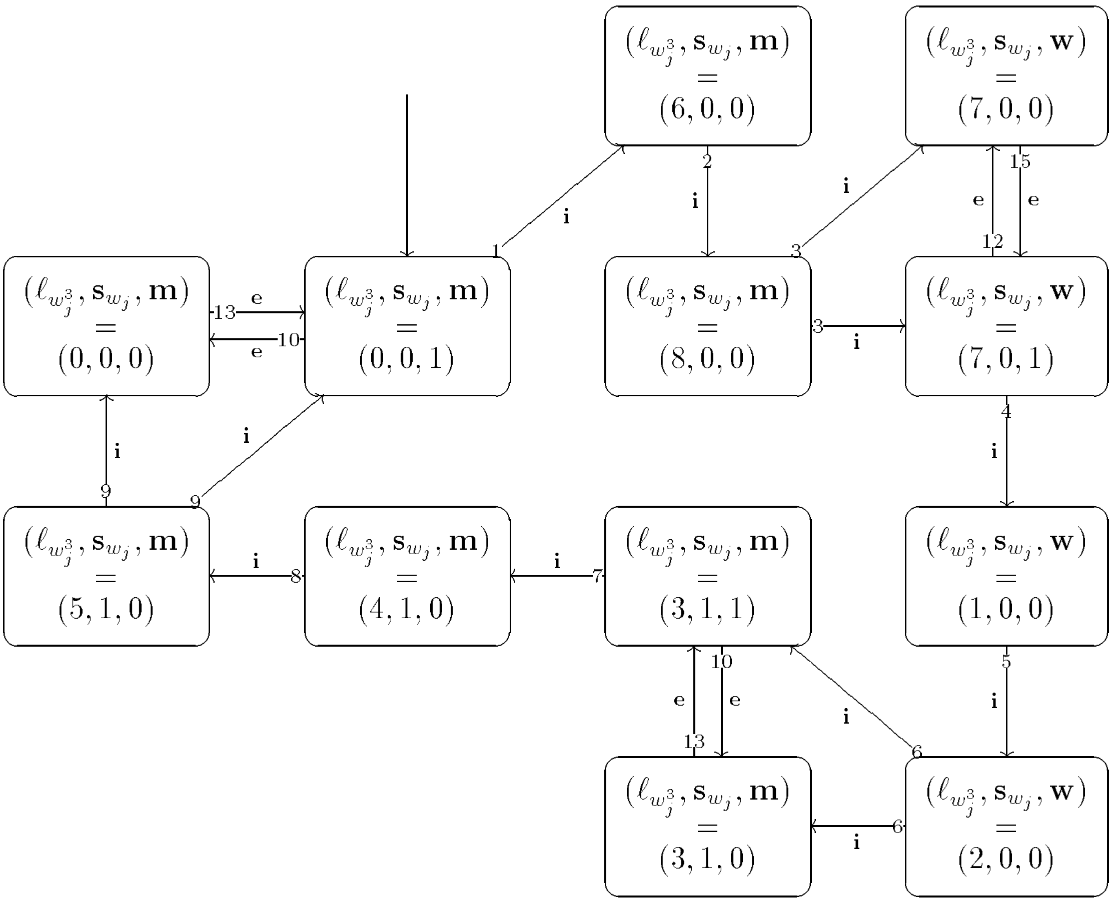

Figure 3.8: Transitions of writer^3_j.

4. **Liveness:**
   $\mathrm{L}_{w^3_j}$ expresses that the P- and V-operations on the semaphores $\mathbf{m}$, $\mathbf{r}$ and $\mathbf{w}$ are strongly fair and all the other transitions are weakly fair.
   Let $\mathrm{WF}_{w^3_j} \triangleq \{\tau_{w^3_{j,k}} \mid k \in \{2, 5, 8\}\}$ and

$$\mathrm{SF}_{w_j^3} \triangleq \{\tau_{w_{j,k}^3} \mid k \in \{1,3,4,6,7,9,10,11,12,13,14,15\}\} \text{ then}$$

$$\mathrm{L}_{w_j^3} \triangleq \bigwedge_{\tau \in \mathrm{WF}_{w_j^3}} (\Diamond\Box En(\tau) \to \Box\Diamond\tau) \wedge \bigwedge_{\tau \in \mathrm{SF}_{w_j^3}} (\Box\Diamond En(\tau) \to \Box\Diamond\tau)$$

3.5.3 Requirement W_3

The extra requirement W_3 should exclude inefficient computations caused by the nondeterminism of `CHOOSE`. So it is natural to make `CHOOSE` more deterministic, i.e., when one can choose between a `V(r)` (`V(w)`) and a `V(m)` operation priority is given to the `V(r)` (`V(w)`) operation. Let q_3 be defined as

$$\begin{array}{ll} & (\mathbf{m} = 1 \wedge \mathbf{bm} > 0 \wedge \neg(\mathbf{aw} = 0 \wedge \mathbf{br} > 0) \wedge \neg(\mathbf{aw} = 0 \wedge \mathbf{ar} = 0 \wedge \mathbf{bw} > 0) \\ \vee & (\mathbf{r} = 1 \wedge \mathbf{aw} = 0 \wedge \mathbf{br} > 0) \\ \vee & (\mathbf{w} = 1 \wedge \mathbf{aw} = 0 \wedge \mathbf{ar} = 0 \wedge \mathbf{bw} > 0) \end{array}$$

Then W_3 is as follows

$$\mathrm{W}_3 \triangleq \Box\left((\bigwedge_{i=1}^{N} \ell_{r_i^3} \in \{0,7,3\} \to q_3) \wedge (\bigwedge_{j=1}^{M} \ell_{w_j^3} \in \{0,7,3\} \to q_3) \right)$$

So in `CHOOSE` priority is given to `V(r)` and `V(w)` by strengthen the guard of `V(m)` with the complement of the guards of `V(r)` and `V(w)`. The same construction as in the previous development step is used to write this down as a machine. Let $p_3 \triangleq (\bigwedge_{i=1}^{N} \ell_{r_i^3} \in \{0,7,3\} \to q_3) \wedge (\bigwedge_{j=1}^{M} \ell_{w_j^3} \in \{0,7,3\} \to q_3)$ then $\mathrm{W}_3 = p_3 \wedge \Box((p_3 \wedge p_3') \vee \mathbf{stut}_3)$. Again the liveness part of W_3 equals **true**.

3.5.4 $\mathcal{S}_3$ relatively refines $\mathcal{S}_2$

Since the semaphores **m**, **r** and **w**, and the shared variables **ar**, **aw**, **br**, **bw** and **bm** are used only by the subcomponents of $\mathcal{S}_3$ and the semaphores **m**, **w** and **r** and the shared variables **ar** and **aw** only by the subcomponents of $\mathcal{S}_2$, we should prove $\mathcal{S}_3 \restriction \{\mathbf{m},\mathbf{w},\mathbf{r},\mathbf{ar},\mathbf{aw},\mathbf{br},\mathbf{bw},\mathbf{bm}\}$ relatively refines $\mathcal{S}_2 \restriction \{\mathbf{m},\mathbf{w},\mathbf{r},\mathbf{ar},\mathbf{aw}\}$. According to definition 35, 36 and theorem 8 $\mathcal{S}_3 \restriction \{\mathbf{m},\mathbf{w},\mathbf{r},\mathbf{ar},\mathbf{aw},\mathbf{br},\mathbf{bw},\mathbf{bm}\}$ relatively refines $\mathcal{S}_2 \restriction \{\mathbf{m},\mathbf{w},\mathbf{r},\mathbf{ar},\mathbf{aw}\}$ with respect to $(\mathrm{W}_3, \mathrm{W}_2)$ iff the following holds:

$$\begin{array}{l} \mathfrak{D}(B_3) = \mathfrak{D}(B_2) \text{ and} \\ \models (\exists \mathrm{X}_3\,.\,(\mathrm{G}_3 \wedge (\epsilon = \mathbf{e} \Rightarrow (\mathrm{m},\mathbf{r},\mathbf{w},\mathrm{ar},\mathrm{aw},\mathrm{br},\mathrm{bw},\mathrm{bm})' = (\mathrm{m},\mathbf{r},\mathbf{w},\mathrm{ar},\mathrm{aw},\mathrm{br},\mathrm{bw},\mathrm{bm})))) \\ \quad \to \\ \quad (\exists \mathrm{X}_2\,.\,(\mathrm{G}_2 \wedge (\epsilon = \mathbf{e} \Rightarrow (\mathrm{m},\mathbf{r},\mathbf{w},\mathrm{ar},\mathrm{aw})' = (\mathrm{m},\mathbf{r},\mathbf{w},\mathrm{ar},\mathrm{aw})))) \end{array}$$

where X_3 are the local variables from $\mathcal{S}_3$, i.e., $\mathrm{X}_3 \triangleq \{\ell_{r_i^3} \mid i = 1,\ldots,N\} \cup \{\ell_{w_j^3} \mid j = 1,\ldots,M\} \cup \{\mathrm{m},\mathbf{r},\mathbf{w},\mathrm{aw},\mathrm{ar},\mathrm{br},\mathrm{bw},\mathrm{bm}\}$ and G_3 is the composition of $\mathcal{S}_{r_i^3}$ $(i = 1,\ldots,N)$ and $\mathcal{S}_{w_j^3}$ $(j = 1,\ldots,M)$ and W_3,

let $\bar{\epsilon}_3 \triangleq e_{3,1},\ldots,\epsilon_{3,N},\epsilon_{3,N+1},\ldots,\epsilon_{3,N+M}$, and

let $\bar{B}_3^A \triangleq B^A_{r_1^3}, \ldots, B^A_{r_N^3}, B^A_{w_1^3}, \ldots, B^A_{w_M^3}$
then $\mathrm{G}_3 \triangleq$

$$\left(\exists \bar{\epsilon}_3.\ \odot_{\bar{B}_3^A}(\epsilon, \bar{\epsilon}_3) \wedge \bigwedge_{i=1}^N \mathrm{H}_{r_i^3}[\epsilon_{3,i}/\epsilon] \wedge \bigwedge_{j=1}^M \mathrm{H}_{w_j^3}[\epsilon_{3,N+j}/\epsilon]\right) \wedge \mathrm{W}_3$$

X_2 are the local variables from $\mathcal{S}_2$, i.e., $\mathrm{X}_2 \triangleq \{\ell_{r_i^2} \mid i = 1, \ldots, N\} \cup \{\ell_{w_j^2} \mid j = 1, \ldots, M\} \cup \{\mathbf{m}, \mathbf{r}, \mathbf{w}, \mathbf{ar}, \mathbf{aw}\}$ and G_2 is the composition of $\mathcal{S}_{r_i^2}$ $(i = 1, \ldots, N)$ and $\mathcal{S}_{w_j^2}$ $(j = 1, \ldots, M)$ and W_2,
let $\bar{\epsilon}_2 \triangleq \epsilon_{2,1}, \ldots, \epsilon_{2,N}, \epsilon_{2,N+1}, \ldots, \epsilon_{2,N+M}$, and
let $\bar{B}_2^A \triangleq B^A_{r_1^2}, \ldots, B^A_{r_N^2}, B^A_{w_1^2}, \ldots, B^A_{w_M^2}$
then $\mathrm{G}_2 \triangleq$

$$\left(\exists \bar{\epsilon}_2.\ \odot_{\bar{B}_2^A}(\epsilon, \bar{\epsilon}_2) \wedge \bigwedge_{i=1}^N \mathrm{H}_{r_i^2}[\epsilon_{2,i}/\epsilon] \wedge \bigwedge_{j=1}^M \mathrm{H}_{w_j^2}[\epsilon_{2,N+j}/\epsilon]\right) \wedge \mathrm{W}_2$$

As seen in the previous development step W_2 is ϵ-free but can not be decomposed into sub-requirements. W_3 is ϵ-free and can be decomposed into sub-requirements. Let $p_{ri} \triangleq (\ell_{r_i^3} \in \{0, 7, 3\} \to q_3)$ and $\mathrm{W}_{r_i^3} \triangleq \Box p_{ri}$, and $p_{wj} \triangleq (\ell_{w_j^3} \in \{0, 7, 3\} \to q_3)$ and $\mathrm{W}_{w_j^3} \triangleq \Box p_{wj}$ then $\mathrm{W}_3 = (\bigwedge_{i=1}^N \mathrm{W}_{r_i^3}) \wedge (\bigwedge_{j=1}^M \mathrm{W}_{w_j^3})$. Now Lemma 9, 10 and 11 can be used for the proof, i.e., following proof rule can be used

$$\begin{array}{ll}
W_3 \subseteq \bigcap_{i=1}^N W_{r_i^3} \cap \bigcap_{j=1}^M W_{w_j^3} & \\
\mathcal{S}_{r_i^3}\ {}_{W_{r_i^3}}\mathbf{ref}^{W_2}\ \mathcal{S}_{r_i^2} & W_{r_i^3} \text{ constraining } B_{r_i^3} \\
\mathcal{S}_{w_j^3}\ {}_{W_{w_j^3}}\mathbf{ref}^{W_2}\ \mathcal{S}_{w_j^2} & W_{w_j^3} \text{ constraining } B_{w_j^3} \\
\hline
\mathcal{S}_3\ {}_{W_3}\mathbf{ref}^{W_2}\ \mathcal{S}_2 &
\end{array}$$

This means we have to prove for $i = 1, \ldots, N$ and $j = 1, \ldots, M$:

$$\begin{array}{ll}
(1) & \left(\exists \mathrm{X}_{r_i^3}.(\mathrm{H}_{r_i^2} \wedge \mathrm{W}_{r_i^3})\right) \to \left(\exists \mathrm{X}_{r_i^2}.(\mathrm{H}_{r_i^2} \wedge \mathrm{W}_2)\right) \\
(2) & \left(\exists \mathrm{X}_{w_j^3}.(\mathrm{H}_{w_j^3} \wedge \mathrm{W}_{w_j^3})\right) \to \left(\exists \mathrm{X}_{w_j^2}.(\mathrm{H}_{w_j^2} \wedge \mathrm{W}_2)\right) \\
(3) & \mathrm{W}_3 \to (\mathrm{W}_{r_i^3} \wedge \mathrm{W}_{w_j^3})
\end{array}$$

ad (1) Rule 3 will be used to prove (1). This means one has to prove (a), (b) and (c) below, for $\bar{f}$ the refinement mapping from $\mathcal{S}_3$ to $\mathcal{S}_2$, defined as: $\bar{f} = f_{\ell_{r_i^2}}, f_{\mathrm{m}}, f_{\mathrm{r}}, f_{\mathrm{w}}, f_{\mathrm{aw}}, f_{\mathrm{ar}}$ where $f_{\ell_{r_i^2}}$ is defined as

$$\begin{array}{l}
if \\
\quad \ell_{r_i^3} = 8 \quad then \quad \ell_{r_i^3} - 2 \\
\quad \ell_{r_i^2} \neq 8 \quad then \quad \ell_{r_i^3} \\
fi
\end{array}$$

, i.e., the updating of bm and br in the first PV-section in reader$_i^3$ is a stuttering step in reader$_i^2$. Note: the refinement mappings for m, r, w, aw and ar are equal to the identity mapping, so we can leave them out.

$$\begin{array}{lll}
(a) & \mathcal{S}_3 \cap Hist(\mathrm{W}_3) \models & (\mathrm{I}_{r_i^3} \wedge p_{ri}) \rightarrow (\mathrm{I}_{r_i^2} \wedge p_2) \left[\bar{f}/\mathrm{X}_2\right] \\
(b) & \mathcal{S}_3 \cap Hist(\mathrm{W}_3) \models & \mathrm{T}_{r_i^3} \wedge ((p_{ri} \wedge p'_{ri}) \vee \mathbf{stut}_{r_i^3}) \\
 & & \rightarrow (\mathrm{T}_{r_i^2} \wedge ((p_2 \wedge p'_2) \vee \mathbf{stut}_2)) \left[\bar{f}/\mathrm{X}_2\right] \\
(c) & \mathcal{S}_3 \cap Hist(\mathrm{W}_3) \models & \mathrm{L}_{r_i^2} \left[\bar{f}/\mathrm{X}_2\right]
\end{array}$$

(a) **Proof 5**

$$\begin{array}{ll}
 & \mathrm{I}_{r_i^3} \wedge p_{ri} \\
= & \quad \%\ \ Def.\ \mathrm{I}_{r_i^3}, p_{ri} \\
 & (\mathrm{m}, \mathrm{bm}, \mathrm{r}, \mathrm{br}, \mathrm{w}, \mathrm{bw}, \mathrm{ar}, \mathrm{aw}, \mathbf{s}_{r_i}, \ell_{r_i^3}) = (1, N+M, 0,0,0,0,0,0,0,0) \\
\rightarrow & \quad \%\ \ Def.\ f_{\ell_{r_i^3}}, \\
 & \qquad \mathrm{bm} = \sharp(k : 1 \leq k \leq N : \ell_{r_k^3} \in \{0, \ldots, 5\}) + \\
 & \qquad\ \ \sharp(n : 1 \leq n \leq M : \ell_{w_n^3} \in \{0,1,2,3,4,5\}) \\
 & \qquad \mathrm{br} = \sharp(k : 1 \leq k \leq N : \ell_{r_k^3} \in \{6,7,8\}) \\
 & \qquad \mathrm{bw} = \sharp(n : 1 \leq n \leq M : \ell_{w_n^3} \in \{6,7,8\}) \\
 & ((\mathrm{m}, \mathrm{r}, \mathrm{w}, \mathrm{ar}, \mathrm{aw}, \mathbf{s}_{r_i}, \ell_{r_i^2}) = (1,0,0,0,0,0,0) \wedge p_2) \left[\bar{f}/\mathrm{X}_2\right] \\
= & \quad \%\ \ Def.\ \mathrm{I}_{r_i^2} \\
 & (\mathrm{I}_{r_i^2} \wedge p_2) \left[\bar{f}/\mathrm{X}_2\right]
\end{array}$$

(b) **Proof 6**

Since $\mathrm{T}_{r_i^2}$ *is of the form* $\mathbf{stut}_{r_i^2} \vee \bigvee_\tau(\epsilon = \mathbf{a}_\tau \wedge trans_\tau)$ *then* $\mathrm{T}_{r_i^2} \wedge ((p_2 \wedge p'_2) \vee \mathbf{stut}_2)$ *is equal to* $\mathbf{stut}_{r_i^2} \vee \bigvee_\tau(\epsilon = \mathbf{a}_\tau \wedge trans_\tau \wedge p_2 \wedge p'_2)$. $\mathrm{T}_{r_i^3}$ *is of the form* $\mathbf{stut}_{r_i^3} \vee \bigvee_\tau(\epsilon = \mathbf{a}_\tau \wedge trans_\tau)$ *so* $\mathrm{T}_{r_i^3} \wedge ((p_{ri} \wedge p'_{ri}) \vee \mathbf{stut}_{r_i^3})$ *is equal to* $\mathbf{stut}_{r_i^3} \vee \bigvee_\tau(\epsilon = \mathbf{a}_\tau \wedge trans_\tau \wedge p_{ri} \wedge p'_{ri})$.

–
$$\begin{array}{ll}
 & \tau_{r_{i,1}^3} \wedge p_{ri} \wedge p'_{ri} \\
= & \left(\epsilon = \mathbf{i} \wedge (\ell_{r_i^3}, \mathrm{m}) = (0,1) \wedge p_{ri} \wedge p'_{ri} \wedge \Psi'_3 = \Psi_3 \left[0, 6/\mathrm{m}, \ell_{r_i^3}\right]\right) \\
\rightarrow & \left(\epsilon = \mathbf{i} \wedge (\ell_{r_i^2}, \mathrm{m}) = (0,1) \wedge p_2 \wedge p'_2 \wedge \Psi'_2 = \Psi_2 \left[0, 6/\mathrm{m}, \ell_{r_i^2}\right]\right) \left[\bar{f}/\mathrm{X}_2\right] \\
= & (\tau_{r_{i,1}^2} \wedge p_2 \wedge p'_2) \left[\bar{f}/\mathrm{X}_2\right]
\end{array}$$

The first P-operation of $reader_i^3$ *corresponds with the first P-operation of* $reader_i^2$.

–
$$\begin{array}{ll}
 & \tau_{r_{i,2}^3} \wedge p_{ri} \wedge p'_{ri} \\
= & \left(\epsilon = \mathbf{i} \wedge \ell_{r_i^3} = 6 \wedge p_{ri} \wedge p'_{ri} \wedge \Psi'_3 = \Psi_3 \left[\mathrm{bm}-1, \mathrm{br}+1, 8/\mathrm{bm}, \mathrm{br}, \ell_{r_i^3}\right]\right) \\
\rightarrow & \left(\epsilon = \mathbf{i} \wedge \Psi'_2 = \Psi_2\right) \left[\bar{f}/\mathrm{X}_2\right] \\
\rightarrow & \mathbf{stut}_{r_i^2} \left[\bar{f}/\mathrm{X}_2\right]
\end{array}$$

The updating of br *and* bm *in* $reader_i^3$ *is an stuttering step in* $reader_i^2$.

–
$$\begin{array}{ll}
 & \tau_{r_{i,3}^3} \wedge p_{ri} \wedge p'_{ri} \\
= & \left(\epsilon = \mathbf{i} \wedge \ell_{r_i^3} = 8 \wedge p_{ri} \wedge p'_{ri} \wedge CHO(7)\right) \\
\rightarrow & \left(\epsilon = \mathbf{i} \wedge \ell_{r_i^2} = 6 \wedge p_2 \wedge p'_2 \wedge CHO(7)\right) \left[\bar{f}/\mathrm{X}_2\right] \\
= & (\tau_{r_{i,2}^2} \wedge p_2 \wedge p'_2) \left[\bar{f}/\mathrm{X}_2\right]
\end{array}$$

The first V-operation of $reader_i^3$ *corresponds to the first V-operation of* $reader_i^2$.

$$
\begin{array}{lll}
- & & \tau_{r^3_{i,4}} \wedge p_{ri} \wedge p'_{ri} \\
& = & \left(\epsilon = \mathbf{i} \wedge (\ell_{r^3_i}, \mathrm{r}) = (7,1) \wedge p_{ri} \wedge p'_{ri} \wedge \Psi'_3 = \Psi_3 \left[0, 1/\mathrm{r}, \ell_{r^3_i}\right]\right) \\
& \rightarrow & \left(\epsilon = \mathbf{i} \wedge (\ell_{r^2_i}, \mathrm{r}) = (7,1) \wedge p_2 \wedge p'_2 \wedge \Psi'_2 = \Psi_2 \left[0, 1/\mathrm{r}, \ell_{r^2_i}\right]\right) \left[\bar{f}/\mathrm{X}_2\right] \\
& = & \left(\tau_{r^2_{i,3}} \wedge p_2 \wedge p'_2\right) \left[\bar{f}/\mathrm{X}_2\right]
\end{array}
$$

The second P-operation of $reader_i^3$ *corresponds to the second P-operation of* $reader_i^2$.

$$
\begin{array}{lll}
- & & \tau_{r^3_{i,5}} \wedge p_{ri} \wedge p'_{ri} \\
& = & \left(\epsilon = \mathbf{i} \wedge \ell_{r^3_i} = 1 \wedge p_{ri} \right. \\
& & \left. \wedge\, p'_{ri} \wedge \Psi'_3 = \Psi_3 \left[\mathrm{br} - 1, \mathrm{ar} + 1, \mathrm{bm} + 1, 2/\mathrm{br}, \mathrm{ar}, \mathrm{bm}, \ell_{r^3_i}\right]\right) \\
& \rightarrow & \left(\epsilon = \mathbf{i} \wedge \ell_{r^2_i} = 1 \wedge p_2 \wedge p'_2 \wedge \Psi'_2 = \Psi_2 \left[\mathrm{ar} + 1, 2/\mathrm{ar}, \ell_{r^2_i}\right]\right) \left[\bar{f}/\mathrm{X}_2\right] \\
& = & \left(\tau_{r^2_{i,4}} \wedge p_2 \wedge p'_2\right) \left[\bar{f}/\mathrm{X}_2\right]
\end{array}
$$

The ar *decrement step of* $reader_i^3$ *corresponds to the* ar *decrement step of* $reader_i^2$.

$$
\begin{array}{lll}
- & & \tau_{r^3_{i,6}} \wedge p_{ri} \wedge p'_{ri} \\
& = & \left(\epsilon = \mathbf{i} \wedge \ell_{r^3_i} = 2 \wedge p_{ri} \wedge p'_{ri} \wedge CHO(3) \wedge \Psi'_3 = \Psi_3 \left[1/\mathrm{s}_{r_i}\right]\right) \\
& \rightarrow & \left(\epsilon = \mathbf{i} \wedge \ell_{r^2_i} = 2 \wedge p_2 \wedge p'_2 \wedge CHO(3) \wedge \Psi'_2 = \Psi_2 \left[1/\mathrm{s}_{r_i}\right]\right) \left[\bar{f}/\mathrm{X}_2\right] \\
& = & \left(\tau_{r^2_{i,5}} \wedge p_2 \wedge p'_2\right) \left[\bar{f}/\mathrm{X}_2\right]
\end{array}
$$

If $reader_i^3$ *becomes critical then* $reader_i^2$ *becomes critical.*

$$
\begin{array}{lll}
- & & \tau_{r^3_{i,7}} \wedge p_{ri} \wedge p'_{ri} \\
& = & \left(\epsilon = \mathbf{i} \wedge (\ell_{r^3_i}, \mathrm{m}) = (3,1) \wedge p_{ri} \wedge p'_{ri} \wedge \Psi'_3 = \Psi_3 \left[0, 4/\mathrm{m}, \ell_{r^3_i}\right]\right) \\
& \rightarrow & \left(\epsilon = \mathbf{i} \wedge (\ell_{r^2_i}, \mathrm{m}) = (3,1) \wedge p_2 \wedge p'_2 \wedge \Psi'_2 = \Psi_2 \left[0, 4/\mathrm{m}, \ell_{r^2_i}\right]\right) \left[\bar{f}/\mathrm{X}_2\right] \\
& = & \left(\tau_{r^2_{i,6}} \wedge p_2 \wedge p'_2\right) \left[\bar{f}/\mathrm{X}_2\right]
\end{array}
$$

The third P-operation of $reader_i^3$ *corresponds to the third P-operation of* $reader_i^2$.

$$
\begin{array}{lll}
- & & \tau_{r^3_{i,8}} \wedge p_{ri} \wedge p'_{ri} \\
& = & \left(\epsilon = \mathbf{i} \wedge \ell_{r^3_i} = 4 \wedge p_{ri} \wedge p'_{ri} \wedge \Psi'_3 = \Psi_3 \left[\mathrm{ar} - 1, 5/\mathrm{ar}, \ell_{r^3_i}\right]\right) \\
& \rightarrow & \left(\epsilon = \mathbf{i} \wedge \ell_{r^2_i} = 4 \wedge p_2 \wedge p'_2 \wedge \Psi'_2 = \Psi_2 \left[\mathrm{ar} - 1, 5/\mathrm{ar}, \ell_{r^2_i}\right]\right) \left[\bar{f}/\mathrm{X}_2\right] \\
& = & \left(\tau_{r^2_{i,7}} \wedge p_2 \wedge p'_2\right) \left[\bar{f}/\mathrm{X}_2\right]
\end{array}
$$

The ar *decrement step of* $reader_i^3$ *corresponds to the* ar *decrement step of* $reader_i^2$.

$$
\begin{array}{lll}
- & & \tau_{r^3_{i,9}} \wedge p_{ri} \wedge p'_{ri} \\
& = & \left(\epsilon = \mathbf{i} \wedge \ell_{r^3_i} = 5 \wedge p_{ri} \wedge p'_{ri} \wedge CHO(0) \wedge \Psi'_3 = \Psi_3 \left[0/\mathrm{s}_{r_i}\right]\right) \\
& \rightarrow & \left(\epsilon = \mathbf{i} \wedge \ell_{r^2_i} = 5 \wedge p_2 \wedge p'_2 \wedge CHO(0) \wedge \Psi'_2 = \Psi_2 \left[0/\mathrm{s}_{r_i}\right]\right) \left[\bar{f}/\mathrm{X}_2\right] \\
& = & \left(\tau_{r^2_{i,8}} \wedge p_2 \wedge p'_2\right) \left[\bar{f}/\mathrm{X}_2\right]
\end{array}
$$

The third V-operation of $reader_i^3$ *corresponds to the third V-operation of* $reader_i^2$.

– $$\begin{array}{ll} & \tau_{r^3_{i,10}} \wedge p_{ri} \wedge p'_{ri} \\ = & \big(\epsilon = \mathbf{e} \wedge \mathrm{m} = 1 \wedge p_{ri} \wedge p'_{ri} \wedge \Psi'_3 = \Psi_3\,[0/\mathrm{m}]\big) \\ \rightarrow & \big(\epsilon = \mathbf{e} \wedge \mathrm{m} = 1 \wedge p_2 \wedge p'_2 \wedge \Psi'_2 = \Psi_2\,[0/\mathrm{m}]\big)\,\big[\bar{f}/\mathrm{X}_2\big] \\ = & (\tau_{r^2_{i,9}} \wedge p_2 \wedge p'_2)\,\big[\bar{f}/\mathrm{X}_2\big] \end{array}$$
If the environment of reader^3_i executes a P-operation then the environment of reader^2_i also executes a P-operation.

– $$\begin{array}{ll} & \tau_{r^3_{i,11}} \wedge p_{ri} \wedge p'_{ri} \\ = & \big(\epsilon = \mathbf{e} \wedge \mathrm{r} = 1 \wedge p_{ri} \wedge p'_{ri} \wedge \Psi'_3 = \Psi_3\,[0/\mathrm{r}]\big) \\ \rightarrow & \big(\epsilon = \mathbf{e} \wedge \mathrm{r} = 1 \wedge p_2 \wedge p'_2 \wedge \Psi'_2 = \Psi_2\,[0/\mathrm{r}]\big)\,\big[\bar{f}/\mathrm{X}_2\big] \\ = & (\tau_{r^2_{i,10}} \wedge p_2 \wedge p'_2)\,\big[\bar{f}/\mathrm{X}_2\big] \end{array}$$
If the environment of reader^3_i executes a P-operation then the environment of reader^2_i also executes a P-operation.

– $$\begin{array}{ll} & \tau_{r^3_{i,12}} \wedge p_{ri} \wedge p'_{ri} \\ = & \big(\epsilon = \mathbf{e} \wedge \mathrm{w} = 1 \wedge p_{ri} \wedge p'_{ri} \wedge \Psi'_3 = \Psi_3\,[0/\mathrm{w}]\big) \\ \rightarrow & \big(\epsilon = \mathbf{e} \wedge \mathrm{w} = 1 \wedge p_2 \wedge p'_2 \wedge \Psi'_2 = \Psi_2\,[0/\mathrm{w}]\big)\,\big[\bar{f}/\mathrm{X}_2\big] \\ = & (\tau_{r^2_{i,11}} \wedge p_2 \wedge p'_2)\,\big[\bar{f}/\mathrm{X}_2\big] \end{array}$$
If the environment of reader^3_i executes a P-operation then the environment of reader^2_i also executes a P-operation.

– $$\begin{array}{ll} & \tau_{r^3_{i,13}} \wedge p_{ri} \wedge p'_{ri} \\ = & \big(\epsilon = \mathbf{e} \wedge \ell_{r^3_i} \in \{0,7,3\} \wedge \mathrm{m} = 0 \wedge p_{ri} \wedge p'_{ri} \wedge \Psi'_3 = \Psi_3\,[1/\mathrm{m}]\big) \\ \rightarrow & \big(\epsilon = \mathbf{e} \wedge \ell_{r^2_i} \in \{0,7,3\} \wedge \mathrm{m} = 0 \wedge p_2 \wedge p'_2 \wedge \Psi'_2 = \Psi_2\,[1/\mathrm{m}]\big)\,\big[\bar{f}/\mathrm{X}_2\big] \\ = & (\tau_{r^2_{i,12}} \wedge p_2 \wedge p'_2)\,\big[\bar{f}/\mathrm{X}_2\big] \end{array}$$
If the environment of reader^3_i executes a V-operation then the environment of reader^2_i also executes a V-operation.

– $$\begin{array}{ll} & \tau_{r^3_{i,14}} \wedge p_{ri} \wedge p'_{ri} \\ = & \big(\epsilon = \mathbf{e} \wedge \ell_{r^3_i} \in \{0,7,3\} \wedge \mathrm{r} = 0 \wedge p_{ri} \wedge p'_{ri} \wedge \Psi'_3 = \Psi_3\,[1/\mathrm{r}]\big) \\ \rightarrow & \big(\epsilon = \mathbf{e} \wedge \ell_{r^2_i} \in \{0,7,3\} \wedge \mathrm{r} = 0 \wedge p_2 \wedge p'_2 \wedge \Psi'_2 = \Psi_2\,[1/\mathrm{r}]\big)\,\big[\bar{f}/\mathrm{X}_2\big] \\ = & (\tau_{r^2_{i,13}} \wedge p_2 \wedge p'_2)\,\big[\bar{f}/\mathrm{X}_2\big] \end{array}$$
If the environment of reader^3_i executes a V-operation then the environment of reader^2_i also executes a V-operation.

– $$\begin{array}{ll} & \tau_{r^3_{i,15}} \wedge p_{ri} \wedge p'_{ri} \\ = & \big(\epsilon = \mathbf{e} \wedge \ell_{r^2_i} \in \{0,7,3\} \wedge \mathrm{w} = 0 \wedge p_{ri} \wedge p'_{ri} \wedge \Psi'_3 = \Psi_3\,[1/\mathrm{w}]\big) \\ \rightarrow & \big(\epsilon = \mathbf{e} \wedge \ell_{r^2_i} \in \{0,7,3\} \wedge \mathrm{w} = 0 \wedge p_2 \wedge p'_2 \wedge \Psi'_2 = \Psi_2\,[1/\mathrm{w}]\big)\,\big[\bar{f}/\mathrm{X}_2\big] \\ = & (\tau_{r^2_{i,14}} \wedge p_2 \wedge p'_2)\,\big[\bar{f}/\mathrm{X}_2\big] \end{array}$$
If the environment of reader^3_i executes a V-operation then the environment of reader^2_i also executes a V-operation.

– $\mathbf{stut}_{r^3_i} \rightarrow \mathbf{stut}_{r^2_i}\big[\bar{f}/\mathrm{X}_2\big]$
since $\mathbf{s}_{r_i}$ doesn't change.

(c) Let $\mathrm{WF}_{r_i^2} \triangleq \{\tau_{r_{i,k}^2} \mid k \in \{4,7\}\}$ and
$\mathrm{SF}_{r_i^2} \triangleq \{\tau_{r_{i,k}^2} \mid k \in \{1,2,3,5,6,8,9,10,11,12,13,14\}\}$ then

$$\mathrm{L}_{r_i^2} \triangleq \bigwedge_{\tau \in \mathrm{WF}_{r_i^2}} (\Diamond\Box En(\tau) \to \Box\Diamond\tau) \wedge \bigwedge_{\tau \in \mathrm{SF}_{r_i^2}} (\Box\Diamond En(\tau) \to \Box\Diamond\tau)$$

Let $\mathrm{WF}_{r_i^3} \triangleq \{\tau_{r_{i,k}^3} \mid k \in \{2,5,8\}\}$ and
$\mathrm{SF}_{r_i^3} \triangleq \{\tau_{r_{i,k}^1} \mid k \in \{1,3,4,6,7,9,10,11,12,13,14,15\}\}$ then

$$\mathrm{L}_{r_i^3} \triangleq \bigwedge_{\tau \in \mathrm{WF}_{r_i^3}} (\Diamond\Box En(\tau) \to \Box\Diamond\tau) \wedge \bigwedge_{\tau \in \mathrm{SF}_{r_i^3}} (\Box\Diamond En(\tau) \to \Box\Diamond\tau)$$

The following holds:

$$\mathcal{S}_3 \cap Hist(\mathrm{W}_3) \models \mathrm{L}_{r_i^3} \to \mathrm{L}_{r_i^2}\left[\bar{f}/\mathrm{X}_2\right]$$

since $\tau_{r_{i,1}^2}$ is relatively refined by $\tau_{r_{i,1}^3}$ and $\tau_{r_{i,2}^3}$, and $\tau_{r_{i,2}^2}$ is relatively refined by $\tau_{r_{i,3}^3}$, and $\tau_{r_{i,3}^2}$ is relatively refined by $\tau_{r_{i,4}^3}$, and $\tau_{r_{i,4}^2}$ is relatively refined by $\tau_{r_{i,5}^3}$, and $\tau_{r_{i,5}^2}$ is relatively refined by $\tau_{r_{i,6}^3}$, and $\tau_{r_{i,6}^2}$ is relatively refined by $\tau_{r_{i,7}^3}$, and $\tau_{r_{i,7}^2}$ is relatively refined by $\tau_{r_{i,8}^3}$, and $\tau_{r_{i,8}^2}$ is relatively refined by $\tau_{r_{i,9}^3}$, and $\tau_{r_{i,9}^2}$ is relatively refined by $\tau_{r_{i,10}^3}$, and $\tau_{r_{i,10}^2}$ is relatively refined by $\tau_{r_{i,11}^3}$, and $\tau_{r_{i,11}^2}$ is relatively refined by $\tau_{r_{i,12}^3}$, and $\tau_{r_{i,12}^2}$ is relatively refined by $\tau_{r_{i,13}^3}$, and $\tau_{r_{i,13}^2}$ is relatively refined by $\tau_{r_{i,14}^3}$, and $\tau_{r_{i,14}^2}$ is relatively refined by $\tau_{r_{i,15}^3}$,
So

$$\mathcal{S}_3 \cap Hist(\mathrm{W}_3) \models \mathrm{L}_{r_i^2}\left[\bar{f}/\mathrm{X}_2\right]$$

ad (2) Analogue to the proof of (1).

ad (3) This is trivial because $\mathrm{W}_3 \leftrightarrow (\bigwedge_{i=1}^{N} \mathrm{W}_{r_i^3} \wedge \bigwedge_{j=1}^{M} \mathrm{W}_{w_j^3})$.

3.6 The fourth development step

We have already seen how we can prevent reader$_i^3$ to choose wrongly between $V(r)$ and $V(w)$. Dijkstra also updates the PV-segments in such a way that only statements that are actually executed are listed. It turns out that we do not anymore need `bm`. Also the guards of `CHOOSE` get simpler. The result of this transformation is:

```
reader_i^4:
    do true → NCS;
              P(m);br:=br+1;if aw>0 → V(m) [] aw=0 →V(r) fi;
              P(r);br,ar:=br-1,ar+1;
              if br=0 → V(m) [] br>0 →V(r)fi;
              READ;
              P(m);ar:=ar-1;
```

```
                if ar>0 ∨ bw=0 →V(m) [] ar=0 ∧ bw>0 → V(w) fi
    od

writer_j^4:
    do true → NCS;
                P(m);bw:=bw+1;
                if aw>0 ∨ ar>0 → V(m) [] aw=0 ∧ ar=0 → V(w) fi;
                P(w);bw,aw:=bw-1,aw+1;V(m);
                WRITE;
                P(m);aw:=aw-1;
                if br=0 ∧ bw=0 → V(m) [] br>0 → V(r) [] bw>0 → V(w) fi
    od
```

$\mathtt{Syn}^4 \ : \ \ \|_{i=1}^{N} \ \mathtt{reader}_i^4 \ \| \ \|_{j=1}^{M} \ \mathtt{writer}_j^4$

In the following sections the DTL machine specifications $\mathcal{S}_{r_i^4}$ (corresponding to program reader_i^4) and $\mathcal{S}_{w_j^4}$ (corresponding to program writer_j^4) are given. It should be clear that the extra requirement W_4 is equal to **true** because no further requirements are imposed on $\mathcal{S}_4$.

3.6.1 Specification $\mathcal{S}_{r_i^4}$

The formal specification $\mathcal{S}_{r_i^4} \triangleq (B_{r_i^4}, \mathrm{H}_{r_i^4})$ where $\mathrm{H}_{r_i^4} \triangleq \mathrm{I}_{r_i^4} \wedge \Box \mathrm{T}_{r_i^4} \wedge \mathrm{L}_{r_i^4}$ and $B_{r_i^4}$, $\mathrm{I}_{r_i^4}$, $\mathrm{T}_{r_i^4}$ and $\mathrm{L}_{r_i^4}$ are as follows:

1. **Basis** $B_{r_i^4} = ((\mathrm{In}_{r_i^4}, \mathrm{Out}_{r_i^4}), (\mathrm{V}_{r_i^4}, \mathrm{X}_{r_i^4}))$

$$\begin{array}{lcl} \mathrm{In}_{r_i^4} & \triangleq & \emptyset, \\ \mathrm{Out}_{r_i^4} & \triangleq & \emptyset, \\ \mathrm{V}_{r_i^4} & \triangleq & \{\mathbf{m}, \mathbf{r}, \mathbf{br}, \mathbf{w}, \mathbf{bw}, \mathbf{ar}, \mathbf{aw}, \mathrm{s}_{r_i}\}, \\ \mathrm{X}_{r_i^4} & \triangleq & \{\ell_{r_i^4}\} \end{array}$$

- $\ell_{r_i^4} = 0$: reader_i^4 is non critical.
- $\ell_{r_i^4} = 6$: reader_i^4 executes first P-action on **m**.
- $\ell_{r_i^4} = 7$: reader_i^4 has updated **br**.
- $\ell_{r_i^4} = 8$: reader_i^4 has left first PV-section.
- $\ell_{r_i^4} = 1$: reader_i^4 has executed P-action on **r**.
- $\ell_{r_i^4} = 2$: reader_i^4 has updated **br** and **ar**.
- $\ell_{r_i^4} = 3$: reader_i^4 is critical.
- $\ell_{r_i^4} = 4$: reader_i^4 has executed second P-action **m**.
- $\ell_{r_i^4} = 5$: reader_i^4 has updated **ar**.

Let $\Psi_4 \triangleq (\mathbf{m}, \mathbf{r}, \mathbf{br}, \mathbf{w}, \mathbf{bw}, \mathbf{ar}, \mathbf{aw}, \mathbf{s}_{r_i}, \ell_{r_i^4})$ and
$\Psi_4' \triangleq (\mathbf{m}', \mathbf{r}', \mathbf{br}', \mathbf{w}', \mathbf{bw}', \mathbf{ar}', \mathbf{aw}', \mathbf{s}_{r_i}', \ell_{r_i^4}')$.

2. **Initial States:**

$$\mathrm{I}_{r_i^4} \triangleq \Psi_4 = (1,0,0,0,0,0,0,0,0)$$

3. **Transitions:**

$$\begin{array}{lcl}
\text{Let } CHO1(X) \triangleq & \vee & (\mathbf{aw} > 0 \wedge \Psi_4' = \Psi_4\left[1, X/\mathbf{m}, \ell_{r_i^4}\right]) \\
 & \vee & (\mathbf{aw} = 0 \wedge \Psi_4' = \Psi_4\left[1, X/\mathbf{r}, \ell_{r_i^4}\right]) \\
\text{Let } CHO2(X) \triangleq & \vee & (\mathbf{br} = 0 \wedge \Psi_4' = \Psi_4\left[1, X/\mathbf{m}, \ell_{r_i^4}\right]) \\
 & \vee & (\mathbf{br} > 0 \wedge \Psi_4' = \Psi_4\left[1, X/\mathbf{r}, \ell_{r_i^4}\right]) \\
\text{Let } CHO3(X) \triangleq & \vee & ((\mathbf{ar} > 0 \vee \mathbf{bw} = 0) \wedge \Psi_4' = \Psi_4\left[1, X/\mathbf{m}, \ell_{r_i^4}\right]) \\
 & \vee & (\mathbf{ar} = 0 \wedge \mathbf{bw} > 0 \wedge \Psi_4' = \Psi_4\left[1, X/\mathbf{w}, \ell_{r_i^4}\right])
\end{array}$$

$\mathrm{T}_{r_i^4} \triangleq$

$\tau_{r_{i,1}^4}$ $\quad \left(\epsilon = \mathbf{i} \wedge (\ell_{r_i^4}, \mathbf{m}) = (0,1) \wedge \Psi_4' = \Psi_4\left[0, 6/\mathbf{m}, \ell_{r_i^4}\right]\right)$

Reader$_i^4$ executes its first P-action on $\mathbf{m}$.

$\tau_{r_{i,2}^4}$ $\quad \vee \left(\epsilon = \mathbf{i} \wedge \ell_{r_i^4} = 6 \wedge \Psi_4' = \Psi_4\left[\mathbf{br}+1, 8/\mathbf{br}, \ell_{r_i^4}\right]\right)$

Reader$_i^4$ updates $\mathbf{br}$.

$\tau_{r_{i,3}^4}$ $\quad \vee \left(\epsilon = \mathbf{i} \wedge \ell_{r_i^4} = 8 \wedge CHO1(7)\right)$

Reader$_i^4$ leaves the first PV-section.

$\tau_{r_{i,4}^4}$ $\quad \vee \left(\epsilon = \mathbf{i} \wedge (\ell_{r_i^4}, \mathbf{r}) = (7,1) \wedge \Psi_4' = \Psi_4\left[0, 1/\mathbf{r}, \ell_{r_i^4}\right]\right)$

Reader$_i^4$ executes its P-action on $\mathbf{r}$.

$\tau_{r_{i,5}^4}$ $\quad \vee \left(\epsilon = \mathbf{i} \wedge \ell_{r_i^4} = 1 \wedge \Psi_4' = \Psi_4\left[\mathbf{br}-1, \mathbf{ar}+1, 2/\mathbf{br}, \mathbf{ar}, \ell_{r_i^4}\right]\right)$

Reader$_i^4$ updates $\mathbf{br}$ and $\mathbf{ar}$.

$\tau_{r_{i,6}^4}$ $\quad \vee \left(\epsilon = \mathbf{i} \wedge \ell_{r_i^4} = 2 \wedge CHO2(3) \wedge \Psi_4' = \Psi_4\left[1/\mathbf{s}_{r_i}\right]\right)$

Reader$_i^4$ becomes critical.

$\tau_{r_{i,7}^4}$ $\quad \vee \left(\epsilon = \mathbf{i} \wedge (\ell_{r_i^4}, \mathbf{m}) = (3,1) \wedge \Psi_4' = \Psi_4\left[0, 4/\mathbf{m}, \ell_{r_i^4}\right]\right)$

Reader$_i^4$ executes its second P-action on $\mathbf{m}$.

$\tau_{r_{i,8}^4}$ $\quad \vee \left(\epsilon = \mathbf{i} \wedge \ell_{r_i^4} = 4 \wedge \Psi_4' = \Psi_4\left[\mathbf{ar}-1, 5/\mathbf{ar}, \ell_{r_i^4}\right]\right)$

Reader$_i^4$ updates $\mathbf{ar}$.

$\tau_{r_{i,9}^4}$ $\quad \vee \left(\epsilon = \mathbf{i} \wedge \ell_{r_i^4} = 5 \wedge CHO3(0) \wedge \Psi_4' = \Psi_4\left[0/\mathbf{s}_{r_i}\right]\right)$

Reader$_i^4$ becomes non critical.

$\tau_{r_{i,10}^4}$ $\quad \vee \left(\epsilon = \mathbf{e} \wedge \mathbf{m} = 1 \wedge \Psi_4' = \Psi_4\left[0/\mathbf{m}\right]\right)$

The environment executes a P-operation on $\mathbf{m}$.

$\tau_{r^4_{i,11}}$ $\quad\vee \ \big(\epsilon = \mathbf{e} \wedge \mathbf{r} = 1 \wedge \Psi_4' = \Psi_4\,[0/\mathbf{r}]\big)$

The environment executes a P-operation on $\mathbf{r}$.

$\tau_{r^4_{i,12}}$ $\quad\vee \ \big(\epsilon = \mathbf{e} \wedge \mathbf{w} = 1 \wedge \Psi_4' = \Psi_4\,[0/\mathbf{w}]\big)$

The environment executes a P-operation on $\mathbf{w}$.

$\tau_{r^4_{i,13}}$ $\quad\vee \ \big(\epsilon = \mathbf{e} \wedge \ell_{r^4_i} \in \{0,7,3\} \wedge \mathbf{m} = 0 \wedge \Psi_4' = \Psi_4\,[1/\mathbf{m}]\big)$

The environment executes a V-operation on $\mathbf{m}$.

$\tau_{r^4_{i,14}}$ $\quad\vee \ \big(\epsilon = \mathbf{e} \wedge \ell_{r^4_i} \in \{0,7,3\} \wedge \mathbf{r} = 0 \wedge \Psi_4' = \Psi_4\,[1/\mathbf{r}]\big)$

The environment executes a V-operation on $\mathbf{r}$.

$\tau_{r^4_{i,15}}$ $\quad\vee \ \big(\epsilon = \mathbf{e} \wedge \ell_{r^4_i} \in \{0,7,3\} \wedge \mathbf{w} = 0 \wedge \Psi_4' = \Psi_4\,[1/\mathbf{w}]\big)$

The environment executes a V-operation on $\mathbf{w}$.

$\tau_{r^4_{i,0}}$ $\quad\vee \ \mathbf{stut}_{r^4_i}$

These transitions are illustrated in figure 3.9

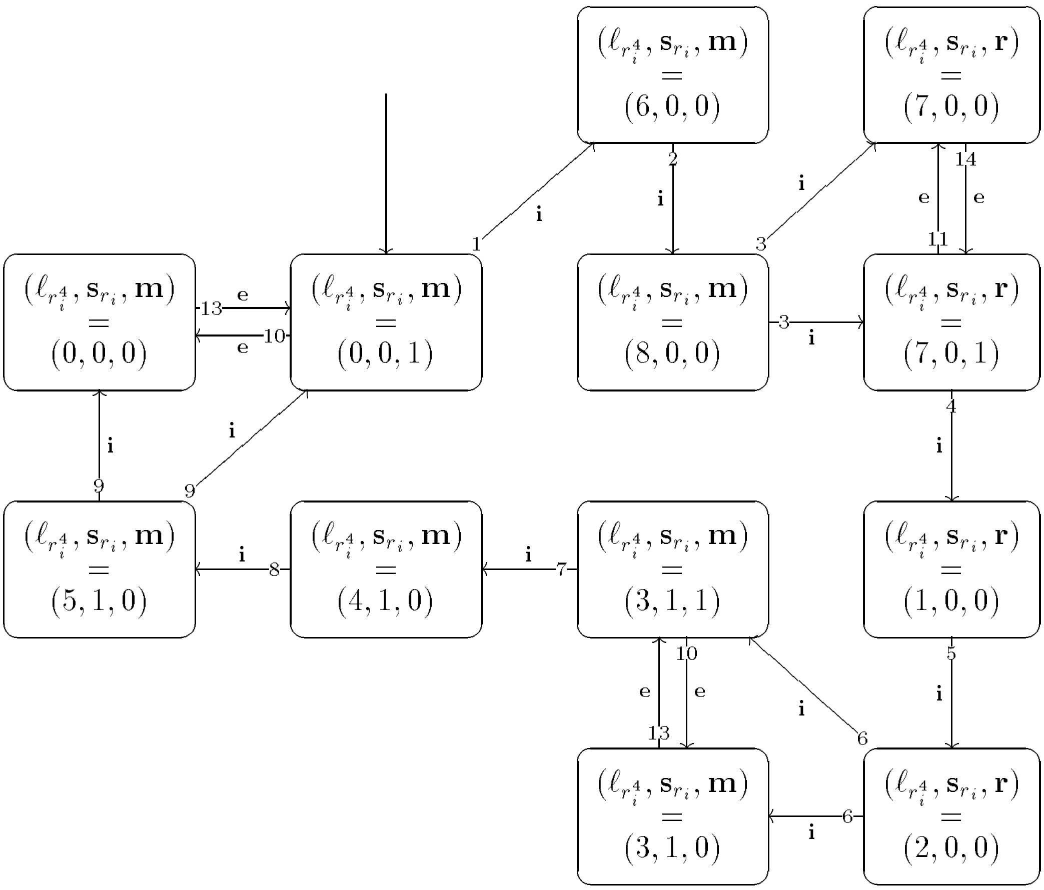

Figure 3.9: Transitions of reader^4_i.

4. **Liveness:**
$L_{r^4_i}$ expresses that the P- and V-operations on the semaphores $\mathbf{m}$, $\mathbf{r}$ and $\mathbf{w}$ are

strongly fair and all the other transitions are weakly fair.
Let $\mathrm{WF}_{r_i^4} \triangleq \{\tau_{r_{i,k}^4} \mid k \in \{2,5,8\}\}$ and
$\mathrm{SF}_{r_i^4} \triangleq \{\tau_{r_{i,k}^4} \mid k \in \{1,3,4,6,7,9,10,11,12,13,14,15\}\}$ then

$$\mathrm{L}_{r_i^4} \triangleq \bigwedge_{\tau \in \mathrm{WF}_{r_i^4}} (\Diamond\Box En(\tau) \rightarrow \Box\Diamond\tau) \wedge \bigwedge_{\tau \in \mathrm{SF}_{r_i^4}} (\Box\Diamond En(\tau) \rightarrow \Box\Diamond\tau)$$

3.6.2 Specification $\mathcal{S}_{w_j^4}$

The formal specification $\mathcal{S}_{w_j^4} \triangleq (B_{w_j^4}, \mathrm{H}_{w_j^4})$ where $\mathrm{H}_{w_j^4} \triangleq \mathrm{I}_{w_j^4} \wedge \Box\mathrm{T}_{w_j^4} \wedge \mathrm{L}_{w_j^4}$ and $B_{w_j^4}$, $\mathrm{I}_{w_j^4}$, $\mathrm{T}_{w_j^4}$ and $\mathrm{L}_{w_j^4}$ are as follows:

1. **Basis** $B_{w_j^4} = ((\mathrm{In}_{w_j^4}, \mathrm{Out}_{w_j^4}), (\mathrm{V}_{w_j^4}, \mathrm{X}_{w_j^4}))$

$$\begin{aligned}
\mathrm{In}_{w_j^4} &\triangleq \emptyset, \\
\mathrm{Out}_{w_j^4} &\triangleq \emptyset, \\
\mathrm{V}_{w_j^4} &\triangleq \{\mathbf{m}, \mathbf{r}, \mathbf{br}, \mathbf{w}, \mathbf{bw}, \mathbf{ar}, \mathbf{aw}, \mathrm{s}_{w_j}\}, \\
\mathrm{X}_{w_j^4} &\triangleq \{\ell_{w_j^4}\}
\end{aligned}$$

- $\ell_{w_j^4} = 0$: writer$_j^4$ is non critical.
- $\ell_{w_j^4} = 6$: writer$_j^4$ executes first P-action on $\mathbf{m}$.
- $\ell_{w_j^4} = 8$: writer$_j^4$ has updated $\mathbf{bw}$.
- $\ell_{w_j^4} = 7$: writer$_j^4$ has left first PV-section.
- $\ell_{w_j^4} = 1$: writer$_j^4$ has executed P-action on $\mathbf{w}$.
- $\ell_{w_j^4} = 2$: writer$_j^4$ has updated $\mathbf{bw}$ and $\mathbf{aw}$.
- $\ell_{w_j^4} = 3$: writer$_j^4$ is critical.
- $\ell_{w_j^4} = 4$: writer$_j^4$ has executed second P-action $\mathbf{m}$.
- $\ell_{w_j^4} = 5$: writer$_j^4$ has updated $\mathbf{aw}$.

Let $\Psi_4 \triangleq (\mathbf{m}, \mathbf{r}, \mathbf{br}, \mathbf{w}, \mathbf{bw}, \mathbf{ar}, \mathbf{aw}, \mathrm{s}_{w_j}, \ell_{w_j^4})$ and
$\Psi_4' \triangleq (\mathbf{m}', \mathbf{r}', \mathbf{br}', \mathbf{w}', \mathbf{bw}', \mathbf{ar}', \mathbf{aw}', \mathrm{s}_{w_j}', \ell_{w_j^4}')$.

2. **Initial States:**

$$\mathrm{I}_{w_j^4} \triangleq \Psi_4 = (1,0,0,0,0,0,0,0,0)$$

3. **Transitions:**

Let $CHO1(X) \triangleq \vee\ ((\mathbf{aw} > 0 \vee \mathbf{ar} > 0) \wedge \Psi_4' = \Psi_4\left[1, X/\mathbf{m}, \ell_{w_j^4}\right])$
$\vee\ (\mathbf{aw} = 0 \wedge \mathbf{ar} = 0 \wedge \Psi_4' = \Psi_4\left[1, X/\mathbf{w}, \ell_{w_j^4}\right])$

Let $CHO2(X) \triangleq \Psi_4' = \Psi_4\left[1, X/\mathbf{m}, \ell_{w_j^4}\right]$

Let $CHO3(X) \triangleq \vee\ (\mathbf{br} = 0 \wedge \mathbf{bw} = 0 \wedge \Psi_4' = \Psi_4\left[1, X/\mathbf{m}, \ell_{w_j^4}\right])$
$\vee\ (\mathbf{br} > 0 \wedge \Psi_4' = \Psi_4\left[1, X/\mathbf{r}, \ell_{w_j^4}\right])$
$\vee\ (\mathbf{bw} > 0 \wedge \Psi_4' = \Psi_4\left[1, X/\mathbf{w}, \ell_{w_j^4}\right])$

$\mathrm{T}_{w_j^4} \triangleq$

$\tau_{w_{i,1}^4}$ $\left(\epsilon = \mathbf{i} \wedge (\ell_{w_j^4}, \mathbf{m}) = (0,1) \wedge \Psi_4' = \Psi_4\left[0, 6/\mathbf{m}, \ell_{w_j^4}\right]\right)$
Writer$_j^4$ executes its first P-action on $\mathbf{m}$.

$\tau_{w_{i,2}^4}$ $\vee\ \left(\epsilon = \mathbf{i} \wedge \ell_{w_j^4} = 6 \wedge \Psi_4' = \Psi_4\left[\mathbf{bw} + 1, 8/\mathbf{bw}, \ell_{w_j^4}\right]\right)$
Writer$_j^4$ updates $\mathbf{bw}$.

$\tau_{w_{i,3}^4}$ $\vee\ \left(\epsilon = \mathbf{i} \wedge \ell_{w_j^4} = 8 \wedge CHO1(7)\right)$
Writer$_j^4$ leaves the first PV-section.

$\tau_{w_{i,4}^4}$ $\vee\ \left(\epsilon = \mathbf{i} \wedge (\ell_{w_j^4}, \mathbf{r}) = (7,1) \wedge \Psi_4' = \Psi_4\left[0, 1/\mathbf{w}, \ell_{w_j^4}\right]\right)$
Writer$_j^4$ executes its P-action on $\mathbf{w}$.

$\tau_{w_{i,5}^4}$ $\vee\ \left(\epsilon = \mathbf{i} \wedge \ell_{w_j^4} = 1 \wedge \Psi_4' = \Psi_4\left[\mathbf{bw} - 1, \mathbf{aw} + 1, 2/\mathbf{bw}, \mathbf{aw}, \ell_{w_j^4}\right]\right)$
Writer$_j^4$ updates $\mathbf{bw}$ and $\mathbf{aw}$.

$\tau_{w_{i,6}^4}$ $\vee\ \left(\epsilon = \mathbf{i} \wedge \ell_{w_j^4} = 2 \wedge CHO2(3) \wedge \Psi_4' = \Psi_4\left[1/\mathbf{s}_{w_j}\right]\right)$
Writer$_j^4$ becomes critical.

$\tau_{w_{i,7}^4}$ $\vee\ \left(\epsilon = \mathbf{i} \wedge (\ell_{w_j^4}, \mathbf{m}) = (3,1) \wedge \Psi_4' = \Psi_4\left[0, 4/\mathbf{m}, \ell_{w_j^4}\right]\right)$
Writer$_j^4$ executes its second P-action on $\mathbf{m}$.

$\tau_{w_{i,8}^4}$ $\vee\ \left(\epsilon = \mathbf{i} \wedge \ell_{w_j^4} = 4 \wedge \Psi_4' = \Psi_4\left[\mathbf{aw} - 1, 5/\mathbf{aw}, \ell_{w_j^4}\right]\right)$
Writer$_j^4$ updates $\mathbf{aw}$.

$\tau_{w_{i,9}^4}$ $\vee\ \left(\epsilon = \mathbf{i} \wedge \ell_{w_j^4} = 5 \wedge CHO3(0) \wedge \Psi_4' = \Psi_4\left[0/\mathbf{s}_{w_j}\right]\right)$
Writer$_j^4$ becomes non critical.

$\tau_{w_{i,10}^4}$ $\vee\ \left(\epsilon = \mathbf{e} \wedge \mathbf{m} = 1 \wedge \Psi_4' = \Psi_4\left[0/\mathbf{m}\right]\right)$
The environment executes a P-operation on $\mathbf{m}$.

$\tau_{w_{i,11}^4}$ $\vee\ \left(\epsilon = \mathbf{e} \wedge \mathbf{r} = 1 \wedge \Psi_4' = \Psi_4\left[0/\mathbf{r}\right]\right)$
The environment executes a P-operation on $\mathbf{r}$.

$\tau_{w_{i,12}^4}$ $\vee\ \left(\epsilon = \mathbf{e} \wedge \mathbf{w} = 1 \wedge \Psi_4' = \Psi_4\left[0/\mathbf{w}\right]\right)$
The environment executes a P-operation on $\mathbf{w}$.

$\tau_{w^4_{i,13}}$ $\quad \vee \; \big(\epsilon = \mathbf{e} \wedge \ell_{w^4_j} \in \{0,7,3\} \wedge \mathbf{m} = 0 \wedge \Psi'_4 = \Psi_4\,[1/\mathbf{m}]\big)$

The environment executes a V-operation on $\mathbf{m}$.

$\tau_{w^4_{i,14}}$ $\quad \vee \; \big(\epsilon = \mathbf{e} \wedge \ell_{w^4_j} \in \{0,7,3\} \wedge \mathbf{r} = 0 \wedge \Psi'_4 = \Psi_4\,[1/\mathbf{r}]\big)$

The environment executes a V-operation on $\mathbf{r}$.

$\tau_{w^4_{i,15}}$ $\quad \vee \; \big(\epsilon = \mathbf{e} \wedge \ell_{w^4_j} \in \{0,7,3\} \wedge \mathbf{w} = 0 \wedge \Psi'_4 = \Psi_4\,[1/\mathbf{w}]\big)$

The environment executes a V-operation on $\mathbf{w}$.

$\tau_{w^4_{i,0}}$ $\quad \vee \; \mathbf{stut}_{w^4_j}$

These transitions are illustrated in figure 3.10

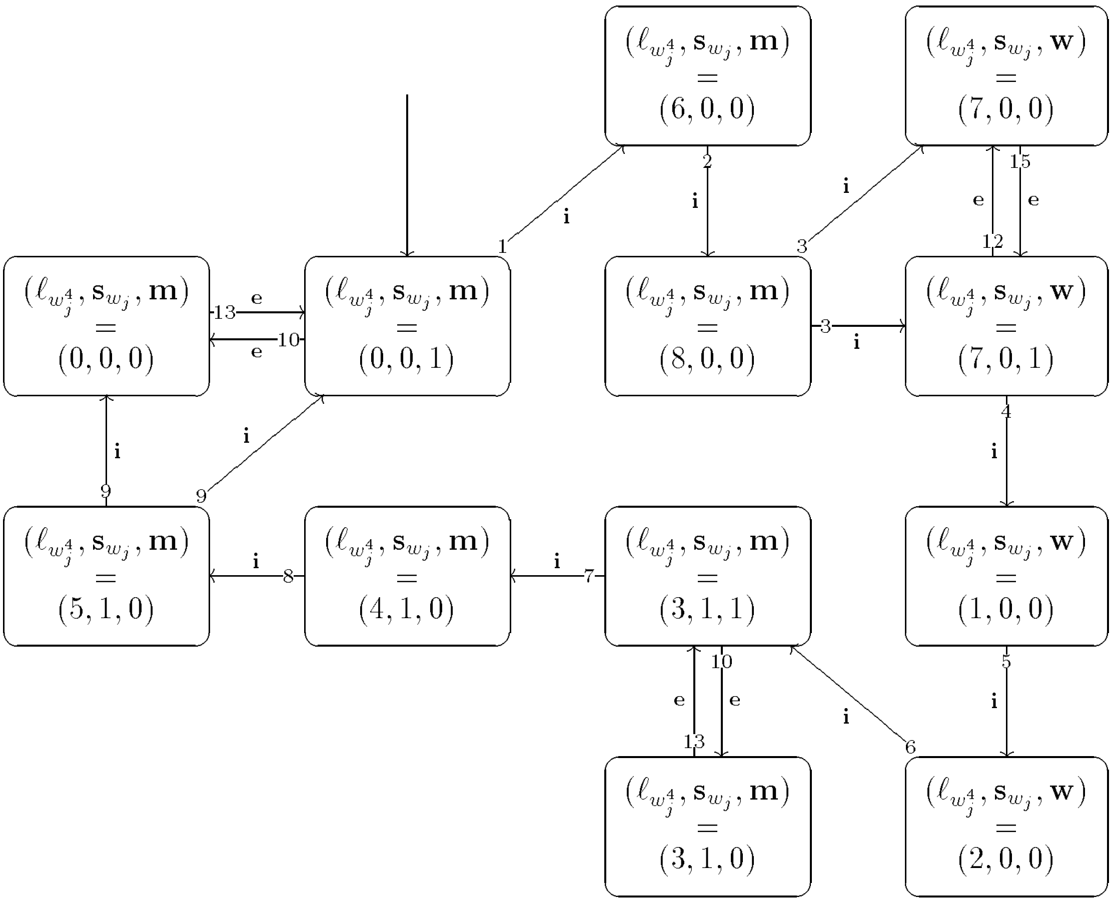

Figure 3.10: Transitions of writer^4_j.

4. **Liveness:**
   $\mathrm{L}_{w^4_j}$ expresses that the P- and V-operations on the semaphores $\mathbf{m}$, $\mathbf{r}$ and $\mathbf{w}$ are strongly fair and all the other transitions are weakly fair.
   Let $\mathrm{WF}_{w^4_j} \triangleq \{\tau_{w^4_{j,k}} \mid k \in \{2,5,8\}\}$ and

$\mathrm{SF}_{w_j^4} \triangleq \{\tau_{w_{j,k}^4} \mid k \in \{1,3,4,6,7,9,10,11,12,13,14,15\}\}$ then

$$\mathrm{L}_{w_j^4} \triangleq \bigwedge_{\tau \in \mathrm{WF}_{w_j^4}} (\Diamond\Box En(\tau) \rightarrow \Box\Diamond\tau) \wedge \bigwedge_{\tau \in \mathrm{SF}_{w_j^4}} (\Box\Diamond En(\tau) \rightarrow \Box\Diamond\tau)$$

3.6.3 $\mathcal{S}_4$ relatively refines $\mathcal{S}_3$

Since the semaphores **m**, **r** and **w**, and the shared variables **ar**, **aw**, **br**, **bw** and **bm** are used only by the subcomponents of $\mathcal{S}_3$ and the semaphores **m**, **w** and **r** and the shared variables **ar**, **aw**, **br** and **bw** only by the subcomponents of $\mathcal{S}_4$, we should prove $\mathcal{S}_4 \restriction \{\mathbf{m}, \mathbf{w}, \mathbf{r}, \mathbf{ar}, \mathbf{aw}, \mathbf{br}, \mathbf{bw}\}$ relatively refines $\mathcal{S}_3 \restriction \{\mathbf{m}, \mathbf{w}, \mathbf{r}, \mathbf{ar}, \mathbf{aw}, \mathbf{bm}, \mathbf{br}, \mathbf{bw}\}$. According to definition 35, 36 and theorem 8 $\mathcal{S}_4 \restriction \{\mathbf{m}, \mathbf{w}, \mathbf{r}, \mathbf{ar}, \mathbf{aw}, \mathbf{br}, \mathbf{bw}\}$ relatively refines $\mathcal{S}_3 \restriction \{\mathbf{m}, \mathbf{w}, \mathbf{r}, \mathbf{ar}, \mathbf{aw}, \mathbf{br}, \mathbf{bw}, \mathbf{bm}\}$ with respect to $(\mathrm{W}_4, \mathrm{W}_3)$ iff the following holds:

$$\mathfrak{D}(B_4) = \mathfrak{D}(B_3) \text{ and}$$
$$\models (\exists \mathrm{X}_4 \,.\, (\mathrm{G}_4 \wedge (\epsilon = \mathbf{e} \Rightarrow (\mathrm{m}, \mathbf{r}, \mathbf{w}, \mathrm{ar}, \mathrm{aw}, \mathrm{br}, \mathrm{bw})' = (\mathrm{m}, \mathbf{r}, \mathbf{w}, \mathrm{ar}, \mathrm{aw}, \mathrm{br}, \mathrm{bw}))))$$
$$\rightarrow$$
$$(\exists \mathrm{X}_3 \,.\, (\mathrm{G}_3 \wedge (\epsilon = \mathbf{e} \Rightarrow (\mathrm{m}, \mathbf{r}, \mathbf{w}, \mathrm{ar}, \mathrm{aw}, \mathrm{br}, \mathrm{bw}, \mathrm{bm})' = (\mathrm{m}, \mathbf{r}, \mathbf{w}, \mathrm{ar}, \mathrm{aw}, \mathrm{br}, \mathrm{bw}, \mathrm{bm}))))$$

where X_4 are the local variables from $\mathcal{S}_4$, i.e., $\mathrm{X}_4 \triangleq \{\ell_{r_i^4} \mid i = 1, \ldots, N\} \cup \{\ell_{w_j^4} \mid j = 1, \ldots, M\} \cup \{\mathrm{m}, \mathbf{r}, \mathbf{w}, \mathrm{aw}, \mathrm{ar}, \mathrm{br}, \mathrm{bw}\}$ and G_4 is the composition of $\mathcal{S}_{r_i^4}$ $(i = 1, \ldots, N)$ and $\mathcal{S}_{w_j^4}$ $(j = 1, \ldots, M)$,

let $\bar{\epsilon}_4 \triangleq \epsilon_{4,1}, \ldots, \epsilon_{4,N}, \epsilon_{4,N+1}, \ldots, \epsilon_{4,N+M}$, and

let $\bar{B}_4^A \triangleq B_{r_1^4}^A, \ldots, B_{r_N^4}^A, B_{w_1^4}^A, \ldots, B_{w_M^4}^A$

then $\mathrm{G}_4 \triangleq$

$$\left(\exists \bar{\epsilon}_4 .\ \odot_{\bar{B}_4^A} (\epsilon, \bar{\epsilon}_4) \wedge \textstyle\bigwedge_{i=1}^N \mathrm{H}_{r_i^4} [\epsilon_{4,i}/\epsilon] \wedge \bigwedge_{j=1}^M \mathrm{H}_{w_j^4} [\epsilon_{4,N+j}/\epsilon]\right)$$

X_3 are the local variables from $\mathcal{S}_3$, i.e., $\mathrm{X}_3 \triangleq \{\ell_{r_i^3} \mid i = 1, \ldots, N\} \cup \{\ell_{w_j^3} \mid j = 1, \ldots, M\} \cup \{\mathbf{m}, \mathbf{r}, \mathbf{w}, \mathbf{ar}, \mathbf{aw}, \mathbf{br}, \mathbf{bm}, \mathbf{bw}\}$ and G_3 is the composition of $\mathcal{S}_{r_i^3}$ $(i = 1, \ldots, N)$ and $\mathcal{S}_{w_j^3}$ $(j = 1, \ldots, M)$ and W_3,

let $\bar{\epsilon}_3 \triangleq \epsilon_{3,1}, \ldots, \epsilon_{3,N}, \epsilon_{3,N+1}, \ldots, \epsilon_{3,N+M}$, and

let $\bar{B}_3^A \triangleq B_{r_1^3}^A, \ldots, B_{r_N^3}^A, B_{w_1^3}^A, \ldots, B_{w_M^3}^A$

then $\mathrm{G}_3 \triangleq$

$$\left(\exists \bar{\epsilon}_3 .\ \odot_{\bar{B}_3^A} (\epsilon, \bar{\epsilon}_3) \wedge \textstyle\bigwedge_{i=1}^N \mathrm{H}_{r_i^3} [\epsilon_{3,i}/\epsilon] \wedge \bigwedge_{j=1}^M \mathrm{H}_{w_j^3} [\epsilon_{3,N+j}/\epsilon]\right) \wedge \mathrm{W}_3$$

As seen in the previous development step W_3 is ϵ-free and can be decomposed into sub-requirements. Let $p_{ri} \triangleq (\ell_{r_i^3} \in \{0,7,3\} \rightarrow q_3)$ and $\mathrm{W}_{r_i^3} \triangleq \Box p_{ri}$, and $p_{wj} \triangleq (\ell_{w_j^3} \in \{0,7,3\} \rightarrow q_3)$ and $\mathrm{W}_{w_j^3} \triangleq \Box p_{wj}$ then $\mathrm{W}_3 = (\bigwedge_{i=1}^N \mathrm{W}_{r_i^3}) \wedge (\bigwedge_{j=1}^M \mathrm{W}_{w_j^3})$. Now Lemma 9, 10 and 11 can be used for the proof, i.e., following proof rule can be used

$$\dfrac{\begin{array}{ll} \bigcap_{i=1}^N W_{r_i^3} \cap \bigcap_{j=1}^M W_{w_j^3} \subseteq W_3 & \\ \mathcal{S}_{r_i^3} \ {}_{W_{r_i^3}}\mathbf{ref}^{\,W_2}\ \mathcal{S}_{r_i^2} & W_{r_i^3} \text{ constraining } B_{r_i^3} \\ \mathcal{S}_{w_j^3} \ {}_{W_{w_j^3}}\mathbf{ref}^{\,W_2}\ \mathcal{S}_{w_j^2} & W_{w_j^3} \text{ constraining } B_{w_j^3} \end{array}}{\mathcal{S}_4 \ {}_{\mathcal{H}}\mathbf{ref}^{\,W_2}\ \mathcal{S}_3}$$

This means we have to prove for $i = 1, \ldots, N$ and $j = 1, \ldots, M$:

$$
\begin{array}{ll}
(1) & \left(\exists \mathrm{X}_{r_i^4} . (\mathrm{H}_{r_i^4})\right) \rightarrow \left(\exists \mathrm{X}_{r_i^3} . (\mathrm{H}_{r_i^3} \wedge \mathrm{W}_{r_i^3})\right) \\
(2) & \left(\exists \mathrm{X}_{w_j^4} . (\mathrm{H}_{w_j^4})\right) \rightarrow \left(\exists \mathrm{X}_{w_j^3} . (\mathrm{H}_{w_j^3} \wedge \mathrm{W}_{w_j^3})\right) \\
(3) & (\mathrm{W}_{r_i^3} \wedge \mathrm{W}_{w_j^3}) \rightarrow \mathrm{W}_3
\end{array}
$$

ad (1) Rule 3 will be used to prove (1). This means one has to prove (a), (b) and (c) below, for $\bar{f}$ the refinement mapping from $\mathcal{S}_4$ to $\mathcal{S}_3$, defined as: $\bar{f} = f_{\ell_{r_i^3}}, f_{\mathrm{m}}, f_{\mathrm{r}}, f_{\mathrm{w}}, f_{\mathrm{aw}}, f_{\mathrm{ar}}, f_{\mathrm{br}}, f_{\mathrm{bw}}, f_{\mathrm{bm}}$ where f_{bm} is defined as

$$N + M - \mathrm{br} - \mathrm{bw}$$

, i.e., bm can be expressed in terms of br and bw. Note: the refinement mappings for $ltr4$, m, r, w, aw, ar, br and bw are equal to the identity mapping, so we can leave them out.

$$
\begin{array}{lll}
(a) & \mathcal{S}_4 \models & \mathrm{I}_{r_i^4} \rightarrow (\mathrm{I}_{r_i^3} \wedge p_{ri}) \left[\bar{f}/\mathrm{X}_3\right] \\
(b) & \mathcal{S}_3 \models & \mathrm{T}_{r_i^4} \rightarrow (\mathrm{T}_{r_i^3} \wedge ((p_{ri} \wedge p'_{ri}) \vee \mathbf{stut}_{r_i^3})) \left[\bar{f}/\mathrm{X}_3\right] \\
(c) & \mathcal{S}_3 \models & \mathrm{L}_{r_i^3} \left[\bar{f}/\mathrm{X}_3\right]
\end{array}
$$

(a) **Proof 7**

$$
\begin{array}{ll}
 & \mathrm{I}_{r_i^4} \\
= & \quad \%\ \ Def.\ \mathrm{I}_{r_i^4} \\
 & (\mathrm{m}, \mathrm{r}, \mathrm{br}, \mathrm{w}, \mathrm{bw}, \mathrm{ar}, \mathrm{aw}, \mathbf{s}_{r_i}, \ell_{r_i^3}) = (1,0,0,0,0,0,0,0,0) \\
\rightarrow & \quad \%\ \ Def.\ f_{\mathrm{bm}} \\
 & ((\mathrm{m}, \mathrm{bm}, \mathrm{r}, \mathrm{br}, \mathrm{w}, \mathrm{bw}, \mathrm{ar}, \mathrm{aw}, \mathbf{s}_{r_i}, \ell_{r_i^3}) = \\
 & \ (1, N+M, 0,0,0,0,0,0,0,0) \wedge p_{ri}) \left[\bar{f}/\mathrm{X}_3\right] \\
= & \quad \%\ \ Def.\ \mathrm{I}_{r_i^3} \\
 & (\mathrm{I}_{r_i^3} \wedge p_{ri}) \left[\bar{f}/\mathrm{X}_3\right]
\end{array}
$$

(b) **Proof 8**

$\mathrm{T}_{r_i^3}$ *is of the form* $\mathbf{stut}_{r_i^3} \vee \bigvee_\tau(\epsilon = \mathbf{a}_\tau \wedge trans_\tau)$ *so* $\mathrm{T}_{r_i^3} \wedge ((p_{ri} \wedge p'_{ri}) \vee \mathbf{stut}_{r_i^3})$ *is equal to* $\mathbf{stut}_{r_i^3} \vee \bigvee_\tau(\epsilon = \mathbf{a}_\tau \wedge trans_\tau \wedge p_{ri} \wedge p'_{ri})$.

$$
\begin{array}{lll}
- & & \tau_{r_{i,1}^4} \\
 & = & \left(\epsilon = \mathbf{i} \wedge (\ell_{r_i^4}, \mathrm{m}) = (0,1) \wedge \Psi'_4 = \Psi_4 \left[0, 6/\mathrm{m}, \ell_{r_i^4}\right]\right) \\
 & \rightarrow & \left(\epsilon = \mathbf{i} \wedge (\ell_{r_i^3}, \mathrm{m}) = (0,1) \wedge p_{ri} \wedge p'_{ri} \wedge \Psi'_3 = \Psi_3 \left[0, 6/\mathrm{m}, \ell_{r_i^3}\right]\right) \left[\bar{f}/\mathrm{X}_3\right] \\
 & = & (\tau_{r_{i,1}^3} \wedge p_{ri} \wedge p'_{ri}) \left[\bar{f}/\mathrm{X}_3\right]
\end{array}
$$

The first P-operation of $reader_i^4$ *corresponds to the first P-operation of* $reader_i^3$.

– $$\begin{array}{ll} & \tau_{r^4_{i,2}} \\ = & \left(\epsilon = \mathbf{i} \wedge \ell_{r^4_i} = 6 \wedge \Psi'_4 = \Psi_4 \left[\mathrm{br}+1, 8/\mathrm{br}, \ell_{r^4_i}\right]\right) \\ \rightarrow & \left(\epsilon = \mathbf{i} \wedge \ell_{r^3_i} = 6 \wedge p_{ri}\right. \\ & \left. p'_{ri} \wedge \Psi'_3 = \Psi_3 \left[\mathrm{bm}-1, \mathrm{br}+1, 8/\mathrm{bm}, \mathrm{br}, \ell_{r^3_i}\right]\right) \left[\bar{f}/\mathrm{X}_3\right] \\ = & \left(\tau_{r^3_{i,2}} \wedge p_{ri} \wedge p'_{ri}\right) \left[\bar{f}/\mathrm{X}_3\right] \end{array}$$

The updating of br *in reader$_i^4$ corresponds to the updating of* br *and* bm *reader$_i^3$.*

– $$\begin{array}{ll} & \tau_{r^4_{i,3}} \\ = & \left(\epsilon = \mathbf{i} \wedge \ell_{r^4_i} = 8 \wedge CHO1(7)\right) \\ \rightarrow & \left(\epsilon = \mathbf{i} \wedge \ell_{r^3_i} = 8 \wedge p_{ri} \wedge p'_{ri} \wedge CHO(7)\right) \left[\bar{f}/\mathrm{X}_3\right] \\ = & \left(\tau_{r^3_{i,3}} \wedge p_{ri} \wedge p'_{ri}\right) \left[\bar{f}/\mathrm{X}_3\right] \end{array}$$

The first V-operation of reader$_i^4$ corresponds to the first V-operation of reader$_i^3$.

– $$\begin{array}{ll} & \tau_{r^4_{i,4}} \\ = & \left(\epsilon = \mathbf{i} \wedge (\ell_{r^4_i}, \mathrm{r}) = (7,1) \wedge \Psi'_4 = \Psi_4 \left[0, 1/\mathrm{r}, \ell_{r^4_i}\right]\right) \\ \rightarrow & \left(\epsilon = \mathbf{i} \wedge (\ell_{r^3_i}, \mathrm{r}) = (7,1) \wedge p_{ri} \wedge p'_{ri} \wedge \Psi'_3 = \Psi_3 \left[0, 1/\mathrm{r}, \ell_{r^3_i}\right]\right) \left[\bar{f}/\mathrm{X}_3\right] \\ = & \left(\tau_{r^3_{i,4}} \wedge p_{ri} \wedge p'_{ri}\right) \left[\bar{f}/\mathrm{X}_3\right] \end{array}$$

The second P-operation of reader$_i^4$ corresponds to the second P-operation of reader$_i^3$.

– $$\begin{array}{ll} & \tau_{r^4_{i,5}} \\ = & \left(\epsilon = \mathbf{i} \wedge \ell_{r^4_i} = 1 \wedge \Psi'_4 = \Psi_4 \left[\mathrm{br}-1, \mathrm{ar}+1, 2/\mathrm{br}, \mathrm{ar}, \ell_{r^4_i}\right]\right) \\ \rightarrow & \left(\epsilon = \mathbf{i} \wedge \ell_{r^3_i} = 1 \wedge p_{ri}\right. \\ & \left. \wedge\, p'_{ri} \wedge \Psi'_3 = \Psi_3 \left[\mathrm{br}-1, \mathrm{ar}+1, \mathrm{bm}+1, 2/\mathrm{br}, \mathrm{ar}, \mathrm{bm}, \ell_{r^3_i}\right]\right) \left[\bar{f}/\mathrm{X}_3\right] \\ = & \left(\tau_{r^3_{i,5}} \wedge p_{ri} \wedge p'_{ri}\right) \left[\bar{f}/\mathrm{X}_3\right] \end{array}$$

The ar *decrement step of reader$_i^4$ corresponds to the* ar *decrement step of reader$_i^3$.*

– $$\begin{array}{ll} & \tau_{r^4_{i,6}} \\ = & \left(\epsilon = \mathbf{i} \wedge \ell_{r^4_i} = 2 \wedge CHO2(3) \wedge \Psi'_4 = \Psi_4 \left[1/\mathbf{s}_{r_i}\right]\right) \\ \rightarrow & \left(\epsilon = \mathbf{i} \wedge \ell_{r^3_i} = 2 \wedge p_{ri} \wedge p'_{ri} \wedge CHO(3) \wedge \Psi'_3 = \Psi_3 \left[1/\mathbf{s}_{r_i}\right]\right) \left[\bar{f}/\mathrm{X}_3\right] \\ = & \left(\tau_{r^3_{i,6}} \wedge p_{ri} \wedge p'_{ri}\right) \left[\bar{f}/\mathrm{X}_3\right] \end{array}$$

If reader$_i^4$ becomes critical then reader$_i^3$ becomes critical.

– $$\begin{array}{ll} & \tau_{r^4_{i,7}} \\ = & \left(\epsilon = \mathbf{i} \wedge (\ell_{r^4_i}, \mathrm{m}) = (3,1) \wedge \Psi'_4 = \Psi_4 \left[0, 4/\mathrm{m}, \ell_{r^4_i}\right]\right) \\ \rightarrow & \left(\epsilon = \mathbf{i} \wedge (\ell_{r^3_i}, \mathrm{m}) = (3,1) \wedge p_{ri} \wedge p'_{ri} \wedge \Psi'_3 = \Psi_3 \left[0, 4/\mathrm{m}, \ell_{r^3_i}\right]\right) \left[\bar{f}/\mathrm{X}_3\right] \\ = & \left(\tau_{r^3_{i,7}} \wedge p_{ri} \wedge p'_{ri}\right) \left[\bar{f}/\mathrm{X}_3\right] \end{array}$$

The third P-operation of reader$_i^4$ corresponds to the third P-operation of reader$_i^3$.

–
$$
\begin{array}{rl}
& \tau_{r^4_{i,8}} \\
= & \left(\epsilon = \mathbf{i} \wedge \ell_{r^4_i} = 4 \wedge \Psi_4' = \Psi_4 \left[\mathrm{ar}-1, 5/\mathrm{ar}, \ell_{r^4_i}\right]\right) \\
\rightarrow & \left(\epsilon = \mathbf{i} \wedge \ell_{r^3_i} = 4 \wedge p_{ri} \wedge p_{ri}' \wedge \Psi_3' = \Psi_3 \left[\mathrm{ar}-1, 5/\mathrm{ar}, \ell_{r^3_i}\right]\right) \left[\bar{f}/\mathrm{X}_3\right] \\
= & \left(\tau_{r^3_{i,8}} \wedge p_{ri} \wedge p_{ri}'\right) \left[\bar{f}/\mathrm{X}_3\right]
\end{array}
$$

The ar *decrement step of reader$_i^4$ corresponds to the* ar *decrement step of reader$_i^3$.*

–
$$
\begin{array}{rl}
& \tau_{r^4_{i,9}} \\
= & \left(\epsilon = \mathbf{i} \wedge \ell_{r^4_i} = 5 \wedge CHO3(0) \wedge \Psi_4' = \Psi_4 \left[0/\mathbf{s}_{r_i}\right]\right) \\
\rightarrow & \left(\epsilon = \mathbf{i} \wedge \ell_{r^3_i} = 5 \wedge p_{ri} \wedge p_{ri}' \wedge CHO(0) \wedge \Psi_3' = \Psi_3 \left[0/\mathbf{s}_{r_i}\right]\right) \left[\bar{f}/\mathrm{X}_3\right] \\
= & \left(\tau_{r^3_{i,9}} \wedge p_{ri} \wedge p_{ri}'\right) \left[\bar{f}/\mathrm{X}_3\right]
\end{array}
$$

The third V-operation of reader$_i^4$ corresponds to the third V-operation of reader$_i^3$.

–
$$
\begin{array}{rl}
& \tau_{r^4_{i,10}} \\
= & \left(\epsilon = \mathbf{e} \wedge \mathrm{m} = 1 \wedge \Psi_4' = \Psi_4 \left[0/\mathrm{m}\right]\right) \\
\rightarrow & \left(\epsilon = \mathbf{e} \wedge \mathrm{m} = 1 \wedge p_{ri} \wedge p_{ri}' \wedge \Psi_3' = \Psi_3 \left[0/\mathrm{m}\right]\right) \left[\bar{f}/\mathrm{X}_3\right] \\
= & \left(\tau_{r^3_{i,10}} \wedge p_{ri} \wedge p_{ri}'\right) \left[\bar{f}/\mathrm{X}_3\right]
\end{array}
$$

If the environment of reader$_i^4$ executes a P-operation then the environment of reader$_i^3$ also executes a P-operation.

–
$$
\begin{array}{rl}
& \tau_{r^4_{i,11}} \\
= & \left(\epsilon = \mathbf{e} \wedge \mathrm{r} = 1 \wedge \Psi_4' = \Psi_4 \left[0/\mathrm{r}\right]\right) \\
\rightarrow & \left(\epsilon = \mathbf{e} \wedge \mathrm{r} = 1 \wedge p_{ri} \wedge p_{ri}' \wedge \Psi_3' = \Psi_3 \left[0/\mathrm{r}\right]\right) \left[\bar{f}/\mathrm{X}_3\right] \\
= & \left(\tau_{r^3_{i,11}} \wedge p_{ri} \wedge p_{ri}'\right) \left[\bar{f}/\mathrm{X}_3\right]
\end{array}
$$

If the environment of reader$_i^4$ executes a P-operation then the environment of reader$_i^3$ also executes a P-operation.

–
$$
\begin{array}{rl}
& \tau_{r^4_{i,12}} \\
= & \left(\epsilon = \mathbf{e} \wedge \mathrm{w} = 1 \wedge \Psi_4' = \Psi_4 \left[0/\mathrm{w}\right]\right) \\
\rightarrow & \left(\epsilon = \mathbf{e} \wedge \mathrm{w} = 1 \wedge p_{ri} \wedge p_{ri}' \wedge \Psi_3' = \Psi_3 \left[0/\mathrm{w}\right]\right) \left[\bar{f}/\mathrm{X}_3\right] \\
= & \left(\tau_{r^3_{i,12}} \wedge p_{ri} \wedge p_{ri}'\right) \left[\bar{f}/\mathrm{X}_3\right]
\end{array}
$$

If the environment of reader$_i^4$ executes a P-operation then the environment of reader$_i^3$ also executes a P-operation.

–
$$
\begin{array}{rl}
& \tau_{r^4_{i,13}} \\
= & \left(\epsilon = \mathbf{e} \wedge \ell_{r^4_i} \in \{0,7,3\} \wedge \mathrm{m} = 0 \wedge \Psi_4' = \Psi_4 \left[1/\mathrm{m}\right]\right) \\
\rightarrow & \left(\epsilon = \mathbf{e} \wedge \ell_{r^3_i} \in \{0,7,3\} \wedge \mathrm{m} = 0 \wedge p_{ri} \wedge p_{ri}' \wedge \Psi_3' = \Psi_3 \left[1/\mathrm{m}\right]\right) \left[\bar{f}/\mathrm{X}_3\right] \\
= & \left(\tau_{r^3_{i,13}} \wedge p_{ri} \wedge p_{ri}'\right) \left[\bar{f}/\mathrm{X}_3\right]
\end{array}
$$

If the environment of reader$_i^4$ executes a V-operation then the environment of reader$_i^3$ also executes a V-operation.

– $\tau_{r^4_{i,14}}$
$= \left(\epsilon = \mathbf{e} \wedge \ell_{r^4_i} \in \{0,7,3\} \wedge \mathrm{r} = 0 \wedge \Psi_4' = \Psi_4\,[1/\mathrm{r}]\right)$
$\to \left(\epsilon = \mathbf{e} \wedge \ell_{r^3_i} \in \{0,7,3\} \wedge \mathrm{r} = 0 \wedge p_{ri} \wedge p_{ri}' \wedge \Psi_3' = \Psi_3\,[1/\mathrm{r}]\right) \left[\bar{f}/\mathrm{X}_3\right]$
$= \left(\tau_{r^3_{i,14}} \wedge p_{ri} \wedge p_{ri}'\right) \left[\bar{f}/\mathrm{X}_3\right]$
If the environment of reader^4_i executes a V-operation then the environment of reader^3_i also executes a V-operation.

– $\tau_{r^4_{i,15}}$
$= \left(\epsilon = \mathbf{e} \wedge \ell_{r^4_i} \in \{0,7,3\} \wedge \mathrm{w} = 0 \wedge \Psi_4' = \Psi_4\,[1/\mathrm{w}]\right)$
$\to \left(\epsilon = \mathbf{e} \wedge \ell_{r^2_i} \in \{0,7,3\} \wedge \mathrm{w} = 0 \wedge p_{ri} \wedge p_{ri}' \wedge \Psi_3' = \Psi_3\,[1/\mathrm{w}]\right) \left[\bar{f}/\mathrm{X}_3\right]$
$= \left(\tau_{r^3_{i,15}} \wedge p_{ri} \wedge p_{ri}'\right) \left[\bar{f}/\mathrm{X}_3\right]$
If the environment of reader^4_i executes a V-operation then the environment of reader^3_i also executes a V-operation.

– $\mathbf{stut}_{r^4_i} \to \mathbf{stut}_{r^3_i} \left[\bar{f}/\mathrm{X}_3\right]$
since $\mathbf{s}_{r_i}$ *doesn't change.*

(c) Let $\mathrm{WF}_{r^4_i} \triangleq \{\tau_{r^4_{i,k}} \mid k \in \{2,5,8\}\}$ and
$\mathrm{SF}_{r^4_i} \triangleq \{\tau_{r^4_{i,k}} \mid k \in \{1,3,4,6,7,9,10,11,12,13,14,15\}\}$ then

$$\mathrm{L}_{r^4_i} \triangleq \bigwedge_{\tau \in \mathrm{WF}_{r^4_i}} (\Diamond\Box En(\tau) \to \Box\Diamond\tau) \wedge \bigwedge_{\tau \in \mathrm{SF}_{r^4_i}} (\Box\Diamond En(\tau) \to \Box\Diamond\tau)$$

Let $\mathrm{WF}_{r^3_i} \triangleq \{\tau_{r^3_{i,k}} \mid k \in \{2,5,8\}\}$ and
$\mathrm{SF}_{r^3_i} \triangleq \{\tau_{r^1_{i,k}} \mid k \in \{1,3,4,6,7,9,10,11,12,13,14,15\}\}$ then

$$\mathrm{L}_{r^3_i} \triangleq \bigwedge_{\tau \in \mathrm{WF}_{r^3_i}} (\Diamond\Box En(\tau) \to \Box\Diamond\tau) \wedge \bigwedge_{\tau \in \mathrm{SF}_{r^3_i}} (\Box\Diamond En(\tau) \to \Box\Diamond\tau)$$

The following holds:

$$\mathcal{S}_4 \models \mathrm{L}_{r^4_i} \to \mathrm{L}_{r^3_i} \left[\bar{f}/\mathrm{X}_3\right]$$

since $\tau_{r^3_{i,k}}$ is relatively refined by $\tau_{r^4_{i,k}}$ for $k = 0, \ldots, 15$.
So

$$\mathcal{S}_4 \models \mathrm{L}_{r^3_i} \left[\bar{f}/\mathrm{X}_3\right]$$

ad (2) Analogue to the proof of (1).

ad (3) This is trivial because $\mathrm{W}_3 \leftrightarrow (\bigwedge_{i=1}^{N} \mathrm{W}_{r^3_i} \wedge \bigwedge_{j=1}^{M} \mathrm{W}_{w^3_j})$.

Chapter 4

Stable Storage Example

This chapter first introduces in sect. 4.1 a *general methodology* for proving fault tolerant systems correct. This general methodology uses the relative refinement concept of sect. 2.3.2. The remaining sections of this chapter give an illustration of this general methodology by applying it to a fault tolerant system consisting of a number of disks implementing stable storage. Section 4.2 introduces this application. In sections 4.3, 4.4, 4.5 and 4.6 the four steps of this general methodology are applied to the stable storage example [Cri85, Sch91].

4.1 The General Methodology

The general methodology consists of four steps. In the first step one gives the abstract specification $\mathcal{S} \triangleq (B, \mathrm{H})$ where H is a DTL formula specifying the fault tolerant system. In this specification no faults are visible, hence they don't occur as observables. The designer's task is to give an implementation of this system under the assumption that only faults from certain classes can occur. These faults are called *anticipated faults*. These are faults which may affect the implementation in that they may give rise to errors in the state of the implementation, resulting subsequently in failures of that implementation. In step 2,3 and 4 of the methodology a fault-tolerant system is developed.

The second step *identifies* the anticipated faults which can affect an implementation $\mathcal{S}_P \triangleq (B_P, \mathrm{H}_P)$. This implementation serves as first approximation to the final implementation of $\mathcal{S}$. It should be clear that $\mathcal{S}_P$ is not a refinement of $\mathcal{S}$ because of the possible occurrences of anticipated faults. $\mathcal{S}_P$ is only a refinement when these faults do not occur, i.e., $\mathcal{S}_P$ is a *relative refinement* of $\mathcal{S}$. So in step 2 we must prove:

(1) $\mathcal{S}_P \;{}_{W_P}\mathbf{ref}\; \mathcal{S}$

In the third step one specifies *how these anticipated faults are detected*, i.e., one has to specify a detection layer $\mathcal{S}_{Ds}$ for these faults. This layer is added in bottom-up fashion to the implementation $\mathcal{S}_P$ of the second step and stops upon detection of the first error, i.e., $\mathcal{S}_{Ds}$ is a *fail-stop* implementation. So the second approximation to the final implementation consists of the composition of $\mathcal{S}_P$ and $\mathcal{S}_{Ds}$. This approximation is clearly not a refinement because when in $\mathcal{S}_P$ a fault occurs, and $\mathcal{S}_{Ds}$ detects the corresponding error, the whole approximation stops. One would like to have (eventually) an approximation that doesn't stop, i.e., the physical disk isn't affected by faults and the detection layer should detect no error. Let $\overline{W} \triangleq (W_{Ds}, W_P)$ where W_P expresses that no faults occur and W_{Ds} expresses that no error is detected. Then we must prove the following:

$$(2) \quad \mathcal{S}_{Ds} \; |\overline{w}| \; \mathcal{S}_P \; \textbf{ref}\ ^{W_P} \mathcal{S}_P.$$

From (1), (2) and the transitivity of relative refinement relation follows:

$$\mathcal{S}_{Ds} \; |\overline{w}| \; \mathcal{S}_P \; \textbf{ref} \; \mathcal{S}.$$

In the fourth step one *specifies the corrective action to be undertaken after detection of an error.* This means in general that one needs *redundancy*, i.e., several copies of $\mathcal{S}_P$ and $\mathcal{S}_D$ components, because when a detection layer $\mathcal{S}_D$ detects an error, the state before that error has to be recovered and that can only be done by accessing another copy of $\mathcal{S}_P$ through its corresponding detection layer $\mathcal{S}_D$. Note that the $\mathcal{S}_D$ component doesn't stop anymore on the detection of an error but merely waits for the corrective action to be undertaken. Say, we need N copies of $\mathcal{S}_P$ and $\mathcal{S}_D$. The final implementation consists then of those N copies of $\mathcal{S}_P$ and $\mathcal{S}_D$ plus a recovery layer $\mathcal{S}_R$. Let W_R express which kind of errors can be recovered. If the following holds:

$$(3) \quad \|_{i=1}^{N} (\mathcal{S}_{P_i} \parallel \mathcal{S}_{D_i}) \parallel \mathcal{S}_R \;{}_{W_R}\textbf{ref} \; \mathcal{S}_{Ds} \; |\overline{w}| \; \mathcal{S}_P$$

then from (1), (2), (3) and the transitivity of relative refinement follows the desired result, i.e.:

$$\|_{i=1}^{N} (\mathcal{S}_{P_i} \parallel \mathcal{S}_{D_i}) \parallel \mathcal{S}_R \;{}_{W_R}\textbf{ref} \; \mathcal{S}$$

This ends our exposition of the general methodology. In the next sections this methodology will be applied to a stable storage example.

4.2 Application: Introduction

Stable storage is defined as follows. A disk is used to store and retrieve data. During these operations some faults can occur in the underlying hardware. To make the disk more reliable one introduces layers for the detection and correction of errors, due to these faults. The system with these detection and correction layers is called "stable storage". This stable storage is a fault tolerant system because it stores and retrieves data in a reliable way under the assumption that faults from a certain class are recovered (corrected). This class consists of two kinds of faults. The first one consists of faults that damage the disk surface -the contents of the disk are said to be corrupted by these faults. The second one consists of faults that affect the disk control system, and results into the contents of the disk being read from or written to the wrong location. Notice that other kinds of faults, such as power failure or physical destruction of the whole stable storage system, are not taken into account. I.e., stable storage should function correctly provided such latter faults do not occur.

4.3 First Step: Stable Storage

4.3.1 Introduction

In this section we give a specification of a stable storage system as we ideally would like to have it. So no faults are observed. If they occur internally, they should be repaired by the system without leaving any observable trace. For that is the meaning of 'stable' here!

4.3.2 Specification

The abstract specification of the stable storage specifies the following: The user signals with a read request event that he wants to read the contents of some location of stable storage. Stable storage will then respond by sending the requested contents. The user signals with a write request event that some data has to be written on some location of stable storage, with a response event the stable storage signals that the write has been performed. Note: we have a very simple stable storage that can handle only one request at a time. The formal specification $\mathcal{S} = (B, \mathrm{H})$ where $\mathrm{H} \triangleq \mathrm{I} \wedge \Box\mathrm{T} \wedge \mathrm{L}$ and B, I, T and L are as follows:

1. **Basis** $B = ((\mathrm{In}, \mathrm{Out}), (\mathrm{V}, \mathrm{X}))$

$$\begin{array}{lcl} \mathrm{In} & \triangleq & \{\mathbf{Rreq}, \mathbf{Wreq}\}, \\ \mathrm{Out} & \triangleq & \{\mathbf{Rres}, \mathbf{Wres}\}, \\ \mathrm{V} & \triangleq & \emptyset, \\ \mathrm{X} & \triangleq & \{\ell, \mathrm{r}, \mathrm{s}, \mathrm{M}[n] \mid n \in SN\} \end{array}$$

where SN is the set of sector numbers: $[1, .., Z]$. Let Inf be the set of information items that could be stored and retrieved by stable storage but that will not be further specified. For $n \in SN$ and $c, d \in Inf$:

- $\mathbf{Rreq}?(n)$: the request to read sector n.
- $\mathbf{Rres}!(c)$: the response to the previous read request where c are the contents of requested sector.
- $\mathbf{Wreq}?(d)$: write information item d onto sector n.
- $\mathbf{Wres}!$: previous write has been performed.
- ℓ: local variable indicating the status of the stable storage; $\ell = 0$ means no requests are issued, $\ell = 1$ means a read request has been issued, and $\ell = 2$ means a write request has been issued.
- r: local variable indicating the requested sector.
- s: local variable indicating the contents of the requested sector or the to be written data.
- $\mathrm{M}[n]$: the physical sector n.

Let $\Psi_0 \triangleq (\ell, \mathrm{r}, \mathrm{s}, \mathrm{M}[1], \ldots, \mathrm{M}[Z])$ and $\Psi_0' \triangleq (\ell', \mathrm{r}', \mathrm{s}', \mathrm{M}'[1], \ldots, \mathrm{M}'[Z])$.

2. **Initial States:**

$$\mathrm{I} \triangleq \ell = 0 \wedge \bigwedge_{i \in SN} \mathrm{M}[i] = dflt$$

Where $dflt \in Inf$ is some default information item.

3. **Transitions:**
T $\triangleq$

τ_1 $\big(\epsilon = \mathbf{Rreq}?(n) \wedge \ell = 0 \wedge \Psi_0' = \Psi_0\,[1, n/\ell, \mathrm{r}]\big)$
The user requests the contents of sector n.

τ_2 $\vee\ \big(\epsilon = \mathbf{Rres}(\mathrm{M}[\mathrm{r}]) \wedge \ell = 1 \wedge \Psi_0' = \Psi_0\,[0/\ell]\big)$
Stable storage responds with the contents of the requested sector.

τ_3 $\vee\ \big(\epsilon = \mathbf{Wreq}?(n, d) \wedge \ell = 0 \wedge \Psi_0' = \Psi_0\,[2, n, d/\ell, \mathrm{r}, \mathrm{s}]\big)$
The user requests that d should be written onto sector n.

τ_4 $\vee\ \big(\epsilon = \mathbf{Wres}! \wedge \ell = 2 \wedge \Psi_0' = \Psi_0\,[0, \mathrm{s}/\ell, \mathrm{M}[\mathrm{r}]]\big)$
Stable storage responds with a signal that requested write is performed.

τ_0 $\vee$ **stut**

These transitions are illustrated in figure 4.1

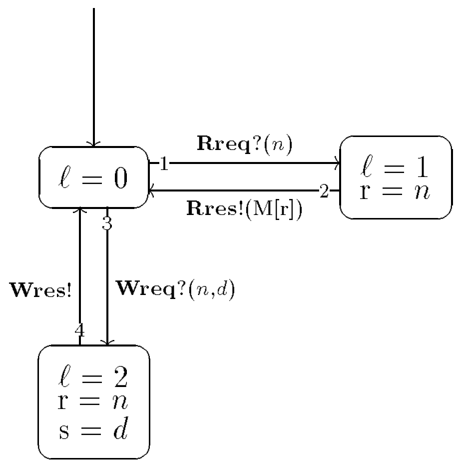

Figure 4.1: Transitions of stable storage.

4. **Liveness condition:**
The liveness condition expresses that the communication transitions are strongly fair. Let SF $= \{\tau_i \mid i \in \{1, 2, 3, 4\}\}$ then

$$\mathrm{L} \triangleq \bigwedge_{\tau \in \mathrm{SF}} (\Box\Diamond En(\tau) \rightarrow \Box\Diamond\tau)$$

4.4 Second Step: Physical Disk

4.4.1 Introduction

In this step, which is the first stage in our task to develop a fault tolerant system, we give the specification of a physical disk. This specification is a first approximation to our fault tolerant system, i.e., it acts as bottom layer of our desired implementation and because the other layers haven't been developed yet it is the only layer we have at this moment. In this specification we must specify, because this is the first stage of our development, which are the anticipated faults our system, i.e., we have to specify which are the faults of our interest that could affect a physical disk. These faults are represented as events in our formalism. This first approximation of stable storage is not a correct one because of these anticipated faults (the physical disk doesn't anticipate on these faults at all!). But under the assumption that these faults don't occur this first implementation is a refinement of stable storage.

4.4.2 Specification

We must specify a physical disk, the anticipated faults and their impact on the physical disk. We take as anticipated faults the following ones (cf. [Cri85, Sch91]):

- Damages of the disk surface causing corruption of the contents of a physical sector.
- Disk control faults causing the contents of a particular physical sector to be read or written at a wrong location.

These two faults are described using two events: the *dam* event standing for a damage to the disk surface and the *csf* event standing for a disk control system fault. As in the specification of stable storage, the user requests with $\mathbf{Rreq}(n)$ that it wants to read the contents of physical sector n. The physical disk then responds with $\mathbf{Rres}(c)$ delivering the requested contents. With $\mathbf{Wreq}(n,d)$ the user signals that d should be written onto sector n. The physical disk responds with **Wres** that the requested information has been written. The formal specification $\mathcal{S}_P = (B_P, \mathrm{H}_P)$ where $\mathrm{H}_P \triangleq \mathrm{I}_P \wedge \Box\mathrm{T}_P \wedge \mathrm{L}_P$ and B_P, I_P, T_P and L_P are as follows:

1. **Basis** $B_P = ((\mathrm{In}_P, \mathrm{Out}_P), (\mathrm{V}_P, \mathrm{X}_P))$

$$\begin{array}{lcl} \mathrm{In}_P & \triangleq & \{\mathbf{Rreq}, \mathbf{Wreq}\}, \\ \mathrm{Out}_P & \triangleq & \{\mathbf{Rres}, \mathbf{Wres}\}, \\ \mathrm{V}_P & \triangleq & \emptyset, \\ \mathrm{X}_P & \triangleq & \{\ell_P, \mathrm{r}_P, \mathrm{s}_P, \mathrm{M}_P[n], \mathrm{F}[n] \mid n \in PN\} \end{array}$$

where PN is the set of physical sector numbers: $[1,..,Y]$. Let Phy be the set of information items that could be stored and retrieved by the physical disk but that will not be further specified. The special information item ⓒ is introduced to model disk surface damage faults. For $n \in PN$ and $c, d \in Phy$:

- **Rreq**?(n): the request to read sector n.
- **Rres**!(c): the response to the previous request where c are the contents of requested sector.
- **Wreq**?(d): write information item d onto sector n.
- **Wres**!: response that previous write has been performed.
- ℓ_P: local variable indicating the status of the physical disk.
- r_P: local variable indicating the requested physical sector.
- s_P: local variable indicating the requested contents or the data to be written.
- $\mathrm{M}_P[n]$: the physical sector n.
- F: the control system, i.e., the control system maps sector n to sector $\mathrm{F}[n]$.

Let $\Psi_1 \triangleq (\ell_P, \mathrm{r}_P, \mathrm{s}_P, \mathrm{M}_P[1], \ldots, \mathrm{M}_P[Y], \mathrm{F}[1], \ldots, \mathrm{F}[Y])$ and
$\Psi'_1 \triangleq (\ell'_P, \mathrm{r}'_P, \mathrm{s}'_P, \mathrm{M}'_P[1], \ldots, \mathrm{M}'_P[Y], \mathrm{F}'[1], \ldots, \mathrm{F}'[Y])$.

2. **Initial States:**

$$\mathrm{I}_P \triangleq \ell_P = 0 \wedge \bigwedge_{i \in PN} (\mathrm{M}_P[i] = dflt \wedge \mathrm{F}[i] = i)$$

All sectors contain the default data item *dflt* and the control system has not been affected by control system faults.

3. **Transitions:**
$\mathrm{T}_P \triangleq$

$\tau_{P,1}$ $\quad \Big(\epsilon = \mathbf{Rreq}?(n) \wedge \ell_P = 0 \wedge \Psi'_1 = \Psi_1\,[1, n/\ell_P, \mathrm{r}_P]\Big)$
The user requests the contents of sector n.

$\tau_{P,2}$ $\quad \vee\ \Big(\epsilon = \mathbf{Rres}!(\mathrm{M}_P[\mathrm{F}[\mathrm{r}_P]]) \wedge \ell_P = 1 \wedge \Psi'_1 = \Psi_1\,[0/\ell_P]\Big)$
The physical disk responds with the contents of the requested sector.

$\tau_{P,3}$ $\quad \vee\ \Big(\epsilon = \mathbf{Wreq}?(n, d) \wedge \ell_P = 0 \wedge \Psi'_1 = \Psi_1\,[2, n, d/\ell_P, \mathrm{r}_P, \mathrm{s}_P]\Big)$
The user requests that d should be written onto sector n.

$\tau_{P,4}$ $\quad \vee\ \Big(\epsilon = \mathbf{Wres}! \wedge \ell_P = 2 \wedge \Psi'_1 = \Psi_1\,[0, \mathrm{s}_P/\ell_P, \mathrm{M}_P[\mathrm{F}[\mathrm{r}_P]]]\Big)$
The physical disk responds with a signal that requested write is performed.

$\tau_{P,5}$ $\quad \vee\ \Big(\epsilon = \mathbf{i} \wedge n \neq j \wedge \Psi'_1 = \Psi_1\,[j/\mathrm{F}[n]]\Big)$
Due to control system fault the sector n is mapped to sector j.

$\tau_{P,6}$ $\quad \vee\ \Big(\epsilon = \mathbf{i} \wedge \Psi'_1 = \Psi_1\,[©/\mathrm{M}_P[n]]\Big)$
Due to disk surface fault the contents of sector n are replaced by corrupted data ©.

$\tau_{P,0}$ $\quad \vee\ \mathbf{stut}_P$

These transitions are illustrated in figure 4.2 where *fault* is either a control system fault or a disk surface fault.

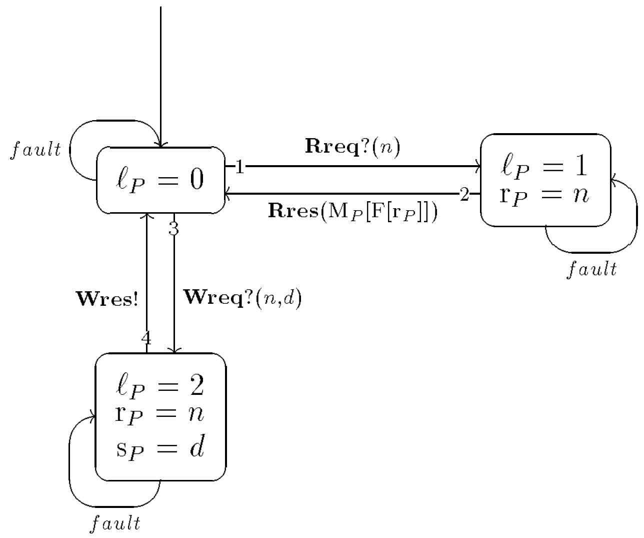

Figure 4.2: Transitions of the physical disk.

4. **Liveness condition:**
   The liveness condition expresses that the communication transitions are strongly fair. Let $\mathrm{SF}_P = \{\tau_{P,i} \mid i \in \{1,2,3,4\}\}$ then

$$\mathrm{L}_P \triangleq \bigwedge_{\tau \in \mathrm{SF}_P} (\Box\Diamond En(\tau) \to \Box\Diamond\tau)$$

4.4.3 Requirement W_P

The requirement W_P expresses that the control system and disk surface faults never occur.

$$\mathrm{W}_P \triangleq \Box(\bigwedge_{i \in PN} (\mathrm{M}_P[i] \neq \copyright \wedge \mathrm{F}[i] = i)$$

This corresponds to the following machine: Let

$$\begin{array}{lcl} p & \triangleq & \bigwedge_{i\in PN}(\mathrm{M}_P[i] \neq \copyright \wedge \mathrm{F}[i] = i) \\ p' & \triangleq & \bigwedge_{i\in PN}(\mathrm{M}'_P[i] \neq \copyright \wedge \mathrm{F}'[i] = i) \end{array}$$

then W_P is equal to the machine $p \wedge \Box((p \wedge p') \vee stut_P)$.

4.4.4 $\mathcal{S}_P$ relatively refines $\mathcal{S}$

We should prove $\mathcal{S}_P$ relatively refines $\mathcal{S}$. Let the external requirement for the system $\mathcal{S}$ be **true** (i.e., no extra requirement is imposed). According to theorem 8 $\mathcal{S}_P$ relatively refines $\mathcal{S}$ with respect to $(\mathrm{W}_P, \mathrm{W})$ iff the following holds:

$\mathfrak{O}(B_P) = \mathfrak{O}(B)$ and
$\models (\exists \mathrm{X}_P \,.\, (\mathrm{G}_P)) \to (\exists \mathrm{X} \,.\, (\mathrm{G}))$

where X_P are the local variables from $\mathcal{S}_P$, i.e., $\mathrm{X}_P \triangleq \{\ell_P, \mathrm{r}_P, \mathrm{s}_P, \mathrm{M}_P[n], \mathrm{F}[n] \mid n \in PN\}$ and G_P is defined as

$$\mathrm{I}_P \wedge \Box\mathrm{T}_P \wedge \mathrm{L}_P \wedge \mathrm{W}_P$$

X are the local variables from $\mathcal{S}$, i.e., $\mathrm{X} \triangleq \{\ell, \mathrm{r}, \mathrm{s}, \mathrm{M}[n] \mid n \in SN\}$ and G is defined as

$$\mathrm{I} \wedge \Box\mathrm{T} \wedge \mathrm{L}$$

Rule 3 will be used to prove

$$\models (\exists \mathrm{X}_P \,.\, (\mathrm{G}_P)) \rightarrow (\exists \mathrm{X} \,.\, (\mathrm{G}))\,.$$

This means one has to prove (a), (b) and (c) below, for $\bar{f}$ the refinement mapping from $\mathcal{S}_P$ to $\mathcal{S}$, defined as: $\bar{f} = f_\ell, f_\mathrm{r}, f_\mathrm{s}, f_{\mathrm{M}[n]}$ $(n \in SN)$. We will assume that the set of sector numbers SN is equal to the set of physical sector numbers PN. The refinement mappings are defined as:

$$\begin{array}{lcl} f_\ell & \triangleq & \ell_P \\ f_\mathrm{r} & \triangleq & \mathrm{r}_P \\ f_\mathrm{s} & \triangleq & \mathrm{s}_P \\ f_{\mathrm{M}[n]} & \triangleq & \mathrm{M}_P[n] \end{array}$$

$$\begin{array}{ll} (a) & \mathcal{S}_P \cap Hist(\mathrm{W}_P) \models (\mathrm{I}_P \wedge p) \rightarrow \mathrm{I}\left[\bar{f}/\mathrm{X}\right] \\ (b) & \mathcal{S}_P \cap Hist(\mathrm{W}_P) \models \mathrm{T}_P \wedge ((p \wedge p') \vee \mathbf{stut}_P) \rightarrow \mathrm{T}\left[\bar{f}/\mathrm{X}\right] \\ (c) & \mathcal{S}_P \cap Hist(\mathrm{W}_P) \models \mathrm{L}\left[\bar{f}/\mathrm{X}\right] \end{array}$$

(a) **Proof 9**

$$\begin{array}{cl} & \mathrm{I}_P \wedge p \\ = & \quad \%\ \ Def.\ \mathrm{I}_P, p \\ & \ell_P = 0 \wedge \bigwedge_{i \in PN}(\mathrm{M}_P[i] = dflt \wedge \mathrm{F}[i] = i) \\ & \wedge \bigwedge_{i \in PN}(\mathrm{M}_P[i] \neq © \wedge \mathrm{F}[i] = i \\ \rightarrow & \quad \%\ \ Def.\ barf \\ & (\ell = 0 \wedge \bigwedge_{i \in SN} \mathrm{M}[i] = dflt)\left[\bar{f}/\mathrm{X}\right] \\ = & \quad \%\ \ Def.\ \mathrm{I} \\ & \mathrm{I}\left[\bar{f}/\mathrm{X}\right] \end{array}$$

(b) **Proof 10**

Since T_P *is of the form* $\mathbf{stut}_P \vee \bigvee_\tau(\epsilon = \mathbf{a}_\tau \wedge trans_\tau)$ *then* $\mathrm{T}_P \wedge ((p \wedge p') \vee \mathbf{stut}_P)$ *is equal to* $\mathbf{stut}_P \vee \bigvee_\tau(\epsilon = \mathbf{a}_\tau \wedge trans_\tau \wedge p \wedge p')$.

– $$\begin{array}{cl} & \tau_{P,1} \wedge p \wedge p' \\ = & \left(\epsilon = \mathbf{Rreq}?(n) \wedge \ell_P = 0 \wedge p \wedge p' \wedge \Psi_1' = \Psi_1\left[1, n/\ell_P, \mathrm{r}_P\right]\right) \\ \rightarrow & \left(\epsilon = \mathbf{Rreq}?(n) \wedge \ell = 0 \wedge \Psi_0' = \Psi_0\left[1, n/\ell, \mathrm{r}\right]\right)\left[\bar{f}/\mathrm{X}\right] \\ = & \tau_1\left[\bar{f}/\mathrm{X}\right] \end{array}$$

The read request at the physical disk level corresponds to the read request at the abstract level.

– $$\begin{array}{rl} & \tau_{P,2} \wedge p \wedge p' \\ = & \left(\epsilon = \mathbf{Rres}!(\mathrm{M}_P[\mathrm{F}[\mathrm{r}_P]]) \wedge \ell_P = 1 \wedge p \wedge p' \wedge \Psi_1' = \Psi_1\,[0/\ell_P]\right) \\ \to & \left(\epsilon = \mathbf{Rres}(\mathrm{M}[\mathrm{r}]) \wedge \ell = 1 \wedge \Psi_0' = \Psi_0\,[0/\ell]\right)\left[\bar{f}/\mathrm{X}\right] \\ = & \tau_2\left[\bar{f}/\mathrm{X}\right] \end{array}$$

The read response at the physical disk level corresponds to the read response at the abstract level.

– $$\begin{array}{rl} & \tau_{P,3} \wedge p \wedge p' \\ = & \left(\epsilon = \mathbf{Wreq}?(n,d) \wedge \ell_P = 0 \wedge p \wedge p' \wedge \Psi_0' = \Psi_0\,[2,n,d/\ell_P,\mathrm{r}_P,\mathrm{s}_P]\right) \\ \to & \left(\epsilon = \mathbf{Wreq}?(n,d) \wedge \ell = 0 \wedge \Psi_0' = \Psi_0\,[2,n,d/\ell,\mathrm{r},\mathrm{s}]\right)\left[\bar{f}/\mathrm{X}\right] \\ = & \tau_3\left[\bar{f}/\mathrm{X}\right] \end{array}$$

The write request at the physical disk level corresponds to the write request at the abstract level.

– $$\begin{array}{rl} & \tau_{P,4} \wedge p \wedge p' \\ = & \left(\epsilon = \mathbf{Wres}! \wedge \ell_P = 2 \wedge p \wedge p' \wedge \Psi_0' = \Psi_0\,[0,\mathrm{s}_P/\ell_P,\mathrm{M}_P[\mathrm{F}[\mathrm{r}_P]]]\right) \\ \to & \left(\epsilon = \mathbf{Wres}! \wedge \ell = 2 \wedge \Psi_0' = \Psi_0\,[0,\mathrm{s}/\ell,\mathrm{M}[\mathrm{r}]]\right)\left[\bar{f}/\mathrm{X}\right] \\ = & \tau_4\left[\bar{f}/\mathrm{X}\right] \end{array}$$

The write response at the physical disk level corresponds to the write response at the abstract level.

– $$\begin{array}{rl} & \tau_{P,5} \wedge p \wedge p' \\ = & \left(\epsilon = \mathbf{i} \wedge n \neq j \wedge p \wedge p' \wedge \Psi_1' = \Psi_1\,[j/\mathrm{F}[n]]\right) \\ = & \mathbf{false} \\ \to & \mathrm{T}\left[\bar{f}/\mathrm{X}\right] \end{array}$$

Due to the external requirement the disk control fault transition can not be taken, i.e., is equal to **false** *and from* **false** *everything can be inferred.*

– $$\begin{array}{rl} & \tau_{P,6} \wedge p \wedge p' \\ = & \left(\epsilon = \mathbf{i} \wedge p \wedge p' \wedge \Psi_1' = \Psi_1\,[©/\mathrm{M}_P[n]]\right) \\ = & \mathbf{false} \\ \to & \mathrm{T}\left[\bar{f}/\mathrm{X}\right] \end{array}$$

Due to the external requirement the disk surface fault transition can not be taken, i.e., is equal to **false** *and from* **false** *everything can be inferred.*

– $\mathbf{stut}_P \to \mathbf{stut}\left[\bar{f}/\mathrm{X}\right]$

(c) Let $\mathrm{SF}_P = \{\tau_{P,i} \mid i \in \{1,2,3,4\}\}$ then

$$\mathrm{L}_P \triangleq \bigwedge_{\tau \in \mathrm{SF}_P} (\Box\Diamond En(\tau) \to \Box\Diamond\tau)$$

. Let $\mathrm{SF} = \{\tau_i \mid i \in \{1,2,3,4\}\}$ then

$$\mathrm{L} \triangleq \bigwedge_{\tau \in \mathrm{SF}} (\Box\Diamond En(\tau) \to \Box\Diamond\tau).$$

Then the following holds

$$\mathcal{S}_P \cap Hist(\mathrm{W}_P) \models \mathrm{L}_P \rightarrow \mathrm{L}\left[\bar{f}/\mathrm{X}\right]$$

since τ_i is relatively refined by $\tau_{P,i}$ for $i = 1, \ldots, 4$. So

$$\mathcal{S}_P \cap Hist(\mathrm{W}_P) \models \mathrm{L}\left[\bar{f}/\mathrm{X}\right]$$

holds.

4.5 Third Step: Fail-Stop Detection Layer

4.5.1 Introduction

In this step, the second stage in our development of the fault tolerant system, we specify in bottom-up fashion on top of the physical disk that has been specified in Section 4.4, the layer that detects the faults that we assumed could affect the physical disk (the anticipated faults). The detection layer acts as a sort of "interface" between the user and the physical disk. It stops when an anticipated fault is detected by the detection mechanism, i.e., the whole system (detection layer plus physical disk) stops when such a fault occurs. It also informs the user which kind of anticipated fault has occurred. This second implementation is "better" than the first one because now the user is certain, under the assumption that the detection mechanism detects all the anticipated faults, that the retrieved data is reliable. The implementation of the detection layer is such that as soon as a fault is detected the system stops. This is called a *fail-stop implementation* [LA90]. As seen above, there are two classes of anticipated faults. Consequently there are two kinds of detection mechanisms. The first one checks whether the contents read from the physical disk are corrupted, i.e., detects errors due to damage of the disk surface. This is done with a cyclic redundancy mechanism [LA90]. The second one checks whether the contents of read from the physical disk originate from the right location. This is done with an address checking mechanism [LA90] which encodes the location of the contents of the physical disk in the contents itself.

4.5.2 Specification

The detection layer consists of three parts: the first part checks whether the data retrieved from the physical disk is affected by a corrupt data fault (the fault that damages the disk surface). This is done with a cyclic redundancy check (CRC) mechanism [LA90]. The second part checks whether the data retrieved from the physical disk is from the correct physical location, i.e., whether it is affected by a disk control system fault. This is done with an address checking (ADR) mechanism [LA90]. The third part prevents further access by the user of the physical disk when one of these two mechanisms detects a fault. This can be easily done because the detection layer acts as "interface" between the user and the physical disk, the detection layer then refuse to communicate with the user and the physical disk. Furthermore this part then gives a message to inform the user which anticipated fault has occurred.

The protocol of this interface between user and physical disk is as follows. The user read requests the contents of some physical sector by issuing a **Rreq**(n) event to the detection disk layer. This detection disk layer issues after receipt of this event a **Rreqp**(m) event to the physical disk. The physical disk then responds with a **Rresp**(c) event delivering the requested contents of that physical sector. The detection layer then responds after checking the contents with a **Rresp**(cd) event delivering either the requested contents or an error message. The user write requests that d should be written on sector n by issuing a **Wreq**(n, d) event to the detection layer. The detection layer then issues a **Wreqp**(m, dd) event to the physical disk requesting that dd is written on sector m. The physical disk then responds with a **Wresp** event that the requested information is written. The detection layer then responds to the user with a **Wres** event that the information is written.

Logical sector numbers are introduced now, but are used in the next step to correct disk surface damage faults, i.e. when the detection layer detects that data from a physical sector number is affected by a disk surface damage fault, the correct data will be written to another physical sector number. In order to retrieve these contents from this new location *logical* sector numbers are introduced. When contents are stored at a new physical sector the logical sector number will be pointing to this new sector. So actually the data are retrieved from their logical sector number. In this step however, the mapping between the logical sector numbers and the physical sector numbers will be the identity mapping because they are not needed here. The detection layer is described more formally by the following specification: $\mathcal{S}_{Ds} = (B_{Ds}, \mathrm{H}_{Ds})$ where $\mathrm{H}_{Ds} \triangleq \mathrm{I}_{Ds} \wedge \Box\mathrm{T}_{Ds} \wedge \mathrm{L}_{Ds}$ and B_{Ds}, I_{Ds}, T_{Ds} and L_{Ds} are as follows:

1. **Basis** $B_{Ds} = ((\mathrm{In}_{Ds}, \mathrm{Out}_{Ds}), (\mathrm{V}_{Ds}, \mathrm{X}_{Ds}))$

$$\begin{array}{lcl}
\mathrm{In}_{Ds} & \triangleq & \{\mathbf{Rreq}, \mathbf{Wreq}, \mathbf{Rresp}, \mathbf{Wresp}\} \\
\mathrm{Out}_{Ds} & \triangleq & \{\mathbf{Rres}, \mathbf{Wres}, \mathbf{Rreqp}, \mathbf{Wreqp}\}, \\
\mathrm{V}_{Ds} & \triangleq & \emptyset, \\
\mathrm{X}_{Ds} & \triangleq & \{\ell_{Ds}, \mathrm{r}_{Ds}, \mathrm{s}_{Ds}, \mathrm{LS}_{Ds}[i] \mid i \in LN\}
\end{array}$$

where LN is the set of logical sector numbers: $([1, .., Y])$. Let Lg the set of data items that the user wants to store on or to retrieve from the physical disk and Phy the set information items that can be stored on or retrieved from the physical disk (Note: an item from Phy is an crc-encoded and address-encoded item of Lg.) For $n \in LN$, $c, d \in Lg$, $m \in PN$ and $cd, dd \in Phy$:

- **Rreq**?(n): the request from the user to read logical sector n.
- **Rres**!(c): the response of the detection layer to the previous request where c are the crc-decoded and address-decoded contents of the requested logical sector n.
- **Wreq**?(n, d): write information item d onto logical sector n.
- **Wres**!: response that previous write has been performed.
- **Rreqp**!(m): the request from the detection layer to read physical sector m.
- **Rresp**?(cd): the response of the physical disk to the previous request where c are the crc-encoded and address-encoded contents of requested physical.

- **Wreqp**!(m, dd): write information item dd onto physical sector m.
- **Wresp**?: response that previous write has been performed.
- ℓ_{Ds}: local variable indicating the status of the detection layer; $\ell_{Ds} = 0$: the detection layer is waiting for a request, $\ell_{Ds} = 1$: the user has issued a read request, $\ell_{Ds} = 2$: the detection layer has issued a read request, $\ell_{Ds} = 3$: the physical has responded to a read request with correct data, $\ell_{Ds} = 4$: the physical disk has responded to a read request with incorrect data, $\ell_{Ds} = 5$: the detection layer has responded to a read request with an error message (stop status), $\ell_{Ds} = 6$: the user has issued a write request, $\ell_{Ds} = 7$: the detection layer has issued a write request, $\ell_{Ds} = 8$: the physical disk has responded to a write request.
- r_{Ds}: local variable indicating the requested sector.
- s_{Ds}: local variable indicating the requested information or the data to be written.
- $\mathrm{LS}_{Ds}[i]$: the physical sector mapped to logical sector. i.

Let $\Psi_2 \triangleq (\ell_{Ds}, \mathrm{r}_{Ds}, \mathrm{s}_{Ds}, \mathrm{LS}_{Ds}[1], \ldots, \mathrm{LS}_{Ds}[Y])$ and
$\Psi_2' \triangleq (\ell'_{Ds}, \mathrm{r}'_{Ds}, \mathrm{s}'_{Ds}, \mathrm{LS}'_{Ds}[1], \ldots, \mathrm{LS}'_{Ds}[Y])$.

2. **Initial states:**

$$\mathrm{I}_{Ds} \triangleq \ell_{Ds} = 0 \wedge \bigwedge_{i \in LN} \mathrm{LS}_{Ds}[i] = i$$

3. **Transitions:**
To describe the two detecting mechanisms as transitions the following functions are needed: (see [LA90] for more information about this CRC-coding)

- $CC : Phy \rightarrow Bool$
(Crc-Check) Is used to check whether data from the physical disk is damaged by a disk surface fault.
- $CD : Phy \rightarrow (Lg \times PN)$
(Crc-Decode) Is used to decode the CRC-coded physical data into address format.
- $CE : (Lg \times PN) \rightarrow Phy$
(Crc-Encode) Is used to encode data in address format into physical CRC format.
- $AC : (Lg \times PN \times PN) \rightarrow Bool$
(Adr-Check) Is used to check whether data is read from the correct physical location.
- $AD : (Lg \times PN) \rightarrow Lg$
(Adr-Decode) Is used to decode data in address format into user format.

- $AE : (LN \times Lg) \rightarrow (Lg \times PN)$
  (Adr-Encode) Is used to encode a physical sector number and a information item given by the user into address format.

Let

$$
\begin{array}{lll}
Good & \triangleq & CC(cd) \wedge AC(CD(cd), \mathrm{LS}_{Ds}[\mathrm{r}_{Ds}]) \\
 & & \text{data has not been affected by faults} \\
A.er & \triangleq & CC(cd) \wedge \neg AC(CD(cd), \mathrm{LS}_{Ds}[\mathrm{r}_{Ds}]) \\
 & & \text{data has been affected by a control system fault} \\
C.er & \triangleq & \neg CC(cd) \\
 & & \text{data has been affected by a disk surface damage} \\
c & \triangleq & AD(CD(cd)) \\
 & & \text{the address- and crc-decoded contents} \\
m & \triangleq & \mathrm{LS}_{Ds}[\mathrm{r}_{Ds}] \\
 & & \text{physical sector} \\
dd & \triangleq & CE(AE(\mathrm{r}_{Ds}, \mathrm{s}_{Ds})) \\
 & & \text{address- and crc-encoded contents} \\
c_1 & \triangleq & \text{address error} \\
 & & \text{address error message} \\
c_2 & \triangleq & \text{crc error} \\
 & & \text{crc error message}
\end{array}
$$

$\mathrm{T}_{Ds} \triangleq$

$\tau_{Ds,1}$ $\quad \left(\epsilon = \mathbf{Rreq}?(n) \wedge \ell_{Ds} = 0 \wedge \Psi_2' = \Psi_2\,[1, n/\ell_{Ds}, \mathrm{r}_{Ds}]\right)$

The user requests the contents of logical sector n.

$\tau_{Ds,2}$ $\quad \vee \left(\epsilon = \mathbf{Rreqp!}(m) \wedge \ell_{Ds} = 1 \wedge \Psi_2' = \Psi_2\,[2/\ell_{Ds}]\right)$

The detection layer requests the to logical sector r_{Ds} mapped physical sector.

$\tau_{Ds,3}$ $\quad \vee \left(\epsilon = \mathbf{Rresp}?(cd) \wedge \ell_{Ds} = 2 \wedge Good \wedge \Psi_2' = \Psi_2\,[3, c/\ell_{Ds}, \mathrm{s}_{Ds}]\right)$

The physical disk responds with the contents of the requested sector and the detection layer detects no error in them.

$\tau_{Ds,4}$ $\quad \vee \left(\epsilon = \mathbf{Rresp}?(cd) \wedge \ell_{Ds} = 2 \wedge A.er \wedge \Psi_2' = \Psi_2\,[4, c_1/\ell_{Ds}, \mathrm{s}_{Ds}]\right)$

The physical disk responds with the contents of the requested sector and the detection layer detects a control system error.

$\tau_{Ds,5}$ $\quad \vee \left(\epsilon = \mathbf{Rresp}(cd) \wedge \ell_{Ds} = 2 \wedge C.er \wedge \Psi_2' = \Psi_2\,[4, c_2/\ell_{Ds}, \mathrm{s}_{Ds}]\right)$

The physical disk responds with the contents of the requested sector and the detection layer detects a disk surface damage error.

$\tau_{Ds,6}$ $\quad \vee \left(\epsilon = \mathbf{Res!}(\mathrm{s}_{Ds}) \wedge \ell_{Ds} = 3 \wedge \Psi_2' = \Psi_2\,[0/\ell_{Ds}]\right)$

The detection layer responds with the contents of the user requested sector.

$\tau_{Ds,7}$ $\quad \vee \left(\epsilon = \mathbf{Res!}(\mathrm{s}_{Ds}) \wedge \ell_{Ds} = 4 \wedge \Psi_2' = \Psi_2\,[5/\ell_{Ds}]\right)$

The detection layer responds with an error message and then stops.

$\tau_{Ds,8}$ $\quad \vee \ \left(\epsilon = \mathbf{Wreq}?(n,d) \wedge \ell_{Ds} = 0 \wedge \Psi_2' = \Psi_2\,[6, n, d/\ell_{Ds}, \mathrm{r}_{Ds}, \mathrm{s}_{Ds}]\right)$

The user requests that d should be written onto logical sector n.

$\tau_{Ds,9}$ $\quad \vee \ \left(\epsilon = \mathbf{Wreqp}!(m, dd) \wedge \ell_{Ds} = 6 \wedge \Psi_2' = \Psi_2\,[7/\ell_{Ds}]\right)$

The detection requests that dd should be written onto physical sector m.

$\tau_{Ds,10}$ $\quad \vee \ \left(\epsilon = \mathbf{Wresp}? \wedge \ell_{Ds} = 7 \wedge \Psi_2' = \Psi_2\,[8/\ell_{Ds}]\right)$

The physical disk responds with a signal to the detection layer that requested write is performed.

$\tau_{Ds,11}$ $\quad \vee \ \left(\epsilon = \mathbf{Wres}! \wedge \ell_{Ds} = 8 \wedge \Psi_2' = \Psi_2\,[0/\ell_{Ds}]\right)$

The detection layer responds with a signal to the user that the requested write is performed.

$\tau_{Ds,0}$ $\quad \vee \ \mathbf{stut}_{Ds}$

These transitions are illustrated in figure 4.3

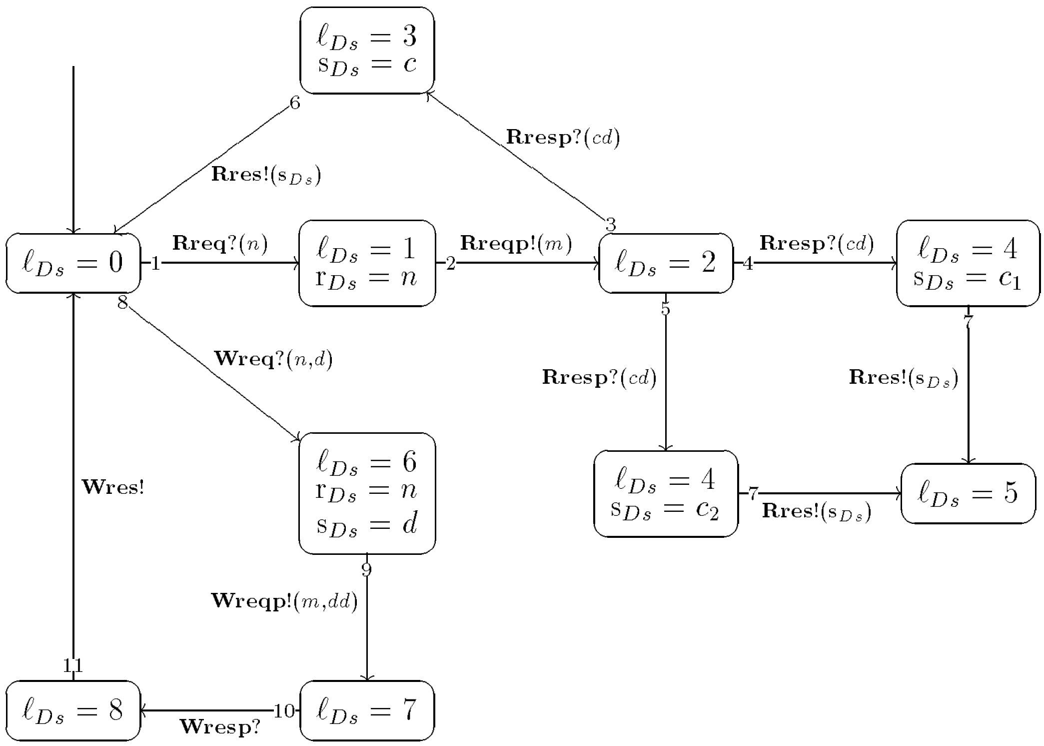

Figure 4.3: Transitions of the fail-stop detection layer.

4. **Liveness condition:**
The liveness condition expresses that the communication transitions are strongly fair. Let $\mathrm{SF}_{Ds} = \{\tau_{Ds,i} \mid i \in \{1, \ldots, 11\}\}$ then

$$\mathrm{L}_{Ds} \triangleq \bigwedge_{\tau \in \mathrm{SF}_{Ds}} (\Box\Diamond En(\tau) \rightarrow \Box\Diamond\tau)$$

4.5.3 Requirement W_{Ds}

The requirement W_{Ds} should express that no errors are detected.

$$\mathrm{W}_P \triangleq \Box(\epsilon = \mathbf{Rresp}?(cd) \rightarrow Good)$$

4.5.4 $\mathcal{S}_{Ds} \parallel \mathcal{S}_P$ relatively refines $\mathcal{S}_P$

The communication channels of $\mathcal{S}_P$ in $\mathcal{S}_{Ds} \parallel \mathcal{S}_P$ should be renamed in order to compose $\mathcal{S}_{Ds}$ with $\mathcal{S}_P$, i.e., instead of H_P as specification we should take

$$\mathrm{H}_P\,[\mathbf{Rreqp}, \mathbf{Wreqp}, \mathbf{Rresp}, \mathbf{Wresp}/\mathbf{Rreq}, \mathbf{Wreq}, \mathbf{Rres}, \mathbf{Wres}]\,.$$

Let $\mathcal{S}_{P1}$ be the specification with this renaming. According to theorem 8 $\mathcal{S}_{Ds}\ |\overline{\mathrm{w}}|\ \mathcal{S}_{P1}$ relatively refines $\mathcal{S}_P$ with respect to $(\mathbf{true}, \mathrm{W}_P)$ iff the following holds:

$$\mathfrak{O}(B_{Ds,P1}) = \mathfrak{O}(B_P) \text{ and}$$
$$\models (\exists \mathrm{X}_{Ds,P1}\,.\,(\mathrm{G}_{Ds,P1})) \rightarrow (\exists \mathrm{X}_P\,.\,(\mathrm{G}_P))$$

where $\mathrm{X}_{Ds,P1}$ are the local variables from $\mathcal{S}_{Ds} \parallel \mathcal{S}_{P1}$, i.e., $\mathrm{X}_{Ds,P1} \triangleq \{\ell_{Ds}, \mathrm{r}_{Ds}, \mathrm{s}_{Ds}, \mathrm{LS}_{Ds}[i] \mid i \in LN\} \cup \{\ell_{P1}, \mathrm{r}_{P1}, \mathrm{s}_{P1}, \mathrm{M}_{P1}[n], \mathrm{F}[n] \mid n \in PN\}$ and $\mathrm{G}_{Ds,P1}$ is defined as

$$\exists \epsilon_1, \epsilon_2 . _{B^A_{Ds}} \odot _{B^A_{P1}} (\epsilon, \epsilon_1, \epsilon_2) \wedge (\mathrm{H}_{Ds} \wedge \mathrm{W}_{Ds})\,[\epsilon_1/\epsilon] \wedge (\mathrm{H}_{P1} \wedge \mathrm{W}_{P1})\,[\epsilon_2/\epsilon]$$

This can be rewritten to following machine specification of $\mathcal{S}_2$: $\mathcal{S}_2 = (B_2, \mathrm{H}_2)$ where $\mathrm{H}_2 \triangleq \mathrm{I}_2 \wedge \Box \mathrm{T}_2 \wedge \mathrm{L}_2$ and B_2, I_2, T_2 and L_2 are as follows:

1. **Basis** $B_2 = ((\mathrm{In}_2, \mathrm{Out}_2), (\mathrm{V}_2, \mathrm{X}_2))$

$$\begin{array}{lcl}
\mathrm{In}_2 & \triangleq & \{\mathbf{Rreq}, \mathbf{Wreq}\} \\
\mathrm{Out}_2 & \triangleq & \{\mathbf{Rres}, \mathbf{Wres}\}, \\
\mathrm{V}_2 & \triangleq & \emptyset, \\
\mathrm{X}_2 & \triangleq & \{\ell_{Ds}, \mathrm{r}_{Ds}, \mathrm{s}_{Ds}, \mathrm{LS}_{Ds}[i] \mid i \in LN\} \\
 & & \cup\{\ell_{P1}, \mathrm{r}_{P1}, \mathrm{s}_{P1}, \mathrm{M}_{P1}[n], \mathrm{F}[n] \mid n \in PN\}
\end{array}$$

Let

$$\begin{array}{lcl}
\Psi_{12} & \triangleq & (\ell_{Ds}, \mathrm{r}_{Ds}, \mathrm{s}_{Ds}, \mathrm{LS}_{Ds}[1], \ldots, \mathrm{LS}_{Ds}[Y], \\
 & & \ell_{P1}, \mathrm{r}_{P1}, \mathrm{s}_{P1}, \mathrm{M}_{P1}[1], \ldots, \mathrm{M}_{P1}[Y], \mathrm{F}[1], \ldots, \mathrm{F}[Y])) \\
\Psi'_{12} & \triangleq & (\ell'_{Ds}, \mathrm{r}'_{Ds}, \mathrm{s}'_{Ds}, \mathrm{LS}'_{Ds}[1], \ldots, \mathrm{LS}'_{Ds}[Y], \\
 & & \ell'_{P1}, \mathrm{r}'_{P1}, \mathrm{s}'_{P1}, \mathrm{M}'_{P1}[1], \ldots, \mathrm{M}'_{P1}[Y], \mathrm{F}'[1], \ldots, \mathrm{F}'[Y])
\end{array}$$

2. **Initial states:**

$$\mathrm{I}_2 \triangleq \ell_{Ds} = 0 \wedge \ell_{P1} = 0 \wedge \bigwedge_{i \in LN} \mathrm{LS}_{Ds}[i] = i \wedge \bigwedge_{i \in PN} (\mathrm{M}_{P1}[i] = dflt \wedge \mathrm{F}[i] = i)$$

3. **Transitions:**
Let

$$\begin{array}{lcl} c & \triangleq & AD(CD(\mathrm{M}_{P1}[\mathrm{F}[\mathrm{r}_{P1}]])) \\ & & \text{the address- and crc-decoded contents} \\ m & \triangleq & \mathrm{LS}_{Ds}[\mathrm{r}_{Ds}] \\ & & \text{physical sector} \\ dd & \triangleq & CE(AE(\mathrm{r}_{Ds}, \mathrm{s}_{Ds})) \\ & & \text{address- and crc-encoded contents} \end{array}$$

$\mathrm{T}_2 \triangleq$

$\tau_{2,1}$ $\Big(\epsilon = \mathbf{Rreq}?(n) \wedge \ell_{Ds} = 0 \wedge \ell_{P1} = 0 \wedge \Psi'_{12} = \Psi_{12}\,[1, n/\ell_{Ds}, \mathrm{r}_{Ds}]\Big)$
The user requests the contents of logical sector n.

$\tau_{2,2}$ $\vee$ $\Big(\epsilon = \mathbf{i} \wedge \ell_{Ds} = 1 \wedge \ell_{P1} = 0 \wedge \Psi'_{12} = \Psi_{12}\,[2, 1, m/\ell_{Ds}, \ell_{P1}, \mathrm{r}_{P1}]\Big)$
The detection layer requests the to logical sector r_{Ds} mapped physical sector.

$\tau_{2,3}$ $\vee$ $\Big(\epsilon = \mathbf{i} \wedge \ell_{Ds} = 2 \wedge \ell_{P1} = 1 \wedge \Psi'_{12} = \Psi_{12}\,[3, c, 0/\ell_{Ds}, \mathrm{s}_{Ds}, \ell_{P1}]\Big)$
The physical disk responds with the contents of the requested sector and because of W_{P1} and W_{Ds} they are correct.

$\tau_{2,4}$ $\vee$ $\Big(\epsilon = \mathbf{Rres}!(\mathrm{s}_{Ds}) \wedge \ell_{Ds} = 3 \wedge \ell_{P1} = 0 \wedge \Psi'_{12} = \Psi_{12}\,[0/\ell_{Ds}]\Big)$
The detection layer responds with the contents of the user requested sector.

$\tau_{2,5}$ $\vee$ $\Big(\epsilon = \mathbf{Wreq}?(n, d) \wedge \ell_{Ds} = 0 \wedge \ell_{P1} = 0 \wedge \Psi'_{12} = \Psi_{12}\,[6, n, d/\ell_{Ds}, \mathrm{r}_{Ds}, \mathrm{s}_{Ds}]\Big)$
The user requests that d should be written onto logical sector n.

$\tau_{2,6}$ $\vee$ $\Big(\epsilon = \mathbf{i} \wedge \ell_{Ds} = 6 \wedge \ell_{P1} = 0 \wedge \Psi'_{12} = \Psi_{12}\,[7, 2, m, dd/\ell_{Ds}, \ell_{P1}, \mathrm{r}_{P1}, \mathrm{s}_{P1}]\Big)$
The detection requests that dd should be written onto physical sector m.

$\tau_{2,7}$ $\vee$ $\Big(\epsilon = \mathbf{i} \wedge \ell_{Ds} = 7 \wedge \ell_{P1} = 2 \wedge \Psi'_{12} = \Psi_{12}\,[8, 0, \mathrm{s}_{P1}/\ell_{Ds}, \ell_{P1}, \mathrm{M}_{P1}[\mathrm{F}[\mathrm{r}_{P1}]]]\Big)$
The physical disk responds with a signal to the detection layer that requested write is performed.

$\tau_{2,8}$ $\vee$ $\Big(\epsilon = \mathbf{Wres}! \wedge \ell_{Ds} = 8 \wedge \ell_{P1} = 0 \wedge \Psi'_{12} = \Psi_{12}\,[0/\ell_{Ds}]\Big)$
The detection layer responds with a signal to the user that the requested write is performed.

$\tau_{2,0}$ $\vee$ $\mathbf{stut}_2$

Figure 4.4 illustrates the transitions of the relative composed system $\mathcal{S}_{Ds}\ |\overline{\mathrm{w}}|\ \mathcal{S}_{P1}$. Due to ${}_{B^A_{Ds}} \odot_{B^A_{P1}} (\epsilon, \epsilon_1, \epsilon_2)$ the communications events with the physical disk are transformed into $\mathbf{i}$ events and due to W_{Ds} and W_{P1} no faults occur and no errors are detected.

4. **Liveness condition:**
The liveness condition expresses that all non-stutter transitions are strongly fair. Let $\mathrm{SF}_{Ds} = \{\tau_{2,i} \mid i \in \{1, \ldots, 8\}\}$ then

$$\mathrm{L}_2 \triangleq \bigwedge_{\tau \in \mathrm{SF}_2} (\Box\Diamond En(\tau) \rightarrow \Box\Diamond\tau)$$

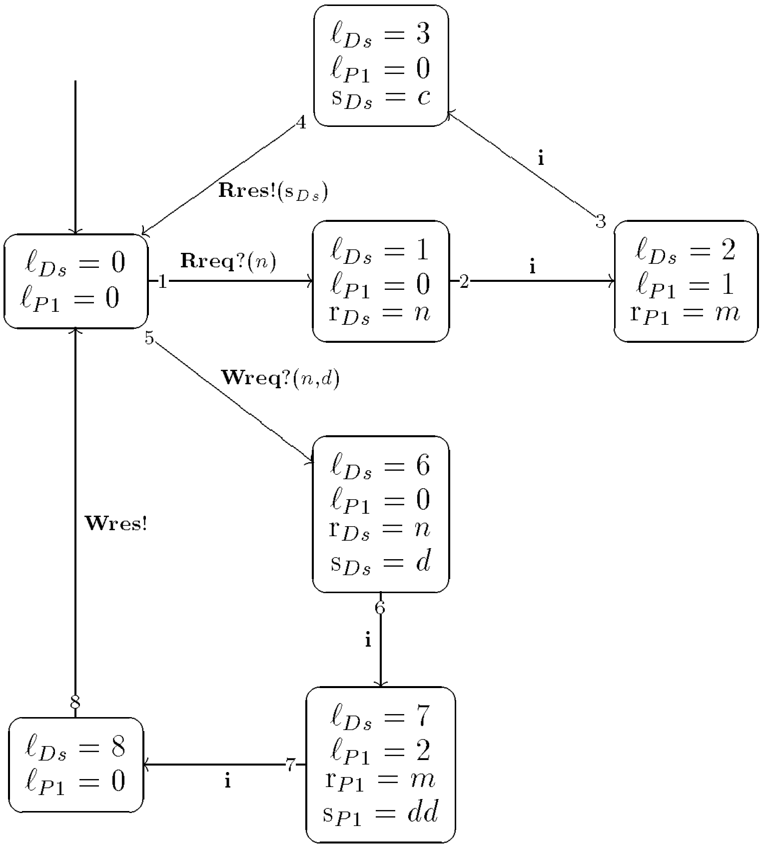

Figure 4.4: Transitions of the relative composed system.

X_P are the local variables from $\mathcal{S}_P$, i.e., $X_P \triangleq \{\ell_P, r_P, s_P, M_P[n], F[n] \mid n \in PN\}$ and G_P is defined as

$$I_P \wedge \Box T_P \wedge L_P \wedge W_P$$

Rule 3 will be used to prove

$$\models (\exists X_2 \,.\, (G_2)) \rightarrow (\exists X_P \,.\, (G_P))\,.$$

This means one has to prove (a), (b) and (c) below, for $\bar{f}$ the refinement mapping from $\mathcal{S}_2$ to $\mathcal{S}_P$, defined as: $\bar{f} = f_{\ell_P}, f_{r_P}, f_{s_P}, f_{M_P[n]}, f_{F_P[n]}$ $(n \in SN)$. The refinement mappings are defined as:

$$
\begin{array}{llll}
f_{\ell_P} & & & \\
if & \ell_{Ds} = 0 & then & \ell_{Ds} \\
 & \ell_{Ds} = 1 & then & \ell_{Ds} \\
 & \ell_{Ds} = 2 & then & \ell_{Ds} - 1 \\
 & \ell_{Ds} = 3 & then & \ell_{Ds} - 2 \\
 & \ell_{Ds} = 6 & then & \ell_{Ds} - 4 \\
 & \ell_{Ds} = 7 & then & \ell_{Ds} - 5 \\
 & \ell_{Ds} = 8 & then & \ell_{Ds} - 6
\end{array}
$$

$$
\begin{array}{lcl}
f_{\mathrm{r}_P} & \triangleq & \mathrm{r}_{Ds} \\
f_{\mathrm{s}_P} & \triangleq & \mathrm{s}_{Ds} \\
f_{\mathrm{M}_P[n]} & \triangleq & AD(CD(\mathrm{M}_{P1}[\mathrm{LS}[n]])) \\
f_{\mathrm{F}_P[n]} & \triangleq & \mathrm{F}_{P1}[\mathrm{LS}[n]]
\end{array}
$$

$$
\begin{array}{ll}
(a) & \mathcal{S}_2 \models (\mathrm{I}_2) \rightarrow (\mathrm{I}_P \wedge p)\left[\bar{f}/\mathrm{X}_P\right] \\
(b) & \mathcal{S}_2 \models \mathrm{T}_2 \rightarrow (\mathrm{T}_P \wedge ((p \wedge p') \vee \mathbf{stut}_P))\left[\bar{f}/\mathrm{X}_P\right] \\
(c) & \mathcal{S}_2 \models \mathrm{L}_P\left[\bar{f}/\mathrm{X}_P\right]
\end{array}
$$

(a) **Proof 11**

$$
\begin{array}{ll}
 & \mathrm{I}_2 \\
= & \quad \%\ \ Def.\ \mathrm{I}_2 \\
 & \ell_{Ds} = 0 \wedge \ell_{P1} = 0 \wedge \bigwedge_{i \in LN} \mathrm{LS}_{Ds}[i] = i \wedge \bigwedge_{i \in PN}(\mathrm{M}_{P1}[i] = dflt \wedge \mathrm{F}[i] = i) \\
\rightarrow & \quad \%\ \ Def.\ \bar{f},\ p \\
 & (\ell_P = 0 \wedge \bigwedge_{i \in PN}(\mathrm{M}_P[i] = dflt \wedge \mathrm{F}[i] = i) \wedge p)\left[\bar{f}/\mathrm{X}_P\right] \\
= & \quad \%\ \ Def.\ \mathrm{I}_P \\
 & (\mathrm{I}_P \wedge p)\left[\bar{f}/\mathrm{X}_P\right]
\end{array}
$$

(b) **Proof 12**

Since T_P *is of the form* $\mathbf{stut}_P \vee \bigvee_\tau(\epsilon = \mathbf{a}_\tau \wedge trans_\tau)$ *then* $\mathrm{T}_P \wedge ((p \wedge p') \vee \mathbf{stut}_P)$ *is equal to* $\mathbf{stut}_P \vee \bigvee_\tau(\epsilon = \mathbf{a}_\tau \wedge trans_\tau \wedge p \wedge p')$.

–
$$
\begin{array}{ll}
 & \tau_{2,1} \\
= & \left(\epsilon = \mathbf{Rreq}?(n) \wedge \ell_{Ds} = 0 \wedge \ell_{P1} = 0 \wedge \Psi_{12}' = \Psi_{12}\left[1, n/\ell_{Ds}, \mathrm{r}_{Ds}\right]\right) \\
\rightarrow & \left(\epsilon = \mathbf{Rreq}?(n) \wedge \ell_P = 0 \wedge p \wedge p' \wedge \Psi_1' = \Psi_1\left[1, n/\ell_P, \mathrm{r}_P\right]\right)\left[\bar{f}/\mathrm{X}_P\right] \\
= & (\tau_{P,1} \wedge p \wedge p')\left[\bar{f}/\mathrm{X}_P\right]
\end{array}
$$

The user read request at the second level corresponds to the user read request at the first level.

–
$$
\begin{array}{ll}
 & \tau_{2,2} \\
= & \left(\epsilon = \mathbf{i} \wedge \ell_{Ds} = 1 \wedge \ell_{P1} = 0 \wedge \Psi_{12}' = \Psi_{12}\left[2, 1, m/\ell_{Ds}, \ell_{P1}, \mathrm{r}_{P1}\right]\right) \\
\rightarrow & \left(\epsilon = \mathbf{i} \wedge \Psi_1' = \Psi_1\right)\left[\bar{f}/\mathrm{X}_P\right] \\
\rightarrow & \mathbf{stut}_P\left[\bar{f}/\mathrm{X}_P\right]
\end{array}
$$

The read request to the physical disk at the second level corresponds to stutter step of the physical disk at the first level.

–
$$
\begin{array}{ll}
 & \tau_{2,3} \\
= & \left(\epsilon = \mathbf{i} \wedge \ell_{Ds} = 2 \wedge \ell_{P1} = 1 \wedge \Psi_{12}' = \Psi_{12}\left[3, c, 0/\ell_{Ds}, \mathrm{s}_{Ds}, \ell_{P1}\right]\right) \\
\rightarrow & \left(\epsilon = \mathbf{i} \wedge \Psi_1' = \Psi_1\right)\left[\bar{f}/\mathrm{X}_P\right] \\
\rightarrow & \mathbf{stut}_P\left[\bar{f}/\mathrm{X}_P\right]
\end{array}
$$

The read response of the physical disk at the second level corresponds to the stutter step of the physical disk at the first level.

– $\tau_{2,4}$

$= \left(\epsilon = \mathbf{Rres}!(\mathrm{s}_{Ds}) \wedge \ell_{Ds} = 3 \wedge \ell_{P1} = 0 \wedge \Psi_{12}' = \Psi_{12}\,[0/\ell_{Ds}]\right)$

$\rightarrow \left(\epsilon = \mathbf{Rres}!(\mathrm{M}_P[\mathrm{F}[\mathrm{r}_P]]) \wedge \ell_P = 1 \wedge p \wedge p' \wedge \Psi_1' = \Psi_1\,[0/\ell_P]\right)\left[\bar{f}/\mathrm{X}_P\right]$

$= (\tau_{P,2} \wedge p \wedge p')\left[\bar{f}/\mathrm{X}_P\right]$

The read response of the detection layer at the second level corresponds to the read response of the physical disk at the first level.

– $\tau_{2,5}$

$= \epsilon = \mathbf{Wreq}?(n, d) \wedge (\ell_{Ds}, \ell_{P1}) = (0, 0)$

$\wedge \Psi_{12}' = \Psi_{12}\,[6, n, d/\ell_{Ds}, \mathrm{r}_{Ds}, \mathrm{s}_{Ds}]$

$\rightarrow \epsilon = \mathbf{Wreq}?(n, d) \wedge \ell_P = 0 \wedge p \wedge p'$

$\wedge \Psi_1' = \Psi_1\,[2, n, d/\ell_P, \mathrm{r}_P, \mathrm{s}_P]\left[\bar{f}/\mathrm{X}_P\right]$

$= (\tau_{P,3} \wedge p \wedge p')\left[\bar{f}/\mathrm{X}_P\right]$

The user write request at the second level corresponds to the user write request at the first level.

– $\tau_{2,6}$

$= \left(\epsilon = \mathbf{i} \wedge \ell_{Ds} = 6 \wedge \ell_{P1} = 0 \wedge \Psi_{12}' = \Psi_{12}\,[7, 2, m, dd/\ell_{Ds}, \ell_{P1}, \mathrm{r}_{P1}, \mathrm{s}_{P1}]\right)$

$\rightarrow \left(\epsilon = \mathbf{i} \wedge \Psi_1' = \Psi_1\right)\left[\bar{f}/\mathrm{X}_P\right]$

$\rightarrow \mathbf{stut}_P\left[\bar{f}/\mathrm{X}_P\right]$

The write request to the physical disk at the second level corresponds to the stutter step of the physical disk at the first level.

– $\tau_{2,7}$

$= \left(\epsilon = \mathbf{i} \wedge \ell_{Ds} = 7 \wedge \ell_{P1} = 2 \wedge \Psi_{12}' = \Psi_{12}\,[8, 0/\ell_{Ds}, \ell_{P1}]\right)$

$\rightarrow \left(\epsilon = \mathbf{i} \wedge \Psi_1' = \Psi_1\right)\left[\bar{f}/\mathrm{X}_P\right]$

$\rightarrow \mathbf{stut}_P\left[\bar{f}/\mathrm{X}_P\right]$

The write response of the physical disk at the second level corresponds to the stutter step of the physical disk at the first level.

– $\tau_{2,8}$

$= \left(\epsilon = \mathbf{Wres}! \wedge \ell_{Ds} = 8 \wedge \ell_{P1} = 0 \wedge \Psi_{12}' = \Psi_{12}\,[0/\ell_{Ds}]\right)$

$\rightarrow \left(\epsilon = \mathbf{Wres}! \wedge \ell_P = 2 \wedge p \wedge p' \wedge \Psi_1' = \Psi_1\,[0, \mathrm{s}_P/\ell_P, \mathrm{M}_P[\mathrm{F}[\mathrm{r}_P]]]\right)\left[\bar{f}/\mathrm{X}_P\right]$

$= (\tau_{P,4} \wedge p \wedge p')\left[\bar{f}/\mathrm{X}_P\right]$

The write response of the detection layer at the second level corresponds to the write response of the physical disk at the first level.

– $\mathbf{stut}_2 \rightarrow \mathbf{stut}_P\left[\bar{f}/\mathrm{X}_P\right]$

(c) Let $\mathrm{SF}_P = \{\tau_{P,i} \mid i \in \{1, 2, 3, 4\}\}$ then

$$\mathrm{L}_P \triangleq \bigwedge_{\tau \in \mathrm{SF}_P} (\Box\Diamond En(\tau) \rightarrow \Box\Diamond\tau)$$

. Let $\mathrm{SF}_2 = \{\tau_{2,i} \mid i \in \{1, \ldots, 8\}\}$ then

$$\mathrm{L}_2 \triangleq \bigwedge_{\tau \in \mathrm{SF}_2} (\Box\Diamond En(\tau) \rightarrow \Box\Diamond\tau).$$

Then the following holds

$$\mathcal{S}_2 \models \mathrm{L}_2 \rightarrow \mathrm{L}_P \left[\bar{f}/\mathrm{X}_P\right]$$

So

$$\mathcal{S}_2 \models \mathrm{L}_P \left[\bar{f}/\mathrm{X}_P\right]$$

holds.

4.6 Fourth Step: Error Recovery Layer

4.6.1 Introduction

In this step the error recovery layer is specified. This is the layer that tries to correct the errors detected by the detection layer. The technique used for error recovery is that of the *mirrored disk concept* [LA90]. This mirror disk concept is as follows: instead of one physical disk and corresponding detection layer N physical disks with identical contents and N corresponding detection layers ($N > 1$) are maintained. In case some information can no longer be retrieved from a disk, the information is still available on another one. The user requests some contents from the error recovery layer. The error recovery layer selects a disk from which it can retrieve these contents. Then it requests these contents from the corresponding detection layer of that disk. The detection layer requests then the contents from the physical disk and checks whether the contents are correct. The detection layer then signals if the contents are correct and if not it will signal which error has it has detected. If the contents are correct the error recovery layer will send them to the user and is then ready for new requests from the user. As seen before the detection layer can detect two kinds of errors: (1) errors due to disk surface damage fault and (2) errors due to disk control system faults. The error recovery layer will react as follows on these errors:

ad (1) First, the error recovery layer selects another disk from which it can retrieve the requested contents and when the corresponding detection layer signals that the contents are correct, the error recovery layer will write these contents to another location of the affected disk. In order to retrieve these contents from this new location *logical* locations are introduced. When contents are stored at a new physical location the logical location will be pointing to this new location. So actually the data are retrieved from their logical location. Subsequently the error recovery layer will send the contents to the user and is ready to receive new requests from the user. When the detection-layer of the second disk also reports an error the error recovery layer will react as described in *ad(1)* and *ad(2)* depending on the kind of error detected.

ad (2) First, the error recovery layer disables the faulty disk and then it will select another disk from which it can retrieve the requested contents and when the corresponding detection layer signals that the contents are correct the error recovery layer will them to the user. When the detection-layer of the second disk also reports an error the error recovery layer will react as described in *ad(1)* and *ad(2)* depending on the kind of error detected.

This error recovery process only works if the following assumptions are made:

- In order to store the contents on a new physical location enough spare locations should be available on an affected disk.
- Furthermore, the following must always hold in order to recover the *ad(1)*-type of error on a disk or to retrieve the contents from a logical location: for all logical locations there exists at least one non-disabled physical disk that has correct data stored on that logical location. This condition guarantees that always, each logical location contains correct data (on which disk we don't know, but it is a non-disabled one and it is not the disk whose type 1 error has to be repaired).

4.6.2 Specification of the Recovery Layer

The error recovery layer acts as interface between the user and the N detection layers of the N physical disks. The user requests with a $\mathbf{Rreq}(n)$ event the contents of some logical sector n. The error recovery layer requests these contents, on receipt of this event, by issuing a $\mathbf{Rreqd}_i(n)$ event to one of the non-disabled detection layers. This detection layer responds with an $\mathbf{Rresd}_i(d)$ event. As seen in the third step there are three possibilities:

1. If this event delivers a message saying that the, to this detection layer corresponding, physical disk has been affected by a disk control system fault then this detection layer will be disabled and the error-recovery layer will send a $\mathbf{Rreqd}_j(n)$ event to another non-disabled detection layer.
2. If this event delivers a message that the, to this detection layer corresponding, physical disk has been affected by a disk surface damage fault then the error recovery layer requests the contents with a $\mathbf{Rreqd}_j(n)$ from another non-disabled detection layer until it finds a detection layer that responds with the correct contents. Then the error recovery layer can "repair" the physical disks that has been affected by a disk surface damage fault at the same logical sector by generating a $\mathbf{Wreqd}_j$ write request event with the correct data to the same logical sector number of the corresponding detection layers of those physical disks. The detections layers will respond with a **Wresd** indicating that the affected physical disks has been repaired. The design decision we make is that the detection layer has to find the spare physical sector to which these contents can be written. After that, the error recovery layer responds with a $\mathbf{Rres}(c)$ event to deliver the requested contents.
3. If this event delivers normal data the error recovery layer will respond with a $\mathbf{Rres}(c)$ event delivering the requested contents.

The user requests with a **Wreq**(n, d) event that d has to be written onto a logical sector n. The error recovery layer requests with a **Wreqd**(n, d) event to all non-disabled detection layers that d has to written on logical sector n to ensure that the corresponding physical disks have identical contents on their logical sectors. The detection layers then respond to these requests with a **Wresd** event. The error recovery layer then responds with a **Wres** event to the user that the write operation has been performed.

The stable storage layer is described by the following specification: $\mathcal{S}_R = (B_R, \mathrm{H}_R)$ where $\mathrm{H}_R \triangleq \mathrm{I}_R \wedge \Box \mathrm{T}_R \wedge \mathrm{L}_R$ and B_R, I_R, T_R and L_R are as follows:

1. **Basis** $B_R = ((\mathrm{In}_R, \mathrm{Out}_R), (\mathrm{V}_R, \mathrm{X}_R))$

$$
\begin{array}{lcl}
\mathrm{In}_R & \triangleq & \{\mathbf{Rreq}, \mathbf{Wreq}, \mathbf{Rresd}_i, \mathbf{Wresd}_i \mid i \in Nd\}, \\
\mathrm{Out}_R & \triangleq & \{\mathbf{Rres}, \mathbf{Wres}, \mathbf{Rreqd}_i, \mathbf{Wreqd}_i \mid i \in Nd\}, \\
\mathrm{V}_R & \triangleq & \emptyset, \\
\mathrm{X}_R & \triangleq & \{\ell_R, \mathrm{r}_R, \mathrm{s}_R, \mathrm{t}_R, \mathrm{G}, \mathrm{A}, \mathrm{W}\}
\end{array}
$$

- **Rreq**$?(n)$: the request from the user to read logical sector n.
- **Rres**$!(c)$: the response of the error recovery layer to the previous request where c are the crc-decoded and address-decoded contents of the requested logical sector.
- **Wreq**$?(n, d)$: user request to write information item d onto logical sector n.
- **Wres**!: write response to the user that the requested information is written.
- **Rreqd**$!_i(n)$: the read request from the error recovery layer towards detection layer i.
- **Rresd**$?_i(c)$: the read response from detection layer i to the previous request where c are the contents of the requested logical sector.
- **Wreqd**$!_i(n, d)$: the write request from the error recovery layer to detection layer i to write information item d onto logical sector n.
- **Wresd**$?_i$: response from detection layer i to the error recovery layer that the requested information has been written.
- ℓ_R: local variable indicating the status of the error recovery layer; $\ell_R = 0$: the error recovery layer is waiting for a request, $\ell_R = 1$: the user has issued a read request or the detection layer responded to a read request with affected data, $\ell_R = 2$: the error recovery layer has issued a read request, $\ell_R = 3$: the detection responded to a read request with correct data or all affected disk are repaired, $\ell_R = 4$: the the detection responded to a read request with correct data and there are affected disks, $\ell_R = 5$: the error recovery layer has issued a write request to repair an affected disk and there are still affected disks to be repaired, $\ell_R = 6$: the error recovery layer has issued a write request to repair an affected disk and there are no more affected disks, $\ell_R = 7$: the user has issued a write request, $\ell_R = 8$: the error recovery layer has issued a write request and there are still to be written disks, $\ell_R = 9$: the error recovery layer has issued a write request and there are no more to be written disks, $\ell_R = 10$: the detection layer of the last to be written disk responded to a write request.

- r_R: local variable indicating the requested sector.
- s_R: local variable indicating the requested contents or the requested contents to be written.
- t_R: local variable indicating the index of the disk to which a request has been issued.
- G: local variable indicating the set of indexes of non-disabled disks.
- A: local variable indicating the set of indexes of by control system faults affected disks.
- W: local variable indicating the set of indexes on which data should be written.

Let $\Psi_3 \triangleq (\ell_R, \mathrm{r}_R, \mathrm{s}_R, \mathrm{t}_R, \mathrm{G}, \mathrm{A}, \mathrm{W})$ and $\Psi_3' \triangleq (\ell_R', \mathrm{r}_R', \mathrm{s}_R', \mathrm{t}_R, \mathrm{G}', \mathrm{A}', \mathrm{W}')$.

2. **Initial States:**

$$\mathrm{I}_R \triangleq \ell_R = 0 \wedge \mathrm{G} = \{1, \ldots, N\} \wedge \mathrm{A} = \emptyset$$

The error recovery layer is waiting for requests from the user and all the N disks are non-disabled.

3. **Transitions:**
Let

- $c_1 \triangleq$ address error
  address error message
- $c_2 \triangleq$ crc error
  crc error message
- $Good1 \triangleq i = \mathrm{t}_R \wedge dc \neq c_1 \wedge dc \neq c_2 \wedge \mathrm{A} = \emptyset$
  data is not affected by faults and the number of affected disks is zero
- $Good2 \triangleq i = \mathrm{t}_R \wedge dc \neq c_1 \wedge dc \neq c_2 \wedge \mathrm{A} \neq \emptyset$
  data is not affected by faults and the number of affected disks is non-zero
- $A.er \triangleq i = \mathrm{t}_R \wedge dc = c_1$
  data is affected by control system fault
- $C.er \triangleq i = \mathrm{t}_R \wedge dc = c_2$
  data is affected by disk surface damage
- $\mathrm{G}^- \triangleq \mathrm{G} \setminus \{i\}$
  set of good disks minus i
- $\mathrm{A}^- \triangleq \mathrm{A} \setminus \{i\}$
  set of affected disks minus i
- $\mathrm{A}^+ \triangleq \mathrm{A} \cup \{i\}$
  set of affected disks plus i
- $\mathrm{W}^- \triangleq \mathrm{W} \setminus \{i\}$
  set of to be written disks minus i

- $C1 \triangleq i \in \mathrm{G} \wedge i \notin \mathrm{A}$
  disk i is good and not affected
- $C2 \triangleq i \in \mathrm{A} \wedge \mathrm{A}^- \neq \emptyset$
  disk i is affected and the number of affected disks is greater than 1
- $C3 \triangleq i \in \mathrm{A} \wedge \mathrm{A}^- = \emptyset$
  disk i is the only affected disk
- $C4 \triangleq i \in \mathrm{W} \wedge \mathrm{W}^- \neq \emptyset$
  disk i should be written onto and the number of to be written disks is greater than 1
- $C5 \triangleq i \in \mathrm{W} \wedge \mathrm{W}^- = \emptyset$
  disk i is the only disk to be written onto

$\mathrm{T}_R \triangleq$

$\tau_{R,1}$ $\big(\epsilon = \mathbf{Rreq}?(n) \wedge \ell_R = 0 \wedge \Psi_3' = \Psi_3\,[1, n/\ell_R, \mathrm{r}_R]\big)$

The user requests the contents of logical sector n.

$\tau_{R,2}$ $\vee\ \big(\epsilon = \mathbf{Rreqd!}_i(\mathrm{r}_R) \wedge \ell_R = 1 \wedge C1 \wedge \Psi_3' = \Psi_3\,[2, i/\ell_R, \mathrm{t}_R]\big)$

The error recovery layer requests the contents of logical sector r_R from an enabled detection layer.

$\tau_{R,3}$ $\vee\ \big(\epsilon = \mathbf{Rresd}?_i(cd) \wedge \ell_R = 2 \wedge Good1 \wedge \Psi_3' = \Psi_3\,[3, cd/\ell_R, \mathrm{s}_R]\big)$

The detection layer responds with the contents of the requested sector and the detection layer has detected no error in them.

$\tau_{R,4}$ $\vee\ \big(\epsilon = \mathbf{Rresd}?_i(cd) \wedge \ell_R = 2 \wedge A.er \wedge \Psi_3' = \Psi_3\,[1, \mathrm{G}^-/\ell_R, \mathrm{G}]\big)$

The detection layer responds with the contents of the requested sector and the detection layer has detected an control system error, so this detection layer will be disabled.

$\tau_{R,5}$ $\vee\ \big(\epsilon = \mathbf{Rresd}?_i(cd) \wedge \ell_R = 2 \wedge C.er \wedge \Psi_3' = \Psi_3\,[1, \mathrm{A}^+/\ell_R, \mathrm{A}]\big)$

The detection layer responds with the contents of the requested sector and the detection layer detects an disk surface damage error, so disk i has to be repaired.

$\tau_{R,6}$ $\vee\ \big(\epsilon = \mathbf{Rresd}?_i(cd) \wedge \ell_R = 2 \wedge Good2 \wedge \Psi_3' = \Psi_3\,[4, cd/\ell_R, \mathrm{s}_R]\big)$

A correct disk has been found so the error recovery layer can repair the affected disks.

$\tau_{R,7}$ $\vee\ \big(\epsilon = \mathbf{Wreqd!}_i(\mathrm{r}_R, \mathrm{s}_R) \wedge \ell_R = 4 \wedge C2 \wedge \Psi_3' = \Psi_3\,[5, i, \mathrm{A}^-/\ell_R, \mathrm{t}_R, \mathrm{A}]\big)$

An affected disk is being repaired and there are still unrepaired disk.

$\tau_{R,8}$ $\vee\ \big(\epsilon = \mathbf{Wresd}?_i \wedge \ell_R = 5 \wedge i = \mathrm{t}_R \wedge \Psi_3' = \Psi_3\,[4/\ell_R]\big)$

The affected disk is repaired.

$\tau_{R,9}$ $\vee\ \big(\epsilon = \mathbf{Wreqd!}_i(\mathrm{r}_R, \mathrm{s}_R) \wedge \ell_R = 4 \wedge C3 \wedge \Psi_3' = \Psi_3\,[6, \mathrm{A}^-/\ell_R, \mathrm{A}]\big)$

An affected disk is being repaired and there are no unrepaired disks.

$\tau_{R,10}$ $\vee\ \big(\epsilon = \mathbf{Wresd}?_i \wedge \ell_R = 6 \wedge i = \mathrm{t}_R \wedge \Psi_3' = \Psi_3\,[3/\ell_R]\big)$

All affected disk are repaired, so the user requested contents can be sent.

$\tau_{R,11}$ $\quad \vee \ \big(\epsilon = \mathbf{Rres!}(\mathrm{s}_R) \wedge \ell_R = 3 \wedge \Psi_3' = \Psi_3\,[0/\ell_R]\big)$

The error recovery layer responds with the requested contents.

$\tau_{R,12}$ $\quad \vee \ \big(\epsilon = \mathbf{Wreq?}(n, d) \wedge \ell_R = 0 \wedge \Psi_3' = \Psi_3\,[7, n, d, \mathrm{G}/\ell_R, \mathrm{r}_R, \mathrm{s}_R, \mathrm{W}]\big)$

The user requests that d should be written onto logical sector n.

$\tau_{R,13}$ $\quad \vee \ \big(\epsilon = \mathbf{Wreqd!}_i(\mathrm{r}_R, \mathrm{s}_R) \wedge \ell_R = 7 \wedge C4 \wedge \Psi_3' = \Psi_3\,[8, i, \mathrm{W}^-/\ell_R, \mathrm{t}_R, \mathrm{W}]\big)$

The requested information is being written to a disk and there are still disks which haven't written them.

$\tau_{R,14}$ $\quad \vee \ \big(\epsilon = \mathbf{Wresd?}_i \wedge \ell_R = 8 \wedge i = \mathrm{t}_R \wedge \Psi_3' = \Psi_3\,[7/\ell_R]\big)$

The requested information is written onto disk i.

$\tau_{R,15}$ $\quad \vee \ \big(\epsilon = \mathbf{Wreqd!}_i(\mathrm{r}_R, \mathrm{s}_R) \wedge \ell_R = 7 \wedge C5 \wedge \Psi_3' = \Psi_3\,[9, i, \mathrm{W}^-/\ell_R, \mathrm{t}_R, \mathrm{W}]\big)$

The requested information is being written to a disk and there are no disks which haven't written them.

$\tau_{R,16}$ $\quad \vee \ \big(\epsilon = \mathbf{Wresd?}_i \wedge \ell_R = 9 \wedge i = \mathrm{t}_R \wedge \Psi_3' = \Psi_3\,[10/\ell_R]\big)$

The requested information is written onto all disks.

$\tau_{R,17}$ $\quad \vee \ \big(\epsilon = \mathbf{Wres!} \wedge \ell_R = 10 \wedge \Psi_3' = \Psi_3\,[0/\ell_R]\big)$

The error recovery layer responds with a signal to the user that requested write is performed.

$\tau_{R,0}$ $\quad \vee \ \mathbf{stut}_R$

These transitions are illustrated in figure 4.5

4. **Liveness Condition:**
The liveness condition expresses that the communication transitions are strongly fair. Let $\mathrm{SF}_R = \{\tau_{R,i} \mid i \in \{1, \ldots, 17\}\}$ then

$$\mathrm{L}_R \triangleq \bigwedge_{\tau \in \mathrm{SF}_R} (\Box\Diamond En(\tau) \rightarrow \Box\Diamond\tau)$$

4.6.3 Specification of the Detection Layer

The detection layer is nearly the same as the fail-stop detection layer the only difference is that when error due to a disk surface fault has been detected the detection layer waits for the corrective action to be undertaken, i.e., a write request of the correct data to the to be repaired logical sector. It therefore selects a spare physical sector and maps the logical sector to it. It then issues a write request to this new physical sector. The physical disk then responds to this write request. The detection layer responds that the disk has been repaired.

The detection layer is described more formally by the following specification: $\mathcal{S}_D = (B_D, \mathrm{H}_D)$ where $\mathrm{H}_D \triangleq \mathrm{I}_D \wedge \Box\mathrm{T}_D \wedge \mathrm{L}_D$ and B_D, I_D, T_D and L_D are as follows:

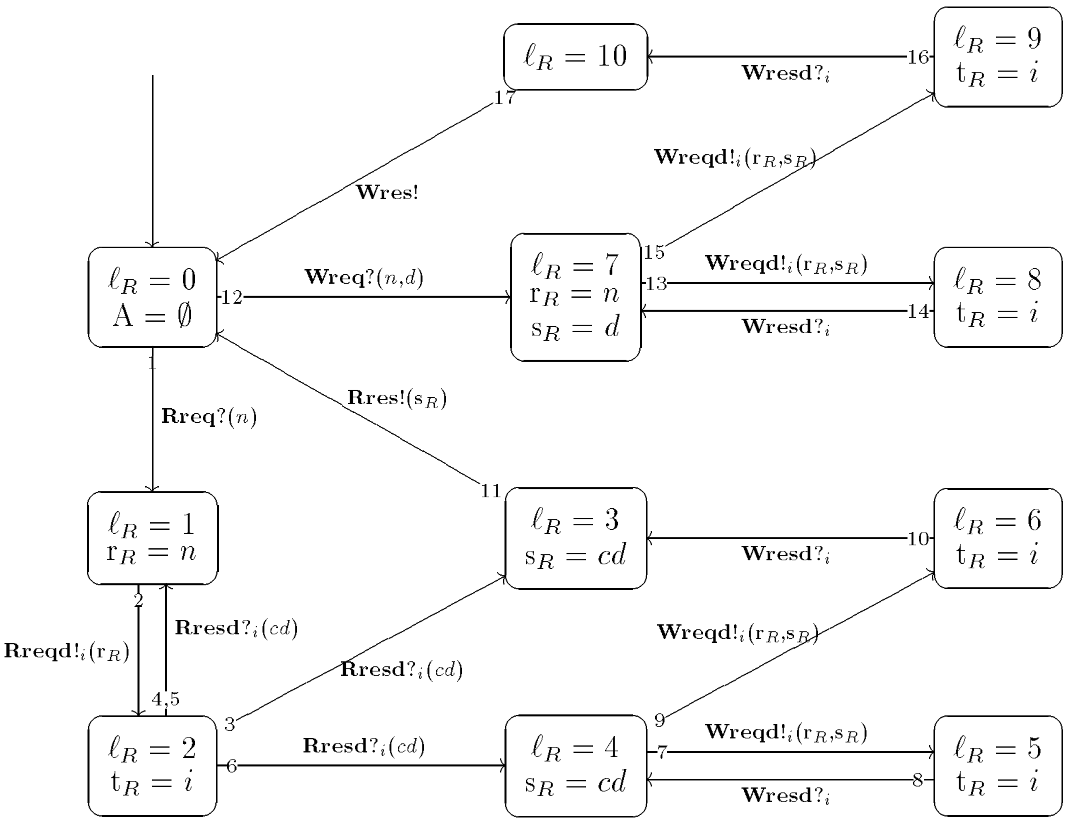

Figure 4.5: Transitions of the error recovery layer.

1. **Basis** $B_D = ((\text{In}_D, \text{Out}_D), (\text{V}_D, \text{X}_D))$

$$\begin{array}{lcl}
\text{In}_D & \triangleq & \{\mathbf{Rreqd}, \mathbf{Wreqd}, \mathbf{Rresp}, \mathbf{Wresp}\}, \\
\text{Out}_D & \triangleq & \{\mathbf{Rresd}, \mathbf{Wresd}, \mathbf{Rreqp}, \mathbf{Wreqp}\}, \\
\text{V}_D & \triangleq & \emptyset, \\
\text{X}_D & \triangleq & \{\ell_D, \text{r}_D, \text{s}_D, \text{LS}_D[i] \mid i \in LN\}
\end{array}$$

where LN is the set of logical sector numbers: $([1, .., Y])$. Let Lg be the set of data items that the user wants to store on or retrieve from the physical disk and Phy be the set information items that can be stored on or retrieved from the physical disk (Note: an item from Phy is an crc-encoded and address-encoded item of Lg.) For $n \in LN$, $c, d \in Lg$, $m \in PN$ and $cd, dd \in Phy$:

- **Rreqd**?(n): the request from the user to read logical sector n.
- **Rresd**!(c): the response of the detection layer to the previous request where c are the crc-decoded and address-decoded contents of the requested logical sector n.
- **Wreqd**?(n, d): write information item d onto logical sector n.
- **Wresd**!: response that previous write has been performed.

- **Rreqp**!(m): the request from the detection layer to read physical sector m.
- **Rresp**?(cd): the response of the physical disk to the previous request where c are the crc-encoded and address-encoded contents of requested physical.
- **Wreqp**!(m, dd): write information item dd onto physical sector m.
- **Wresp**?: response that previous write has been performed.
- ℓ_D: local variable indicating the status of the detection layer; $\ell_D = 0$: the detection layer is waiting for a request, $\ell_D = 1$: the user has issued a read request, $\ell_D = 2$: the detection layer has issued a read request, $\ell_D = 3$: the physical has responded to a read request with correct data, $\ell_D = 4$: the physical disk has responded to a read request with incorrect data, $\ell_D = 5$: the detection layer has responded to a read request with an address error message (stop status), $\ell_D = 6$: the user has issued a write request, $\ell_D = 7$: the detection layer has issued a write request, $\ell_D = 8$: the physical disk has responded to a write request, $\ell_D = 9$: the detection layer has responded to a read request with a crc error message (can be repaired), $\ell_D = 9$: the user has issued a write request in order to repair the corresponding disk.
- r_D: local variable indicating the requested sector.
- s_D: local variable indicating the requested information or the data to be written.
- $\mathrm{LS}_D[i]$: the physical sector mapped to logical sector

Let $\Psi_2 \triangleq (\ell_D, \mathrm{r}_D, \mathrm{s}_D, \mathrm{LS}_D[1], \ldots, \mathrm{LS}_D[Y])$ and
$\Psi_2' \triangleq (\ell_D', \mathrm{r}_D', \mathrm{s}_D', \mathrm{LS}_D'[1], \ldots, \mathrm{LS}_D'[Y])$.

2. **Initial states:**

$$\mathrm{I}_D \triangleq \ell_D = 0 \bigwedge_{i \in LN} \mathrm{LS}_D[i] = i$$

3. **Transitions:**
The same detection mechanism as the fail-stop detection layer is used. Let *spare* be

a function that returns a spare physical sector number. Let

Good	$\triangleq$	$CC(cd) \wedge AC(CD(cd), \mathrm{LS}_D[\mathrm{r}_D])$ data has not been affected by faults
A.er	$\triangleq$	$CC(cd) \wedge \neg AC(CD(cd), \mathrm{LS}_D[\mathrm{r}_D])$ data has been affected by a control system fault
C.er	$\triangleq$	$\neg CC(cd)$ data has been affected by a disk surface damage
c	$\triangleq$	$AD(CD(cd))$ the address- and crc-decoded contents
m	$\triangleq$	$\mathrm{LS}_D[\mathrm{r}_D]$ physical sector
dd	$\triangleq$	$CE(AE(\mathrm{r}_D, \mathrm{s}_D))$ address- and crc-encoded contents
x	$\triangleq$	*spare* spare physical sector
c_1	$\triangleq$	address error address error message
c_2	$\triangleq$	crc error crc error message

$\mathrm{T}_D \triangleq$

$\tau_{D,1}$ $\quad \Big(\epsilon = \mathbf{Rreqd}?(n) \wedge \ell_D = 0 \wedge \Psi_2' = \Psi_2\,[1, n/\ell_D, \mathrm{r}_D]\Big)$

The user requests the contents of logical sector n.

$\tau_{D,2}$ $\quad \vee\ \Big(\epsilon = \mathbf{Rreqp}!(m) \wedge \ell_D = 1 \wedge \Psi_2' = \Psi_2\,[2/\ell_D]\Big)$

The detection layer requests the to logical sector r_D mapped physical sector.

$\tau_{D,3}$ $\quad \vee\ \Big(\epsilon = \mathbf{Rresp}?(cd) \wedge \ell_D = 2 \wedge \mathit{Good} \wedge \Psi_2' = \Psi_2\,[3, c/\ell_D, \mathrm{s}_D]\Big)$

The physical disk responds with the contents of the requested sector and the detection layer detects no error in them.

$\tau_{D,4}$ $\quad \vee\ \Big(\epsilon = \mathbf{Rresp}?(cd) \wedge \ell_D = 2 \wedge A.er \wedge \Psi_2' = \Psi_2\,[4, c_1/\ell_D, \mathrm{s}_D]\Big)$

The physical disk responds with the contents of the requested sector and the detection layer detects an control system error.

$\tau_{D,5}$ $\quad \vee\ \Big(\epsilon = \mathbf{Rresp}?(cd) \wedge \ell_D = 2 \wedge C.er \wedge \Psi_2' = \Psi_2\,[4, c_2/\ell_D, \mathrm{s}_D]\Big)$

The physical disk responds with the contents of the requested sector and the detection layer detects an disk surface damage error.

$\tau_{D,6}$ $\quad \vee\ \Big(\epsilon = \mathbf{Rresd}!(\mathrm{s}_D) \wedge \ell_D = 3 \wedge \Psi_2' = \Psi_2\,[0/\ell_D]\Big)$

The detection layer responds with the contents of the user requested sector.

$\tau_{D,7}$ $\quad \vee\ \Big(\epsilon = \mathbf{Rresd}!(\mathrm{s}_D) \wedge \ell_D = 4 \wedge \mathrm{s}_D = c_1 \wedge \Psi_2' = \Psi_2\,[5/\ell_D]\Big)$

In case of an address error the detection layer responds with the corresponding error message and then stops.

$\tau_{D,8}$ $\vee$ $\left(\epsilon = \mathbf{Rresd!}(\mathrm{s}_D) \wedge \ell_D = 4 \wedge \mathrm{s}_D = c_2 \wedge \Psi_2' = \Psi_2\,[9/\ell_D]\right)$
The detection layer responds with an error message and waits for the corrective action.

$\tau_{D,9}$ $\vee$ $\left(\epsilon = \mathbf{Wreqd?}(n,d) \wedge \ell_D = 9 \wedge \Psi_2' = \Psi_2\,[10, n, d, x/\ell_D, \mathrm{r}_D, \mathrm{s}_D, \mathrm{LS}_D[n]]\right)$
The user requests that d should be written on a spare physical sector.

$\tau_{D,10}$ $\vee$ $\left(\epsilon = \mathbf{Wreqp!}(m,dd) \wedge \ell_D = 10 \wedge \Psi_2' = \Psi_2\,[7/\ell_D]\right)$
The detection layer requests that dd should be written onto physical sector m.

$\tau_{D,11}$ $\vee$ $\left(\epsilon = \mathbf{Wreqd?}(n,d) \wedge \ell_D = 0 \wedge \Psi_2' = \Psi_2\,[6, n, d/\ell_D, \mathrm{r}_D, \mathrm{s}_D]\right)$
The user requests that d should be written onto logical sector n.

$\tau_{D,12}$ $\vee$ $\left(\epsilon = \mathbf{Wreqp!}(m,dd) \wedge \ell_D = 6 \wedge \Psi_2' = \Psi_2\,[7/\ell_D]\right)$
The detection requests that dd should be written onto physical sector m.

$\tau_{D,13}$ $\vee$ $\left(\epsilon = \mathbf{Wresp!} \wedge \ell_D = 7 \wedge \Psi_2' = \Psi_2\,[8/\ell_D]\right)$
The physical disk responds with a signal to the detection layer that requested write is performed.

$\tau_{D,14}$ $\vee$ $\left(\epsilon = \mathbf{Wresd!} \wedge \ell_D = 8 \wedge \Psi_2' = \Psi_2\,[0/\ell_D]\right)$
The detection layer responds with a signal to the user that requested write is performed.

$\tau_{D,0}$ $\vee$ $\mathbf{stut}_D$

These transitions are illustrated in figure 4.6

4. **Liveness conditions:**
The liveness condition expresses that the communication transitions are strongly fair. Let $\mathrm{SF}_D = \{\tau_{D,i} \mid i \in \{1,\ldots,14\}\}$ then

$$\mathrm{L}_D \triangleq \bigwedge_{\tau \in \mathrm{SF}_D} (\Box\Diamond En(\tau) \rightarrow \Box\Diamond\tau)$$

4.6.4 Requirement W_R

The error recovery requirement should express that for all logical locations there exists at least one non-disabled disk that has correct data stored on that logical location and enough spare locations should be available on an affected disk.

$$\begin{array}{l}\mathrm{W}_R \triangleq \\ \Box(\bigwedge_{n\in LN}(\exists i \in \mathrm{G}.CC_i(\mathrm{M}_{Pi}[\mathrm{LS}_{Di}[n]]) \wedge AC_i(CD_i(\mathrm{M}_{Pi}[\mathrm{LS}_{Di}[n]], \mathrm{LS}_{Di}[n])))) \\ \Box(\forall i \in \mathrm{G}.\exists m \in PN_i.m = spare_i)\end{array}$$

This corresponds to the following machine: Let

$$\begin{array}{lcl} p_3 & \triangleq & (\bigwedge_{n\in LN}(\exists i \in \mathrm{G}.CC_i(\mathrm{M}_{Pi}[\mathrm{LS}_{Di}[n]]) \wedge AC_i(CD_i(\mathrm{M}_{Pi}[\mathrm{LS}_{Di}[n]], \mathrm{LS}_{Di}[n])))) \\ & & \wedge(\forall i \in \mathrm{G}.\exists m \in PN_i.m = spare_i) \\ p_3' & \triangleq & (\bigwedge_{n\in LN}(\exists i \in \mathrm{G}'.CC_i(\mathrm{M}'_{Pi}[\mathrm{LS}'_{Di}[n]]) \wedge AC_i(CD_i(\mathrm{M}'_{Pi}[\mathrm{LS}'_{Di}[n]], \mathrm{LS}'_{Di}[n])))) \\ & & \wedge(\forall i \in \mathrm{G}'.\exists m \in PN_i.m = spare_i) \end{array}$$

then W_R is equal to the machine $p_3 \wedge \Box((p_3 \wedge p_3') \vee stut_3)$.

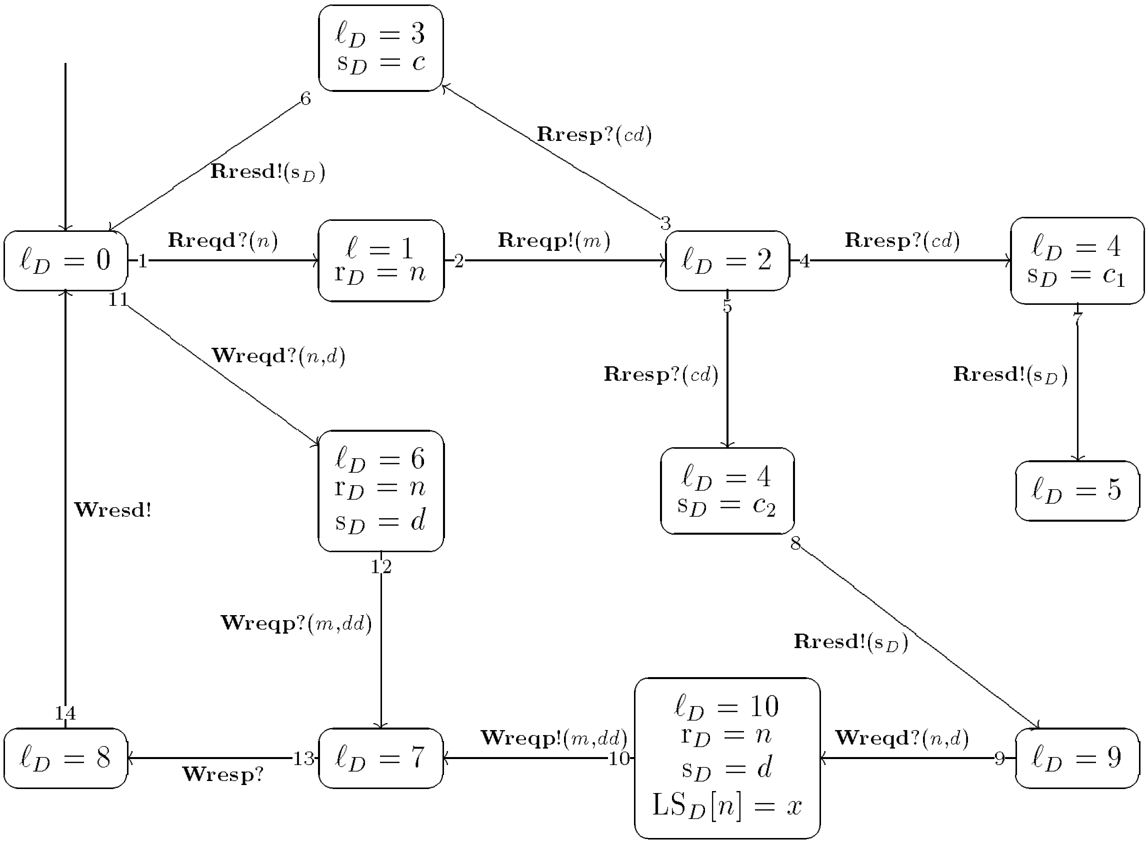

Figure 4.6: Transitions of the detection layer.

4.6.5 $\|_{i=1}^{N} (\mathcal{S}_{Di} \parallel \mathcal{S}_{Pi}) \parallel \mathcal{S}_R$ relatively refines $\mathcal{S}_{Ds} \parallel \mathcal{S}_P$

First we construct the system $\mathcal{S}_3 \triangleq \|_{i=1}^{N} (\mathcal{S}_{Di} \parallel \mathcal{S}_{Pi}) \parallel \mathcal{S}_R$ then according to theorem 8 $\mathcal{S}_3$ relatively refines $\mathcal{S}_2$ ($=\mathcal{S}_{Ds} \parallel \mathcal{S}_{P1}$) with respect to $(\mathrm{W}_R, \mathbf{true})$ iff the following holds:

$$\mathfrak{O}(B_3) = \mathfrak{O}(B_2) \text{ and}$$
$$\models (\exists \mathrm{X}_3 \,.\, (\mathrm{G}_3)) \rightarrow (\exists \mathrm{X}_2 \,.\, (\mathrm{G}_2))$$

where X_2 are the local variables from $\mathcal{S}_{Ds} \parallel \mathcal{S}_{P1}$, i.e.,
$\mathrm{X}_2 \triangleq \{\ell_{Ds}, \mathrm{r}_{Ds}, \mathrm{s}_{Ds}, \mathrm{LS}_{Ds}[i] \mid i \in LN\} \cup \{\ell_{P1}, \mathrm{r}_{P1}, \mathrm{s}_{P1}, \mathrm{M}_{P1}[n], \mathrm{F}[n] \mid n \in PN\}$ and G_2 is defined as

$$\exists \epsilon_1, \epsilon_2 . _{B_{Ds}^A} \odot_{B_{P1}^A} (\epsilon, \epsilon_1, \epsilon_2) \wedge (\mathrm{H}_{Ds} \wedge \mathrm{W}_{Ds})\,[\epsilon_1/\epsilon] \wedge (\mathrm{H}_{P1} \wedge \mathrm{W}_{P1})\,[\epsilon_2/\epsilon]$$

This can be rewritten to following machine specification of $\mathcal{S}_2$: $\mathcal{S}_2 = (B_2, \mathrm{H}_2)$ where $\mathrm{H}_2 \triangleq \mathrm{I}_2 \wedge \Box \mathrm{T}_2 \wedge \mathrm{L}_2$ and B_2, I_2, T_2 and L_2 are defined in section 4.5. X_3 are the local variables from $\mathcal{S}_3$, i.e., $\mathrm{X}_3 \triangleq (\bigcup_{j=1}^{N} \{\ell_{Dj}, \mathrm{r}_{Dj}, \mathrm{s}_{Dj}, \mathrm{LS}_{Dj}[i] \mid i \in LN\} \cup \{\ell_{Pj}, \mathrm{r}_{Pj}, \mathrm{s}_{Pj}, \mathrm{M}_{Pj}[n], \mathrm{F}_j[n] \mid n \in PN\}) \cup \{\ell_R, \mathrm{r}_R, \mathrm{s}_R, \mathrm{t}_R, \mathrm{G}, \mathrm{A}, \mathrm{W}\}$. Let $\bar{\epsilon} \triangleq \epsilon_{1,1}, \ldots, \epsilon_{1,N}, \epsilon_{2,1}, \ldots, \epsilon_{2,N}, \epsilon 3$ and let $\bar{B}^A \triangleq B_{D1}^A, \ldots, B_{DN}^A, B_{P1}^A, \ldots, B_{PN}^A, B_R^A$ then G_3 is defined as

$$(\exists \bar{e}. \odot_{\bar{B}^A} (\epsilon, \bar{e})(\textstyle\bigwedge_{j=1}^{N} (\mathrm{H}_{Dj})\,[\epsilon_{1,j}/\epsilon] \wedge (\mathrm{H}_{Pj})\,[\epsilon_{2,j}/\epsilon]) \wedge \mathrm{H}_R\,[\epsilon_3/\epsilon]) \wedge \mathrm{W}_R$$

The $(\exists \bar{e}.\ \odot_{\bar{B}^A}(\epsilon, \bar{e})(\bigwedge_{j=1}^{N}(\mathrm{H}_{Dj})\,[\epsilon_{1,j}/\epsilon] \wedge (\mathrm{H}_{Pj})\,[\epsilon_{2,j}/\epsilon]) \wedge \mathrm{H}_R\,[\epsilon_3/\epsilon])$ part can be rewritten to following machine specification $\mathcal{S}_3 \triangleq (B_3, \mathrm{H}_3)$ where $\mathrm{H}_3 \triangleq \mathrm{I}_3 \wedge \Box \mathrm{T}_3 \wedge \mathrm{L}_3$ and B_3, I_3, T_3 and L_3 are as follows:

1. **Basis** $B_3 = ((\mathrm{In}_3, \mathrm{Out}_3), (\mathrm{V}_3, \mathrm{X}_3))$

$$
\begin{array}{lcl}
\mathrm{In}_3 & \triangleq & \{\mathbf{Rreq}, \mathbf{Wreq}\} \\
\mathrm{Out}_3 & \triangleq & \{\mathbf{Rres}, \mathbf{Wres}\}, \\
\mathrm{V}_3 & \triangleq & \emptyset, \\
\mathrm{X}_3 & \triangleq & \text{as above}
\end{array}
$$

Let

$$
\begin{array}{lcl}
\Psi_3 & \triangleq & ((\ell_{Dj}, \mathrm{r}_{Dj}, \mathrm{s}_{Dj}, \mathrm{LS}_{Dj}[1], \ldots, \mathrm{LS}_{Dj}[Y], \\
 & & \ell_{Pj}, \mathrm{r}_{Pj}, \mathrm{s}_{Pj}, \mathrm{M}_{Pj}[1], \ldots, \mathrm{M}_{Pj}[Y], \mathrm{F}_j[1], \ldots, \mathrm{F}_j[Y])_{j=1,\ldots,N}, \\
 & & \ell_R, \mathrm{r}_R, \mathrm{s}_R, \mathrm{t}_R, \mathrm{G}, \mathrm{A}, \mathrm{W}) \\
\Psi_3' & \triangleq & ((\ell_{Dj}', \mathrm{r}_{Dj}', \mathrm{s}_{Dj}', \mathrm{LS}_{Dj}'[1], \ldots, \mathrm{LS}_{Dj}'[Y], \\
 & & \ell_{Pj}', \mathrm{r}_{Pj}', \mathrm{s}_{Pj}', \mathrm{M}_{Pj}'[1], \ldots, \mathrm{M}_{Pj}'[Y], \mathrm{F}_j'[1], \ldots, \mathrm{F}_j'[Y])_{j=1,\ldots,N} \\
 & & \ell_R', \mathrm{r}_R', \mathrm{s}_R', \mathrm{t}_R', \mathrm{G}', \mathrm{A}', \mathrm{W}')
\end{array}
$$

2. **Initial states:**

$$
\mathrm{I}_3 \triangleq \bigwedge_{j=1}^{N} (\mathrm{I}_{Dj} \wedge \mathrm{I}_{Pj}) \wedge \mathrm{I}_R
$$

3. **Transitions:**
Let

- $c_1 \triangleq$ address error
  address error message
- $c_2 \triangleq$ crc error
  crc error message
- $\mathit{Good}1 \triangleq i = \mathrm{t}_R \wedge dc \neq c_1 \wedge dc \neq c_2 \wedge \mathrm{A} = \emptyset$
  data is not affected by faults and the number of affected disks is zero
- $\mathit{Good}2 \triangleq i = \mathrm{t}_R \wedge dc \neq c_1 \wedge dc \neq c_2 \wedge \mathrm{A} \neq \emptyset$
  data is not affected by faults and the number of affected disks is non-zero
- $A.er \triangleq i = \mathrm{t}_R \wedge dc = c_1$
  data is affected by control system fault
- $C.er \triangleq i = \mathrm{t}_R \wedge dc = c_2$
  data is affected by disk surface damage
- $\mathrm{G}^- \triangleq \mathrm{G} \setminus \{i\}$
  set of good disks minus i

- $A^- \triangleq A \setminus \{i\}$
  set of affected disks minus i
- $A^+ \triangleq A \cup \{i\}$
  set of affected disks plus i
- $W^- \triangleq W \setminus \{i\}$
  set of to be written disks minus i
- $C1 \triangleq i \in G \wedge i \notin A$
  disk i is good and not affected
- $C2 \triangleq i \in A \wedge A^- \neq \emptyset$
  disk i is affected and the number of affected disks is greater than 1
- $C3 \triangleq i \in A \wedge A^- = \emptyset$
  disk i is the only affected disk
- $C4 \triangleq i \in W \wedge W^- \neq \emptyset$
  disk i should be written onto and the number of to be written disks is greater than 1
- $C5 \triangleq i \in W \wedge W^- = \emptyset$
  disk i is the only disk to be written onto
- $q \triangleq (\ell_{Di}, \ell_{Pi}, \ell_R)$
  status of detection layer i and physical disk i and the error recovery layer.

$T_3 \triangleq$

$\tau_{3,1}$ $\quad \Big(\epsilon = \mathbf{Rreq}?(n) \wedge \ell_R = 0 \wedge \Psi_3' = \Psi_3\,[1, n/\ell_R, \mathrm{r}_R]\Big)$

The user requests the contents of logical sector n.

$\tau_{3,2}$ $\quad \vee\ \Big(\epsilon = \mathbf{i} \wedge \ell_R = 1 \wedge C1 \wedge \Psi_3' = \Psi_3\,[2, i, 1, \mathrm{r}_R/\ell_R, \mathrm{t}_R, \ell_{Di}, \mathrm{r}_{Di}]\Big)$

The error recovery layer requests the contents of logical sector r_R from an enabled detection layer i.

$\tau_{3,3}$ $\quad \vee\ \Big(\epsilon = \mathbf{i} \wedge q = (1,0,2) \wedge \Psi_3' = \Psi_3\,[2, 1, m/\ell_{Di}, \ell_{Pi}, \mathrm{r}_{Pi}]\Big)$

The detection layer i requests the to logical sector r_{Di} mapped physical sector from physical disk i.

$\tau_{3,4}$ $\quad \vee\ \Big(\epsilon = \mathbf{i} \wedge q = (2,1,2) \wedge Good_i \wedge \Psi_3' = \Psi_3\,[3, c, 0/\ell_{Di}, \mathrm{s}_{Di}, \ell_{Pi}]\Big)$

The physical disk i responds with the contents of the requested sector and the detection layer i detects no error in them.

$\tau_{3,5}$ $\quad \vee\ \Big(\epsilon = \mathbf{i} \wedge q = (2,1,2) \wedge A.er_i \wedge \Psi_3' = \Psi_3\,[4, c_1, 0/\ell_{Di}, \mathrm{s}_{Di}, \ell_{Pi}]\Big)$

The physical disk i responds with the contents of the requested sector and the detection layer i detects a control system error.

$\tau_{3,6}$ $\quad \vee\ \Big(\epsilon = \mathbf{i} \wedge q = (2,1,2) \wedge C.er_i \wedge \Psi_2' = \Psi_2\,[4, c_2, 0/\ell_{Di}, \mathrm{s}_{Di}, \ell_{Pi}]\Big)$

The physical disk i responds with the contents of the requested sector and the detection layer i detects a disk surface damage error.

$\tau_{3,7}$ $\quad \vee \ \big(\epsilon = \mathbf{i} \wedge q = (3,0,2) \wedge \mathit{Good}1 \wedge \Psi_3' = \Psi_3\,[0,3,\mathrm{s}_{Di}/\ell_{Di},\ell_R,\mathrm{s}_R]\big)$

The detection layer i responds with the contents of the requested sector and the detection layer i has detected no error in them.

$\tau_{3,8}$ $\quad \vee \ \big(\epsilon = \mathbf{i} \wedge q = (4,0,2) \wedge A.er_i \wedge \Psi_3' = \Psi_3\,[5,1,\mathrm{G}^-/\ell_{Di},\ell_R,\mathrm{G}]\big)$

The detection layer i responds with the contents of the requested sector and the detection layer i has detected an control system error, so this detection layer will be disabled.

$\tau_{3,9}$ $\quad \vee \ \big(\epsilon = \mathbf{i} \wedge q = (4,0,2) \wedge C.er_i \wedge \Psi_3' = \Psi_3\,[9,1,\mathrm{A}^+/\ell_{Di},\ell_R,\mathrm{A}]\big)$

The detection layer i responds with the contents of the requested sector and the detection layer i detects an disk surface damage error, so physical disk i has to be repaired.

$\tau_{3,10}$ $\quad \vee \ \big(\epsilon = \mathbf{i} \wedge q = (3,0,2) \wedge \mathit{Good}2 \wedge \Psi_3' = \Psi_3\,[0,4,\mathrm{s}_{Di}/\ell_{Di},\ell_R,\mathrm{s}_R]\big)$

A correct disk i has been found so the error recovery layer can repair the affected disks.

$\tau_{3,11}$ $\quad \vee \ (\epsilon = \mathbf{i} \wedge q = (9,0,4) \wedge C2$
$\quad\quad \wedge \Psi_3' = \Psi_3\,[10,\mathrm{r}_R,\mathrm{s}_R,x_i,5,i,\mathrm{A}^-/\ell_{Di},\mathrm{r}_{Di},\mathrm{s}_{Di},\mathrm{LS}_{Di},\ell_R,\mathrm{t}_R,\mathrm{A}])$

An affected disk i is being repaired and there are still unrepaired disk.

$\tau_{3,12}$ $\quad \vee \ \big(\epsilon = \mathbf{i} \wedge q = (10,0,5) \wedge \Psi_3' = \Psi_3\,[7,2,m_i,dd_i/\ell_{Di},\ell_{Pi},\mathrm{r}_{Pi},\mathrm{s}_{Pi}]\big)$

An affected disk i is being repaired and there are still unrepaired disk.

$\tau_{3,13}$ $\quad \vee \ \big(\epsilon = \mathbf{i} \wedge q = (7,2,5) \wedge \Psi_3' = \Psi_3\,[8,0,\mathrm{s}_{Pi}/\ell_{Di},\ell_{Pi},\mathrm{M}_{Pi}[\mathrm{F}_{Pi}[\mathrm{r}_{Pi}]]]\big)$

An affected disk i is being repaired and there are still unrepaired disk.

$\tau_{3,14}$ $\quad \vee \ \big(\epsilon = \mathbf{i} \wedge q = (8,0,5) \wedge i = \mathrm{t}_R \wedge \Psi_3' = \Psi_3\,[0,4/\ell_{Di},\ell_R]\big)$

The affected disk is repaired.

$\tau_{3,15}$ $\quad \vee \ (\epsilon = \mathbf{i} \wedge q = (9,0,4) \wedge C3$
$\quad\quad \wedge \Psi_3' = \Psi_3\,[10,6,\mathrm{r}_R,\mathrm{s}_R,x_i,\mathrm{A}^-/\ell_{Di},\mathrm{r}_{Di},\mathrm{s}_{Di},\mathrm{LS}_{Di},\ell_R,\mathrm{A}])$

An affected disk is being repaired and there are no further unrepaired disks.

$\tau_{3,16}$ $\quad \vee \ \big(\epsilon = \mathbf{i} \wedge q = (10,0,6) \wedge \Psi_3' = \Psi_3\,[7,2,m_i,dd_i/\ell_{Di},\ell_{Pi},\mathrm{r}_{Pi},\mathrm{s}_{Pi}]\big)$

An affected disk i is being repaired and there are no further unrepaired disks.

$\tau_{3,17}$ $\quad \vee \ \big(\epsilon = \mathbf{i} \wedge q = (7,2,6) \wedge \Psi_3' = \Psi_3\,[8,0,\mathrm{s}_{Pi}/\ell_{Di},\ell_{Pi},\mathrm{M}_{Pi}[\mathrm{F}_{Pi}[\mathrm{r}_{Pi}]]]\big)$

An affected disk i is being repaired and there are no further unrepaired disks.

$\tau_{3,18}$ $\quad \vee \ \big(\epsilon = \mathbf{i} \wedge q = (8,0,6) \wedge i = \mathrm{t}_R \wedge \Psi_3' = \Psi_3\,[0,3/\ell_{Di},\ell_R]\big)$

All affected disk are repaired, so the user requested contents can be sent.

$\tau_{3,19}$ $\quad \vee \ \big(\epsilon = \mathbf{Rres!}(\mathrm{s}_R) \wedge \ell_R = 3 \wedge \Psi_3' = \Psi_3\,[0/\ell_R]\big)$

The error recovery layer responds with the requested contents.

$\tau_{3,20}$ $\quad \vee \ \big(\epsilon = \mathbf{Wreq}?(n,d) \wedge \ell_R = 0 \wedge \Psi_3' = \Psi_3\,[7,n,d,\mathrm{G}/\ell_R,\mathrm{r}_R,\mathrm{s}_R,\mathrm{W}]\big)$

The user requests that d should be written onto logical sector n.

$\tau_{3,21}$ $\quad \vee \ (\epsilon = \mathbf{i} \wedge q = (0,0,7) \wedge C4$
$\quad\quad \wedge \Psi_3' = \Psi_3\,[8,6,\mathrm{r}_R,\mathrm{s}_R,i,\mathrm{W}^-/\ell_R,\ell_{Di},\mathrm{r}_{Di},\mathrm{s}_{di},\mathrm{t}_R,\mathrm{W}])$

The requested information is being written to a disk and there are still unwritten disks.

$\tau_{3,22}$ $\quad \vee \ \big(\epsilon = \mathbf{i} \wedge q = (6,0,8) \wedge \Psi_3' = \Psi_3\,[7, 2, m_i, dd_i/\ell_{Di}, \ell_{Pi}, \mathrm{r}_{Pi}, \mathrm{s}_{Pi}]\big)$

The requested information is being written to a disk and there are still unwritten disks.

$\tau_{3,23}$ $\quad \vee \ \big(\epsilon = \mathbf{i} \wedge q = (7,2,8) \wedge \Psi_3' = \Psi_3\,[8, 0, \mathrm{s}_{Pi}/\ell_{Di}, \ell_{Pi}, \mathrm{M}_{Pi}[\mathrm{F}_{Pi}[\mathrm{r}_{Pi}]]]\big)$

The requested information is being written to a disk and there are still unwritten disks.

$\tau_{3,24}$ $\quad \vee \ \big(\epsilon = \mathbf{i} \wedge q = (8,0,8) \wedge i = \mathrm{t}_R \wedge \Psi_3' = \Psi_3\,[0, 7/\ell_{Di}, \ell_R]\big)$

The requested information is written onto disk i.

$\tau_{3,25}$ $\quad \vee \ (\epsilon = \mathbf{i} \wedge q = (0,0,7) \wedge C5$
$\quad\quad \wedge \Psi_3' = \Psi_3\,[9, 6, \mathrm{r}_R, \mathrm{s}_R, i, \mathrm{W}^-/\ell_R, \ell_{Di}, \mathrm{r}_{Di}, \mathrm{s}_{Di}, \mathrm{t}_R, \mathrm{W}])$

The requested information is being written to a disk and there are no further unwritten disks.

$\tau_{3,26}$ $\quad \vee \ \big(\epsilon = \mathbf{i} \wedge q = (6,0,9) \wedge \Psi_3' = \Psi_3\,[7, 2, m_i, dd_i/\ell_{Di}, \ell_{Pi}, \mathrm{r}_{Pi}, \mathrm{s}_{Pi}]\big)$

The requested information is being written to a disk and there are no further unwritten disks.

$\tau_{3,27}$ $\quad \vee \ \big(\epsilon = \mathbf{i} \wedge q = (7,2,9) \wedge \Psi_3' = \Psi_3\,[8, 0, \mathrm{s}_{Pi}/\ell_{Di}, \ell_{Pi}, \mathrm{M}_{Pi}[\mathrm{F}_{Pi}[\mathrm{r}_{Pi}]]]\big)$

The requested information is being written to a disk and there are no further unwritten disks.

$\tau_{3,28}$ $\quad \vee \ \big(\epsilon = \mathbf{i} \wedge q = (8,0,9) \wedge i = \mathrm{t}_R \wedge \Psi_3' = \Psi_3\,[0, 10/\ell_{Di}, \ell_R]\big)$

The requested information is written onto all disks.

$\tau_{3,29}$ $\quad \vee \ \big(\epsilon = \mathbf{Wres!} \wedge \ell_R = 10 \wedge \Psi_3' = \Psi_3\,[0/\ell_R]\big)$

The error recovery layer responds with a signal to the user that requested write is performed.

$\tau_{3,0}$ $\quad \vee \ \mathbf{stut}_3$

These transitions are illustrated in figure 4.7 with the transitions for the physical disk omitted.

4. **Liveness Condition:**
   The liveness condition expresses that all non-stuttering transitions are strongly fair. Let $\mathrm{SF}_3 = \{\tau_{3,i} \mid i \in \{1, \ldots, 29\}\}$ then

$$\mathrm{L}_3 \triangleq \bigwedge_{\tau \in \mathrm{SF}_3} (\Box\Diamond En(\tau) \rightarrow \Box\Diamond\tau)$$

Rule 3 will be used to prove

$$\models (\exists \mathrm{X}_3 \,.\, (\mathrm{G}_3)) \rightarrow (\exists \mathrm{X}_2 \,.\, (\mathrm{G}_2))\,.$$

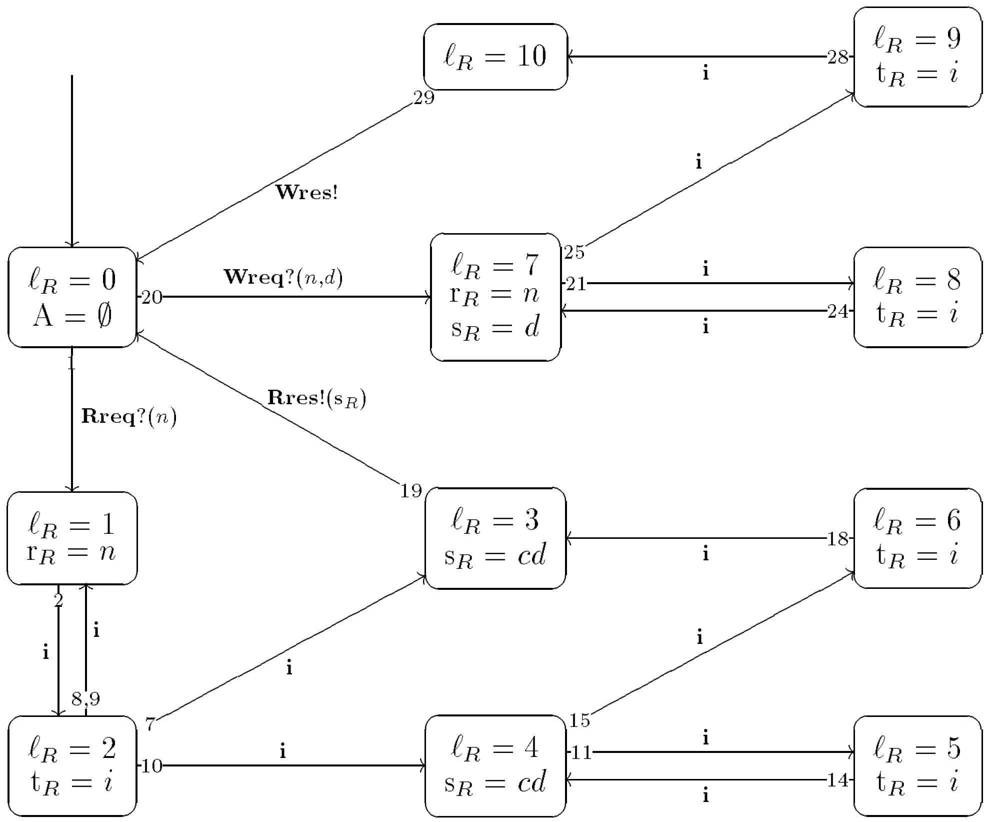

Figure 4.7: Transitions of the final implementation of stable storage.

This means one has to prove (a), (b) and (c) below, for $\bar{f}$ the refinement mapping from $\mathcal{S}_3$ to $\mathcal{S}_2$, defined as: $\bar{f} = f_{\ell_{D_s}}, f_{\mathrm{r}_{D_s}}, f_{\mathrm{s}_{D_s}}, f_{\mathrm{LS}_{D_s}[m]}, \ldots, f_{\mathrm{LS}_{D_s}[Y]}, f_{\ell_{P1}}, f_{\mathrm{r}_{P1}}, f_{\mathrm{s}_{P1}}, f_{\mathrm{M}_{P1}[n]}, f_{\mathrm{F}_{P1}[n]}$ ($n \in SN$, $m \in LN$). The refinement mappings are defined as:

$$
\begin{array}{llll}
f_{\ell_{P1}} & & & \\
if & \ell_R = 0 & then & \ell_R \\
 & \ell_R = 1 & then & \ell_R - 1 \\
 & \ell_R = 2 \wedge \ell_{Pi} = 0 & then & \ell_R - 2 \\
 & \ell_R = 2 \wedge \ell_{Pi} = 1 & then & \ell_R - 1 \\
 & \ell_R = 3 & then & \ell_R - 3 \\
 & \ell_R = 4 & then & \ell_R - 4 \\
 & \ell_R = 5 & then & \ell_R - 5 \\
 & \ell_R = 6 & then & \ell_R - 6 \\
 & \ell_R = 7 & then & \ell_R - 7 \\
 & \ell_R = 8 \wedge \ell_{Pi} = 0 & then & \ell_R - 8 \\
 & \ell_R = 8 \wedge \ell_{Pi} = 2 & then & \ell_R - 6 \\
 & \ell_R = 9 \wedge \ell_{Pi} = 0 & then & \ell_R - 9 \\
 & \ell_R = 9 \wedge \ell_{Pi} = 2 & then & \ell_R - 7 \\
 & \ell_R = 10 & then & \ell_R - 10
\end{array}
$$

$$
\begin{array}{llll}
f_{loc\ell_{Ds}} & & & \\
if & \ell_R = 0 & then & \ell_R \\
 & \ell_R = 1 & then & \ell_R \\
 & \ell_R = 2 \wedge \ell_{Pi} = 0 & then & \ell_R - 1 \\
 & \ell_R = 2 \wedge \ell_{Pi} = 1 & then & \ell_R - 1 \\
 & \ell_R = 3 & then & \ell_R \\
 & \ell_R = 4 & then & \ell_R - 2 \\
 & \ell_R = 5 & then & \ell_R - 3 \\
 & \ell_R = 6 & then & \ell_R - 4 \\
 & \ell_R = 7 & then & \ell_R - 1 \\
 & \ell_R = 8 & then & \ell_R - 1 \\
 & \ell_R = 9 & then & \ell_R - 2 \\
 & \ell_R = 10 & then & \ell_R - 2
\end{array}
$$

For $i \in \mathrm{G} \wedge i \notin \mathrm{A}$ (physical i is not affected by any fault)

$$
\begin{array}{lcl}
f_{\mathrm{r}_{P1}} & \triangleq & \mathrm{r}_{Pi} \\
f_{\mathrm{s}_{P1}} & \triangleq & \mathrm{s}_{Pi} \\
f_{\mathrm{M}_{P1}[n]} & \triangleq & \mathrm{M}_{Pi}[n] \\
f_{\mathrm{F}_{P1}[n]} & \triangleq & \mathrm{F}_{Pi}[n] \\
f_{\mathrm{r}_{Ds}} & \triangleq & \mathrm{r}_{Di} \\
f_{\mathrm{s}_{Ds}} & \triangleq & \mathrm{s}_{Di} \\
f_{\mathrm{LS}_{Ds}[m]} & \triangleq & \mathrm{LS}_{Di}[m]
\end{array}
$$

$$
\begin{array}{ll}
(a) & \mathcal{S}_3 \cap Hist(\mathrm{W}_R) \models (\mathrm{I}_3 \wedge p_3) \rightarrow (\mathrm{I}_2)\left[\bar{f}/\mathrm{X}_2\right] \\
(b) & \mathcal{S}_3 \cap Hist(\mathrm{W}_R) \models (\mathrm{T}_3 \wedge ((p_3 \wedge p_3') \vee \mathbf{stut}_3) \rightarrow (\mathrm{T}_2)\left[\bar{f}/\mathrm{X}_2\right] \\
(c) & \mathcal{S}_3 \cap Hist(\mathrm{W}_R) \models \mathrm{L}_2\left[\bar{f}/\mathrm{X}_2\right]
\end{array}
$$

(a) **Proof 13**

$$
\begin{array}{ll}
 & \mathrm{I}_3 \wedge p_3 \\
\rightarrow & \quad \%\ \ Def.\ \mathrm{I}_3, p_3, \bar{f}, \mathrm{I}_2 \\
 & (\mathrm{I}_2)\left[\bar{f}/\mathrm{X}_2\right]
\end{array}
$$

(b) **Proof 14**

Since T_3 *is of the form* $\mathbf{stut}_3 \vee \bigvee_\tau(\epsilon = \mathbf{a}_\tau \wedge trans_\tau)$ *then* $\mathrm{T}_3 \wedge ((p_3 \wedge p_3') \vee \mathbf{stut}_3)$ *is equal to* $\mathbf{stut}_3 \vee \bigvee_\tau(\epsilon = \mathbf{a}_\tau \wedge trans_\tau \wedge p_3 \wedge p_3')$.

– $\tau_{3,1} \wedge p_3 \wedge p_3'$

$\rightarrow \ (\tau_{2,1})\left[\bar{f}/\mathrm{X}_2\right]$

The user read request at the third level corresponds to the user read request at the second level.

- $$\begin{aligned} & \tau_{3,2} \wedge p_3 \wedge p'_3 \\ \rightarrow\ & \mathbf{stut}_2 \left[\bar{f}/\mathrm{X}_2\right] \end{aligned}$$
  The read request to the detection layer i at the third level corresponds to the stutter step at the second level.
- $$\begin{aligned} & \tau_{3,3} \wedge p_3 \wedge p'_3 \\ \rightarrow\ & (\tau_{2,2}) \left[\bar{f}/\mathrm{X}_2\right] \end{aligned}$$
  The read request to physical disk i at the third level corresponds to the read request to the physical disk at the second level.
- $$\begin{aligned} & \tau_{3,4} \wedge p_3 \wedge p'_3 \\ \rightarrow\ & (\tau_{2,3}) \left[\bar{f}/\mathrm{X}_2\right] \end{aligned}$$
  The read response of the physical disk i at the third level corresponds to the read response of the physical disk at the second level because no errors are detected.
- $$\begin{aligned} & \tau_{3,5} \wedge p_3 \wedge p'_3 \\ \rightarrow\ & \mathbf{stut}_2 \left[\bar{f}/\mathrm{X}_2\right] \end{aligned}$$
  The read response of the physical disk i at the third level corresponds to the stutter step at the second level because a control system error is detected.
- $$\begin{aligned} & \tau_{3,6} \wedge p_3 \wedge p'_3 \\ \rightarrow\ & \mathbf{stut}_2 \left[\bar{f}/\mathrm{X}_2\right] \end{aligned}$$
  The read response of the physical disk i at the third level corresponds to the stutter step at the second level because a disk surface error is detected.
- $$\begin{aligned} & \tau_{3,7} \wedge p_3 \wedge p'_3 \\ \rightarrow\ & \mathbf{stut}_2 \left[\bar{f}/\mathrm{X}_2\right] \end{aligned}$$
  The read response of the detection i at the third level corresponds to the stutter step at the second level.
- $$\begin{aligned} & \tau_{3,8} \wedge p_3 \wedge p'_3 \\ \rightarrow\ & \mathbf{stut}_2 \left[\bar{f}/\mathrm{X}_2\right] \end{aligned}$$
  The read response of the detection i at the third level corresponds to the stutter step at the second level.
- $$\begin{aligned} & \tau_{3,9} \wedge p_3 \wedge p'_3 \\ \rightarrow\ & \mathbf{stut}_2 \left[\bar{f}/\mathrm{X}_2\right] \end{aligned}$$
  The read response of the detection i at the third level corresponds to the stutter step at the second level.
- $$\begin{aligned} & \tau_{3,10} \wedge p_3 \wedge p'_3 \\ \rightarrow\ & \mathbf{stut}_2 \left[\bar{f}/\mathrm{X}_2\right] \end{aligned}$$
  The read response of the detection i at the third level corresponds to the stutter step at the second level.
- *For* $j = 11, \ldots, 18$
  $$\begin{aligned} & \tau_{3,j} \wedge p_3 \wedge p'_3 \\ \rightarrow\ & \mathbf{stut}_2 \left[\bar{f}/\mathrm{X}_2\right] \end{aligned}$$

The correction step at the third level corresponds to the stutter step at the second level.

– $$\begin{aligned} & \tau_{3,19} \wedge p_3 \wedge p_3' \\ \to \ & (\tau_{2,4}) \left[\bar{f}/\mathrm{X}_2\right] \end{aligned}$$

The read response to the user at the third level corresponds to read response to the user at the second level.

– $$\begin{aligned} & \tau_{3,20} \wedge p_3 \wedge p_3' \\ \to \ & (\tau_{2,4}) \left[\bar{f}/\mathrm{X}_2\right] \end{aligned}$$

The write request of the user at the third level corresponds to the write request of the user at the second level.

– *For* $j = 21, 25$

$$\begin{aligned} & \tau_{3,j} \wedge p_3 \wedge p_3' \\ \to \ & \mathbf{stut}_2 \left[\bar{f}/\mathrm{X}_2\right] \end{aligned}$$

The write request to the detection layer i at the third level corresponds to the stutter step at the second level.

– *For* $j = 22, 26$

$$\begin{aligned} & \tau_{3,j} \wedge p_3 \wedge p_3' \\ \to \ & (\tau_{2,6}) \left[\bar{f}/\mathrm{X}_2\right] \end{aligned}$$

The write request to the physical disk i at the third level corresponds to the write request to the physical disk at the second level.

– *For* $j = 23, 27$

$$\begin{aligned} & \tau_{3,j} \wedge p_3 \wedge p_3' \\ \to \ & (\tau_{2,7}) \left[\bar{f}/\mathrm{X}_2\right] \end{aligned}$$

The write response of the physical disk i at the third level corresponds to the write response of the physical disk at the second level.

– *For* $j = 24, 28$

$$\begin{aligned} & \tau_{3,j} \wedge p_3 \wedge p_3' \\ \to \ & \mathbf{stut}_2 \left[\bar{f}/\mathrm{X}_2\right] \end{aligned}$$

The write response of the detection layer i at the third level corresponds to the stutter step at the second level.

– $$\begin{aligned} & \tau_{3,29} \wedge p_3 \wedge p_3' \\ \to \ & (\tau_{2,8}) \left[\bar{f}/\mathrm{X}_2\right] \end{aligned}$$

The write response to the user at the third level corresponds to the write response to the user at the second level.

– $$\mathbf{stut}_3 \to \mathbf{stut}_2 \left[\bar{f}/\mathrm{X}_2\right]$$

(c) Let $\mathrm{SF}_3 = \{\tau_{3,i} \mid i \in \{1, \ldots, 29\}\}$ then

$$\mathrm{L}_3 \triangleq \bigwedge_{\tau \in \mathrm{SF}_3} (\Box\Diamond En(\tau) \rightarrow \Box\Diamond\tau)$$

. Let $\mathrm{SF}_2 = \{\tau_{2,i} \mid i \in \{1, \ldots, 8\}\}$ then

$$\mathrm{L}_2 \triangleq \bigwedge_{\tau \in \mathrm{SF}_2} (\Box\Diamond En(\tau) \rightarrow \Box\Diamond\tau).$$

Then the following holds

$$\mathcal{S}_3 \cap Hist(\mathrm{W}_3) \models \mathrm{L}_3 \rightarrow \mathrm{L}_2 \left[\bar{f}/\mathrm{X}_3\right]$$

So

$$\mathcal{S}_3 \cap Hist(\mathrm{W}_3) \models \mathrm{L}_2 \left[\bar{f}/\mathrm{X}_2\right]$$

holds.

Bibliography

[Acz83] P. Aczel. On an inference rule for parallel composition, 1983. Unpublished, University of Manchester.

[AFK88] K. R. Apt, N. Francez, and S. Katz. Appraising fairness in languages for distributed programming. *Distributed Computing*, 2(4):226–241, 1988.

[AL91] M. Abadi and L. Lamport. The existence of refinement mappings. *Theoretical Computer Science*, 82(2):253–284, May 1991.

[AL93a] M. Abadi and L. Lamport. Composing specifications. *ACM Transactions on Programming Languages and Systems*, 15(1):73–132, 1993.

[AL93b] M. Abadi and L. Lamport. Conjoining specifications. Technical Report 118, Digital Systems Research Center, 1993.

[AS85] B. Alpern and F.B. Schneider. Defining liveness. *Information Processing Letters*, 21(4):181–185, 1985.

[AS87] B. Alpern and F. Schneider. Proving boolean combinations of deterministic properties. In *Proceedings of the second symposium on logic in computer science*, pages 131–137. IEEE, June 1987.

[BKP86] H. Barringer, R. Kuiper, and A. Pnueli. A really abstract concurrent model and its temporal semantics. In *Proc. 13th ACM Symp. Princ. of Prog. Lang.*, pages 173–183, 1986.

[Bur82] J.P. Burgess. Axioms for tense logic, i. "since" and "until". *Notre Dame Jornal of Formal Logic*, 23(4):367–374, October 1982.

[Bur84] J.P. Burgess. Basic tense logic. In D. Gabbay and F. Guenthner, editors, *Handbook of Philosophical Logic.*, volume II, pages 89–133. Reidel Publishers, 1984.

[CC94] A. Cau and P. Collette. Parallel composition of assumption-commitment specifications: a unifying approach for shared variable and distributed message passing concurrency. To appear in Acta Informatica, 1994.

[CdR93a] A. Cau and W.-P. de Roever. Specifying fault tolerance within stark's formalism. In *Proc. of the Twenty-Third International Symposium on Fault-Tolerant Computing*, pages 392–401. IEEE, 1993.

[CdR93b] A. Cau and W.-P. de Roever. Using relative refinement for fault tolerance. In *Proceedings of FME'93 symposium: industrial strength formal methods*, 1993.

[CKdR92] A. Cau, R. Kuiper, and W.-P. de Roever. Formalising Dijkstra's development strategy within Stark's formalism. In C. B. Jones, R. C. Shaw, and T. Denvir, editors, *Proc. 5th. BCS-FACS Refinement Workshop*, 1992.

[Cri85] F. Cristian. A rigorous approach to fault-tolerant programming. *IEEE Transactions on Software Engineering*, 11(1):23–31, 1985.

[Dij79] E.W. Dijkstra. A tutorial on the split binary semaphore, 1979. EWD 703.

[DK90] E. Diepstraten and R. Kuiper. Abadi & Lamport and Stark: towards a proof theory for stuttering, dense domains and refinements mappings. In *LNCS 430:Proc. of the REX Workshop on Stepwise Refinement of Distributed Systems, Models, Formalisms, Correctness*, pages 208–238. Springer-Verlag, 1990.

[Hoa84] C.A.R. Hoare. *Communicating Sequential Processes.* Prentice-Hall, London, 1984.

[Jon83] C.B. Jones. Tentative steps towards a development method for interfering programs. *ACM Transactions on Programming Languages and Systems*, 5(4):596–619, 1983.

[KMP93] Y. Kesten, Z. Manna, and A. Pnueli. Temporal verification of simulation and refinement. In J.W. de Bakker, W.-P. de Roever, and G. Rozenberg, editors, *LNCS 803: A Decade of Concurrency, Reflections and Perspectives*, pages 273–346. Springer-Verlag, 1993.

[LA90] P.A. Lee and T. Anderson. *Fault Tolerance Principles and Practice*, volume 3 of *Dependable Computing and Fault-Tolerant Systems.* Springer-Verlag, second, revised edition, 1990.

[Lam] L. Lamport. TLA - Temporal Logic of Actions. The hypertext page on TLA: www.research.digital.com/ SRC/ personal/ Leslie_Lamport/ tla/ tla.html.

[Lam83] L. Lamport. What good is temporal logic. In R.E.A. Manson, editor, *Information Processing 83: Proc. of the IFIP 9th World Congress*, pages 657–668. Elsevier Science Publishers, North Holland, 1983.

[Lam89] L. Lamport. A simple approach to specifying concurrent systems. *Communications of the ACM*, 32(1):32–45, January 1989.

[Lam91] L. Lamport. The temporal logic of actions. Technical Report 79, Digital Systems Research Center, 1991.

[Lam94] L. Lamport. The temporal logic of actions. To appear in ACM TOPLAS, July? 1994.

[LGdR79] S. Lee, S. Gerhart, and W.-P. de Roever. The evolution of list-copying algorithms and the need for structured program verification. In *Proc. of 6th POPL*, 1979.

[MC81] J. Misra and K.M. Chandy. Proofs of networks of processes. *IEEE Transactions on Software Engineering*, 7(4):417–426, July 1981.

[MP89] Z. Manna and A. Pnueli. An exercise in the verification of multi-process programs. Technical report, Stanford University, 1989.

[PJ91] P.K. Pandya and M. Joseph. P–a logic - a compositional proof system for distributed programs. *Distributed Computing*, 5:37–54, 1991.

[Pnu85] A. Pnueli. In transition from global to modular temporal reasoning about programs. In *NATO ASI Series F 13: Logics and models of concurrent systems*, pages 123–144. Springer-Verlag, 1985.

[PWT90] P.R.H. Place, W.G. Wood, and M. Tudball. Survey of formal specification techniques for reactive systems. Technical Report, 1990.

[Sch91] H. Schepers. Terminology and Paradigms for Fault Tolerance. Computing Science Notes 91/08 of the Department of Mathematics and Computing Science Eindhoven University of Technology, 1991.

[Sta84] E.W. Stark. *Foundations of a Theory of Specification for Distributed Systems.* PhD thesis, Massachusetts Inst. of Technology, 1984. Available as Report No. MIT/LCS/TR-342.

[Sta85] E.W. Stark. A Proof Technique for Rely/Guarantee Properties. In *LNCS 206: Fifth Conference on Foundations of Software Technology and Theoretical Computer Science*, pages 369–391. Springer-Verlag, 1985.

[Sta88] E.W. Stark. Proving entailment between conceptual state specifications. *Theoretical Computer Science*, 56:135–154, 1988.

[Sti88] C. Stirling. A generalization of owicki-gries hoare logic for a concurrent while language. *Theoretical Computer Science*, 58:347–359, 1988.

[Stø91] K. Stølen. A method for the development of totally correct shared-state parallel programs. In J.C.M. Baeten and J.F. Groote, editors, *LNCS 527: Proceedings of Concur '91*, pages 510–525. Springer-Verlag, 1991.

[WD88] J.C.P. Woodcock and B. Dickinson. Using vdm with rely and guarantee-conditions. In R. Bloomfield, L. Marshall, and R. Jones, editors, *LNCS 328: Proceedings of VDM '88, The Way Ahead*, pages 434–458. Springer-Verlag, 1988.

[Wri87] M. Wriedt. Allgemeine Topologie I. Technical report, Christian-Albrechts-Universität zu Kiel, 1987. Vorlesungsskript ausgearbeitet von M. Jäger.

[XCC94] Q. Xu, A. Cau, and P. Collette. On unifying assumption–commitment style proof rules for concurrency. In B. Jonsson and J. Parrow, editors, *LNCS 836: CONCUR'94: Concurrency Theory*, pages 267–282. Springer-Verlag, 1994.

[ZCdR92] J. Zwiers, J. Coenen, and W.-P. de Roever. A note on compositional refinemnt. In C. B. Jones, R. C. Shaw, and T. Denvir, editors, *5th Refinement Workshop*, Workshops in Computing, pages 342–366, London, January 1992. BCS-FACS, Springer Verlag.

[ZdBdR84] J. Zwiers, A. de Bruin, and W.-P. de Roever. A proof system for partial correctness of dynamic networks of processes. In *LNCS 164: Proc. of the Conference on Logics of Programs 1983*, pages 513–527. Springer-Verlag, 1984.

[ZdRvEB84] J. Zwiers, W.-P. de Roever, and P. van Emde Boas. Compositionality and concurrent networks: soundness and completeness of a proof system. Technical report, University of Nijmegen, 1984. Technical Report 57.

Appendix A

Proofs of Dense Model Theorems

A.1 Proof of Theorem 1

Theorem 1 (Relationship between histories and infinite sequences)
Let $h \in \mathcal{H}/\simeq_h$ then $(sel_i)_{i\geq 0} \in SEQ/\simeq_s$ where sel_i is as follows:
if $nn(h) < \infty$:

$$\begin{array}{ll} sel_{2*i+1} = h(i) & 0 \leq i < nn(h) \\ sel_{2*i} = \lim\limits_{i \leftarrow t_1} h(t_1) & 0 \leq i \leq nn(h) \\ sel_{2*i+1} = \lim\limits_{k \leftarrow t_1} h(t_1) & k = nn(h) \wedge k \leq i \\ sel_{2*i} = \lim\limits_{k \leftarrow t_1} h(t_1) & k = nn(h) \wedge k \leq i \end{array}$$

if $nn(h) = \infty$:

$$\begin{array}{ll} sel_{2*i+1} = h(i) & 0 \leq i \\ sel_{2*i} = \lim\limits_{i \leftarrow t_1} h(t_1) & 0 \leq i \end{array}$$

Let $seq = (sel_i)_{i\geq 0} \in SEQ/\simeq_s$ then $h \in \mathcal{H}/\simeq_h$ where h is as follows:
if $ns(seq) < \infty$:

$$\begin{array}{ll} h(0) = sel_0 & \\ h(t) = sel_{2*t-1} & t \in \mathbb{N} \wedge 0 < t \leq ns(seq) \\ h(t) = sel_{2*t} & t \in \mathbb{N} \wedge t > ns(seq) \\ h(t) = sel_{2*i} & i < t < i+1 \end{array}$$

if $ns(seq) = \infty$:

$$\begin{array}{ll} h(0) = sel_0 & \\ h(t) = sel_{2*t-1} & t \in \mathbb{N} \\ h(t) = sel_{2*i} & i < t < i+1 \end{array}$$

Proof 15 *Let $h \in \mathcal{H}/\simeq_h$ then h is of the form $h_1 \circ \mathrm{di}(h_1)$ for some $h_1 \in \mathcal{H}$. According to Def. 10 h is then of the form that at discrete points the non-stutter steps and at all other points the stutter steps occur. The construction of seq above is such that at odd points the* *non-stutter steps (or λ-steps if number of non-stutter steps is finite) and at even points the λ-step occur, i.e., a sequence from $SEQ/\simeq_s$.*

Let $seq = (sel_i)_{i\geq 0} \in SEQ/\simeq_s$ then, according to Def. 11, seq is such that at odd points non-stutter steps occur (or λ-steps if the number of non-stutter stesp is finite) and at the even points λ steps. The construction of h above is such that at discrete points greater than zero the non-stutter steps occur (or λ steps if the number of non-stutter steps is finite) and at all other points the λ steps, i.e. a history from $\mathcal{H}/\simeq_h$.

A.2 Proof of Lemma 1

Lemma 1
Given machine $M = (B, I, T)$ then

$Comp(M)$ is a safety set.

Proof 16 *One has to prove that $Comp(M)$ is* **closed**, *i.e., $\mathcal{H}\setminus Comp(M)$ is an open set, i.e., $\mathcal{H}\setminus Comp(M) \in \tau_d$ (τ_d is the topological space defined in Def. 14).*

$$
\begin{array}{ll}
 & \mathcal{H}\setminus Comp(M) \in \tau_d \\
= & \quad \%\ \ Def.\ 14\ \tau_d \\
 & \forall h : \exists \varepsilon > 0 : \forall h_1 : \\
 & \ (h \in \mathcal{H}\setminus Comp(M) \wedge d(h,h_1) < \varepsilon) \to h_1 \in \mathcal{H}\setminus Comp(M) \\
= & \quad \%\ \ Contraposition \\
 & \forall h : \exists \varepsilon > 0 : \forall h_1 : h_1 \in Comp(M) \wedge d(h,h_1) < \varepsilon) \to h \in Comp(M) \\
= & \quad \%\ \ Def.\ 14\ d(h,h_1) \\
 & \forall h : \forall t : \forall h_1 : (h\downharpoonright_t = h_1\downharpoonright_t \wedge h_1 \in Comp(M)) \to h \in Comp(M) \\
\leftarrow & \quad \%\ \ Pred.\ Calc. \\
 & \forall h : \forall h_1 : \forall t : (h\downharpoonright_t = h_1\downharpoonright_t \wedge h_1 \in Comp(M)) \to h \in Comp(M) \\
\leftarrow & \quad \%\ \ Pred.\ Calc. \\
 & \forall h : \forall h_1 : (h = h_1 \wedge h_1 \in Comp(M)) \to h \in Comp(M) \\
\leftarrow & \quad \%\ \ Pred.\ Calc. \\
 & true
\end{array}
$$

A.3 Proof of Theorem 2

Theorem 2
Let rexp be a rigid expression, exp be an expression, evexp an event expression and p a temporal formula then

$$
\begin{array}{ll}
a & \forall t, h_0, h_1 : h_0 \simeq_{\theta_h} h_1 \to ((h_0,t) \models rexp = (h_1, \mathrm{di}(h_1)\circ \mathrm{di}^{-1}(h_0)(t)) \models rexp) \\
b & \forall t, h_0, h_1 : h_0 \simeq_{\theta_h} h_1 \to ((h_0,t) \models exp = (h_1, \mathrm{di}(h_1)\circ \mathrm{di}^{-1}(h_0)(t)) \models exp) \\
c & \forall t, h_0, h_1 : h_0 \simeq_{\theta_h} h_1 \to ((h_0,t) \models evexp = (h_1, \mathrm{di}(h_1)\circ \mathrm{di}^{-1}(h_0)(t)) \models evexp) \\
d & \forall t, h_0, h_1 : h_0 \simeq_{\theta_h} h_1 \to ((h_0,t) \models p \ \mathit{iff}\ (h_1, \mathrm{di}(h_1)\circ \mathrm{di}^{-1}(h_0)(t)) \models p)
\end{array}
$$

Proof 17

a $\forall t, h_0, h_1 : h_0 \simeq_{\theta_h} h_1 \rightarrow ((h_0, t) \models rexp = (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models rexp)$

The proof proceeds by induction on the structure of rexp

- $rexp = \mu$:

$$\begin{array}{ll} & (h_0, t) \models \mu \\ = & \quad \% \;\; h_0 = h_1 \circ \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0) \\ & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models \mu \end{array}$$

- $rexp = n$:

$$\begin{array}{ll} & (h_0, t) \models n \\ = & \quad \% \;\; Def.\ 20 \\ & \theta_{h_0}(0)(n) \\ = & \quad \% \;\; h_0 = h_1 \circ \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0), \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(0) = 0 \\ & \theta_{h_1}(\mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(0))(n) \\ = & \quad \% \;\; Def.\ 20 \\ & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models n \end{array}$$

- $exp = n'$:

$$\begin{array}{ll} & (h_0, t) \models n' \\ = & \quad \% \;\; Def.\ 20 \\ & \theta_{h_0}(0)(n) \\ = & \quad \% \;\; h_0 = h_1 \circ \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0), \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(0) = 0 \\ & \theta_{h_1}(\mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(0))(n) \\ = & \quad \% \;\; Def.\ 20 \\ & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models n' \end{array}$$

- $exp = \grave{}n$:

$$\begin{array}{ll} & (h_0, t) \models \grave{}n \\ = & \quad \% \;\; Def.\ 20 \\ & \theta_{h_0}(0)(n) \\ = & \quad \% \;\; h_0 = h_1 \circ \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0), \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(0) = 0 \\ & \theta_{h_1}(\mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(0))(n) \\ = & \quad \% \;\; Def.\ 20 \\ & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models \grave{}n \end{array}$$

- $rexp = rexp_1 + rexp_2$:

$$\begin{array}{ll} & (h_0, t) \models rexp_1 + rexp_2 \\ = & \quad \% \;\; Def.\ 20 \\ & (h_0, t) \models rexp_1 + (h_0, t) \models rexp_2 \\ = & \quad \% \;\; Induction \\ & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models rexp_1 + (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models rexp_2 \\ = & \quad \% \;\; Def.\ 20 \\ & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models rexp_1 + rexp_2 \end{array}$$

$b \quad \forall t, h_0, h_1 : h_0 \simeq_{\theta_h} h_1 \rightarrow ((h_0, t) \models exp = (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models exp)$

The proof proceeds by induction on structure of exp:

- $exp = rexp$:

$$\begin{array}{cl} & (h_0, t) \models rexp \\ = & \quad \%\ \ Theorem\ 2a \\ & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models rexp \end{array}$$

- $exp = \mathbf{v}$:

$$\begin{array}{cl} & (h_0, t) \models \mathbf{v} \\ = & \quad \%\ \ Def.\ 20 \\ & \theta_{h_0}(t)(\mathbf{v}) \\ = & \quad \%\ \ h_0 = h_1 \circ \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0) \\ & \theta_{h_1}(\mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t))(\mathbf{v}) \\ = & \quad \%\ \ Def.\ 20 \\ & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models \mathbf{v} \end{array}$$

- $exp = \mathbf{v}'$:

$$\begin{array}{cl} & (h_0, t) \models \mathbf{v}' \\ = & \quad \%\ \ Def.\ 20 \\ & \lim_{t \leftarrow t_1} \theta_{h_0}(t_1)(\mathbf{v}) \\ = & \quad \%\ \ h_0 = h_1 \circ \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0) \\ & \lim_{t \leftarrow t_1} \theta_{h_1}(\mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t_1))(\mathbf{v}) \\ = & \quad \%\ \ t_2 = \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t_1) \\ & \lim_{\mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t) \leftarrow t_2} \theta_{h_1}(t_2)(\mathbf{v}) \\ = & \quad \%\ \ Def.\ 20 \\ & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models \mathbf{v}' \end{array}$$

- $exp = \grave{\mathbf{v}}$:
  $t = 0$

$$\begin{array}{cl} & (h_0, 0) \models \grave{\mathbf{v}} \\ = & \quad \%\ \ Def.\ 20 \\ & \theta_{h_0}(0)(\mathbf{v}) \\ = & \quad \%\ \ h_0 = h_1 \circ \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0) \\ & \theta_{h_1}(\mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(0))(\mathbf{v}) \\ = & \quad \%\ \ Def.\ 20, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(0) = 0 \\ & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(0)) \models \grave{\mathbf{v}} \end{array}$$

$t > 0$

$$
\begin{array}{ll}
 & (h_0, t) \models \grave{\mathbf{v}} \\
= & \quad \% \;\; Def.\ 20 \\
 & \lim\limits_{t_1 \to t} \theta_{h_0}(t_1)(\mathbf{v}) \\
= & \quad \% \;\; h_0 = h_1 \circ \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0) \\
 & \lim\limits_{t_1 \to t} \theta_{h_1}(\mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t_1))(\mathbf{v}) \\
= & \quad \% \;\; t_2 = \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t_1) \\
 & \lim\limits_{t_2 \to \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)} \theta_{h_1}(t_2)(\mathbf{v}) \\
= & \quad \% \;\; Def.\ 20 \\
 & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models \grave{\mathbf{v}}
\end{array}
$$

- $exp = \mathrm{x}$:

$$
\begin{array}{ll}
 & (h_0, t) \models \mathrm{x} \\
= & \quad \% \;\; Def.\ 20 \\
 & \theta_{h_0}(t)(\mathrm{x}) \\
= & \quad \% \;\; h_0 = h_1 \circ \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0) \\
 & \theta_{h_1}(\mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t))(\mathrm{x}) \\
= & \quad \% \;\; Def.\ 20 \\
 & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models \mathrm{x}
\end{array}
$$

- $exp = \mathrm{x}'$:

$$
\begin{array}{ll}
 & (h_0, t) \models \mathrm{x}' \\
= & \quad \% \;\; Def.\ 20 \\
 & \lim\limits_{t \leftarrow t_1} \theta_{h_0}(t_1)(\mathrm{x}) \\
= & \quad \% \;\; h_0 = h_1 \circ \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0) \\
 & \lim\limits_{t \leftarrow t_1} \theta_{h_1}(\mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t_1))(\mathrm{x}) \\
= & \quad \% \;\; t_2 = \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t_1) \\
 & \lim\limits_{\mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t) \leftarrow t_2} \theta_{h_1}(t_2)(\mathrm{x}) \\
= & \quad \% \;\; Def.\ 20 \\
 & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models \mathrm{x}'
\end{array}
$$

- $exp = \grave{\mathrm{x}}$:

$$
\begin{array}{ll}
 & (h_0, 0) \models \grave{\mathrm{x}} \\
= & \quad \% \;\; Def.\ 20 \\
 & \theta_{h_0}(0)(\mathrm{x}) \\
= & \quad \% \;\; h_0 = h_1 \circ \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0) \\
 & \theta_{h_1}(\mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(0))(\mathrm{x}) \\
= & \quad \% \;\; Def.\ 20, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(0) = 0 \\
 & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(0)) \models \grave{\mathrm{x}}
\end{array}
$$

$t > 0$

$$
\begin{array}{ll}
 & (h_0, t) \models \text{`x} \\
= & \quad \% \;\; Def.\ 20 \\
 & \lim\limits_{t_1 \to t} \theta_{h_0}(t_1)(\mathrm{x}) \\
= & \quad \% \;\; h_0 = h_1 \circ \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0) \\
 & \lim\limits_{t_1 \to t} \theta_{h_1}(\mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t_1))(\mathrm{x}) \\
= & \quad \% \;\; t_2 = \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t_1) \\
 & \lim\limits_{t_2 \to \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)} \theta_{h_1}(t_2)(\mathrm{x}) \\
= & \quad \% \;\; Def.\ 20 \\
 & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models \text{`x}
\end{array}
$$

- *$exp = exp_1 + exp_2$:*

$$
\begin{array}{ll}
 & (h_0, t) \models exp_1 + exp_2 \\
= & \quad \% \;\; Def.\ 20 \\
 & (h_0, t) \models exp_1 + (h_0, t) \models exp_2 \\
= & \quad \% \;\; Induction \\
 & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models exp_1 + (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models exp_2 \\
= & \quad \% \;\; Def.\ 20 \\
 & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models exp_1 + exp_2
\end{array}
$$

$c \quad \forall t, h_0, h_1 : h_0 \simeq_{\theta_h} h_1 \to ((h_0, t) \models evexp = (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models evexp)$

The proof proceeds by induction on structure of evexp:

- *$evexp = \mathbf{a}?$:*

$$
\begin{array}{ll}
 & (h_0, t) \models \mathbf{a}? \\
= & \quad \% \;\; Def.\ 20 \\
 & \mathbf{a}? \\
= & \quad \% \;\; Def.\ 20 \\
 & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models \mathbf{a}?
\end{array}
$$

- *$evexp = \mathbf{a}!$:*

$$
\begin{array}{ll}
 & (h_0, t) \models \mathbf{a}! \\
= & \quad \% \;\; Def.\ 20 \\
 & \mathbf{a}! \\
= & \quad \% \;\; Def.\ 20 \\
 & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models \mathbf{a}!
\end{array}
$$

- $evexp = \mathbf{i}$:

$$
\begin{array}{ll}
 & (h_0, t) \models \mathbf{i} \\
= & \quad \% \quad Def.\ 20 \\
 & \mathbf{i} \\
= & \quad \% \quad Def.\ 20 \\
 & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models \mathbf{i}
\end{array}
$$

- $evexp = \mathbf{e}$:

$$
\begin{array}{ll}
 & (h_0, t) \models \mathbf{e} \\
= & \quad \% \quad Def.\ 20 \\
 & \mathbf{e} \\
= & \quad \% \quad Def.\ 20 \\
 & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models \mathbf{e}
\end{array}
$$

- $evexp = \lambda$:

$$
\begin{array}{ll}
 & (h_0, t) \models \lambda \\
= & \quad \% \quad Def.\ 20 \\
 & \lambda \\
= & \quad \% \quad Def.\ 20 \\
 & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models \lambda
\end{array}
$$

- $evexp = \epsilon$:

$$
\begin{array}{ll}
 & (h_0, t) \models \epsilon \\
= & \quad \% \quad Def.\ 20 \\
 & \psi_{h_0}(t)(\epsilon) \\
= & \quad \% \quad h_0 = h_1 \circ \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0) \\
 & \psi_{h_1}(\mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t))(\epsilon) \\
= & \quad \% \quad Def.\ 20 \\
 & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models \epsilon
\end{array}
$$

- $evexp = \epsilon'$:

$$
\begin{array}{ll}
 & (h_0, t) \models \epsilon' \\
= & \quad \% \quad Def.\ 20 \\
 & \lim_{t \leftarrow t_1} \psi_{h_0}(t_1)(\epsilon) \\
= & \quad \% \quad h_0 = h_1 \circ \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0) \\
 & \lim_{t \leftarrow t_1} \psi_{h_1}(\mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t_1))(\epsilon) \\
= & \quad \% \quad t_2 = \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t_1) \\
 & \lim_{\mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t) \leftarrow t_2} \psi_{h_1}(t_2)(\epsilon) \\
= & \quad \% \quad Def.\ 20 \\
 & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models \epsilon'
\end{array}
$$

- $evexp = {`}\epsilon$:

$t = 0$

$$
\begin{array}{ll}
 & (h_0, 0) \models {`}\epsilon \\
= & \quad \% \;\; Def.\ 20 \\
 & \psi_{h_0}(0)(\epsilon) \\
= & \quad \% \;\; h_0 = h_1 \circ \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0) \\
 & \psi_{h_1}(\mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(0))(\epsilon) \\
= & \quad \% \;\; Def.\ 20, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(0) = 0 \\
 & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(0)) \models {`}\epsilon
\end{array}
$$

$t > 0$

$$
\begin{array}{ll}
 & (h_0, t) \models {`}\epsilon \\
= & \quad \% \;\; Def.\ 20 \\
 & \lim\limits_{t_1 \to t} \psi_{h_0}(t_1)(\epsilon) \\
= & \quad \% \;\; h_0 = h_1 \circ \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0) \\
 & \lim\limits_{t_1 \to t} \theta_{h_1}(\mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t_1))(\epsilon) \\
= & \quad \% \;\; t_2 = \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t_1) \\
 & \lim\limits_{t_2 \to \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)} \psi_{h_1}(t_2)(\epsilon) \\
= & \quad \% \;\; Def.\ 20 \\
 & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models {`}\epsilon
\end{array}
$$

$d \quad \forall t, h_0, h_1 : h_0 \simeq_{\theta_h} h_1 \to ((h_0, t) \models p \text{ } \mathit{iff} \text{ } (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models p)$

The proof prooceeds by induction on structure of p:

- $p = \mathbf{true}$:

$$
\begin{array}{ll}
 & (h_0, t) \models \mathbf{true} \\
= & \quad \% \;\; Def.\ 20 \\
 & true \\
= & \quad \% \;\; Def.\ 20 \\
 & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models \mathbf{true}
\end{array}
$$

- $p = (exp_1 = exp_2)$:

$$
\begin{array}{ll}
 & (h_0, t) \models exp_1 = exp_2 \\
= & \quad \% \;\; Def.\ 20 \\
 & (h_0, t) \models exp_1 = (h_0, t) \models exp_2 \\
= & \quad \% \;\; Theorem\ 2b \\
 & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models exp_1 = (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models exp_2 \\
= & \quad \% \;\; Def.\ 20 \\
 & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models exp_1 = exp_2
\end{array}
$$

- $p = (exp_1 < exp_2)$:

$$
\begin{array}{ll}
& (h_0, t) \models exp_1 < exp_2 \\
= & \quad \%\ Def.\ 20 \\
& (h_0, t) \models exp_1 <?(h_0, t) \models exp_2 \\
= & \quad \%\ Theorem\ 2b \\
& (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models exp_1 < (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models exp_2 \\
= & \quad \%\ Def.\ 20 \\
& (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models exp_1 < exp_2
\end{array}
$$

- $p = (evexp_1 = evexp_2)$:

$$
\begin{array}{ll}
& (h_0, t) \models evexp_1 = evexp_2 \\
= & \quad \%\ Def.\ 20 \\
& (h_0, t) \models evexp_1 = (h_0, t) \models evexp_2 \\
= & \quad \%\ Theorem\ 2c \\
& (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models evexp_1 = (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models evexp_2 \\
= & \quad \%\ Def.\ 20 \\
& (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models evexp_1 = evexp_2
\end{array}
$$

- $p = \neg p_0$:

$$
\begin{array}{ll}
& (h_0, t) \models \neg p_0 \\
= & \quad \%\ Def.\ 20 \\
& not\ (h_0, t) \models p_0 \\
= & \quad \%\ Induction \\
& not\ (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models p_0 \\
= & \quad \%\ Def.\ 20 \\
& (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models \neg p_0
\end{array}
$$

- $p = p_1 \vee p_2$:

$$
\begin{array}{ll}
& (h_0, t) \models p_1 \vee p_2 \\
= & \quad \%\ Def.\ 20 \\
& (h_0, t) \models p_1\ or\ (h_0, t) \models p_2 \\
= & \quad \%\ Induction \\
& (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models p_1\ or\ (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models p_2 \\
= & \quad \%\ Def.\ 20 \\
& (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models p_1 \vee p_2
\end{array}
$$

- $p = p_1 \; \widehat{\mathcal{U}} \; p_2$:

$$
\begin{array}{ll}
 & (h_0, t) \models p_1 \; \widehat{\mathcal{U}} \; p_2 \\
= & \quad \% \;\; Def.\ 20 \\
 & \exists t_0 > t : (h_0, t_0) \models p_2 \; and \; \forall t_1 \in (t, t_0) : (h_0, t_1) \models p_1 \\
= & \quad \% \;\; Induction \\
 & \exists t_0 > t : (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t_0)) \models p_2 \\
 & \; and \; \forall t_1 \in (t, t_0) : (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t_1)) \models p_1 \\
= & \quad \% \;\; t_2 = \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t_0), t_3 = \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t_1) \\
 & \exists t_2 > \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t) : (h_1, t_2) \models p_2 \\
 & \; and \; \forall t_3 \in (\mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t), t_2) : (h_1, t_3) \models p_1 \\
= & \quad \% \;\; Def.\ 20 \\
 & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models p_1 \; \widehat{\mathcal{U}} \; p_2
\end{array}
$$

- $p = p_1 \; \widehat{\mathcal{S}} \; p_2$:

$$
\begin{array}{ll}
 & (h_0, t) \models p_1 \; \widehat{\mathcal{S}} \; p_2 \\
= & \quad \% \;\; Def.\ 20 \\
 & \exists t_0 < t : (h_0, t_0) \models p_2 \; and \; \forall t_1 \in (t_0, t) : (h_0, t_1) \models p_1 \\
= & \quad \% \;\; Induction \\
 & \exists t_0 < t : (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t_0)) \models p_2 \\
 & \; and \; \forall t_1 \in (t_0, t) : (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t_1)) \models p_1 \\
= & \quad \% \;\; t_2 = \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t_0), t_3 = \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t_1) \\
 & \exists t_2 < \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) : (h_1, t_2) \models p_2 \\
 & \; and \; \forall t_3 \in (t_2, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) : (h_1, t_3) \models p_1 \\
= & \quad \% \;\; Def.\ 20 \\
 & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models p_1 \; \widehat{\mathcal{S}} \; p_2
\end{array}
$$

- $p = \exists \mathrm{x}.p_0$:

$$
\begin{array}{ll}
 & (h_0, t) \models \exists \mathrm{x}.p_0 \\
= & \quad \% \;\; Def.\ 20 \\
 & \exists h_2 : h_2 \;\; \mathrm{x}\text{-}variant \; of \, h_0 \wedge (h_2, t) \models p_0 \\
= & \quad \% \;\; h_1 = h_0 \circ \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0) \\
 & \exists h_2 : h_2 \;\; \mathrm{x}\text{-}variant \; of \, h_1 \circ \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0) \wedge (h_2, t) \models p_0 \\
= & \quad \% \;\; h_3 = h_1 \circ \mathrm{di}(h_0) \circ \mathrm{di}^{-1}(h_1), \\
 & \qquad\quad h_2 \;\; \mathrm{x}\text{-}variant \; of \, h_1 \circ \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0) \\
 & \qquad\quad \leftrightarrow h_2 \circ \mathrm{di}(h_0) \circ \mathrm{di}^{-1}(h_1) \;\; \mathrm{x}\text{-}variant \; of \, h_1 \\
 & \exists h_3 : h_3 \;\; \mathrm{x}\text{-}variant \; of \, h_1 \wedge (h_3, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models p_0 \\
= & \quad \% \;\; Def.\ 20 \\
 & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models \exists \mathrm{x}.p_0
\end{array}
$$

- $p = \exists \epsilon . p_0$:

$$
\begin{array}{ll}
 & (h_0, t) \models \exists \epsilon . p_0 \\
= & \quad \%\ \ Def.\ 20 \\
 & \exists h_2 : h_2\ \ \epsilon\textit{-variant of}\ h_0 \wedge (h_2, t) \models p_0 \\
= & \quad \%\ \ h_1 = h_0 \circ \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0) \\
 & \exists h_2 : h_2\ \ \epsilon\textit{-variant of}\ h_1 \circ \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0) \wedge (h_2, t) \models p_0 \\
= & \quad \%\ \ h_3 = h_1 \circ \mathrm{di}(h_0) \circ \mathrm{di}^{-1}(h_1), \\
 & \qquad h_2\ \ \epsilon\textit{-variant of}\ h_1 \circ \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0) \\
 & \qquad \leftrightarrow h_2 \circ \mathrm{di}(h_0) \circ \mathrm{di}^{-1}(h_1)\ \ \epsilon\textit{-variant of}\ h_1 \\
 & \exists h_3 : h_3\ \ \epsilon\textit{-variant of}\ h_1 \wedge (h_3, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models p_0 \\
= & \quad \%\ \ Def.\ 20 \\
 & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models \exists \epsilon . p_0
\end{array}
$$

- $p = \exists n . p_0$:

$$
\begin{array}{ll}
 & (h_0, t) \models \exists n . p_0 \\
= & \quad \%\ \ Def.\ 20 \\
 & \exists h_2 : h_2\ \ n\textit{-variant of}\ h_0 \wedge (h_2, t) \models p_0 \\
= & \quad \%\ \ h_1 = h_0 \circ \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0) \\
 & \exists h_2 : h_2\ \ n\textit{-variant of}\ h_1 \circ \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0) \wedge (h_2, t) \models p_0 \\
= & \quad \%\ \ h_3 = h_1 \circ \mathrm{di}(h_0) \circ \mathrm{di}^{-1}(h_1), \\
 & \qquad h_2\ \ n\textit{-variant of}\ h_1 \circ \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0) \\
 & \qquad \leftrightarrow h_2 \circ \mathrm{di}(h_0) \circ \mathrm{di}^{-1}(h_1)\ \ \epsilon\textit{-variant of}\ h_1 \\
 & \exists h_3 : h_3\ \ n\textit{-variant of}\ h_1 \wedge (h_3, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models p_0 \\
= & \quad \%\ \ Def.\ 20 \\
 & (h_1, \mathrm{di}(h_1) \circ \mathrm{di}^{-1}(h_0)(t)) \models \exists n . p_0
\end{array}
$$

A.4 Proof of Lemma 2

Lemma 2
Let exp_0 be an expression, exp be a state expression, $w \in \mathfrak{V} \cup \mathfrak{X}$, $rexp$ be a state rigid expression, $n \in \mathfrak{R}$, $evexp_0$ an event expression, $evexp$ a state event expression, $\epsilon \in \mathfrak{E}$, and p a temporal formula. Then the following holds:

$$
\begin{array}{ll}
a & (h, t) \models exp_0\,[exp/w] = ((h : w \rightsquigarrow exp), t) \models exp_0 \\
b & (h, t) \models exp_0\,[rexp/n] = ((h : n \rightsquigarrow rexp), t) \models exp_0 \\
c & (h, t) \models evexp_0\,[evexp/\epsilon] = ((h : \epsilon \rightsquigarrow evexp), t) \models evexp_0 \\
d & (h, t) \models p\,[exp/w]\ \ \textit{iff}\ ((h : w \rightsquigarrow exp), t) \models p \\
e & (h, t) \models p\,[rexp/n]\ \ \textit{iff}\ ((h : n \rightsquigarrow rexp), t) \models p \\
f & (h, t) \models p\,[evexp/\epsilon]\ \ \textit{iff}\ ((h : \epsilon \rightsquigarrow evexp), t) \models p
\end{array}
$$

Proof 18

$$
a \quad (h, t) \models exp_0\,[exp/w] = ((h : w \rightsquigarrow exp), t) \models exp_0
$$

Proof by induction on the structure of exp_0:

- $exp_0 = rexp$:

$$\begin{array}{ll} & (h,t) \models rexp\,[exp/w] \\ = & \quad \%\ \ Def.\ 22 \\ & (h,t) \models rexp \\ = & \quad \%\ \ Def.\ 26, w \notin varrexp \\ & ((h : w \rightsquigarrow exp), t) \models rexp \end{array}$$

- $exp_0 = \mathbf{v}$:
  $\mathbf{v} \equiv w$

$$\begin{array}{ll} & (h,t) \models \mathbf{v}\,[exp/w] \\ = & \quad \%\ \ Def.\ 22 \\ & (h,t) \models exp \\ = & \quad \%\ \ Def.\ 26 \\ & ((h : w \rightsquigarrow exp), t) \models \mathbf{v} \end{array}$$

  $\mathbf{v} \not\equiv w$

$$\begin{array}{ll} & (h,t) \models \mathbf{v}\,[exp/w] \\ = & \quad \%\ \ Def.\ 22 \\ & (h,t) \models \mathbf{v} \\ = & \quad \%\ \ Def.\ 26 \\ & ((h : w \rightsquigarrow exp), t) \models \mathbf{v} \end{array}$$

- $exp_0 = \mathbf{v}'$:
  $\mathbf{v} \equiv w$

$$\begin{array}{ll} & (h,t) \models \mathbf{v}'\,[exp/w] \\ = & \quad \%\ \ Def.\ 22 \\ & (h,t) \models exp' \\ = & \quad \%\ \ Def.\ 26 \\ & ((h : w \rightsquigarrow exp), t) \models \mathbf{v}' \end{array}$$

  $\mathbf{v} \not\equiv w$

$$\begin{array}{ll} & (h,t) \models \mathbf{v}'\,[exp/w] \\ = & \quad \%\ \ Def.\ 22 \\ & (h,t) \models \mathbf{v}' \\ = & \quad \%\ \ Def.\ 26 \\ & ((h : w \rightsquigarrow exp), t) \models \mathbf{v}' \end{array}$$

- $exp_0 = \grave{\mathbf{v}}$:
  $\mathbf{v} \equiv w$

$$\begin{array}{ll} & (h,t) \models \grave{\mathbf{v}}\,[exp/w] \\ = & \quad \%\ \ Def.\ 22 \\ & (h,t) \models \grave{}exp \\ = & \quad \%\ \ Def.\ 26 \\ & ((h : w \rightsquigarrow exp), t) \models \grave{\mathbf{v}} \end{array}$$

$\mathbf{v} \not\equiv w$

$$
\begin{array}{ll}
 & (h,t) \models \grave{\mathbf{v}}\,[exp/w] \\
= & \quad \%\ \ Def.\ 22 \\
 & (h,t) \models \grave{\mathbf{v}} \\
= & \quad \%\ \ Def.\ 26 \\
 & ((h : w \rightsquigarrow exp), t) \models \grave{\mathbf{v}}
\end{array}
$$

- $exp_0 = \mathrm{x}$:

  $\mathrm{x} \equiv w$

$$
\begin{array}{ll}
 & (h,t) \models \mathrm{x}\,[exp/w] \\
= & \quad \%\ \ Def.\ 22 \\
 & (h,t) \models exp \\
= & \quad \%\ \ Def.\ 26 \\
 & ((h : w \rightsquigarrow exp), t) \models \mathrm{x}
\end{array}
$$

  $\mathrm{x} \not\equiv w$

$$
\begin{array}{ll}
 & (h,t) \models \mathrm{x}\,[exp/w] \\
= & \quad \%\ \ Def.\ 22 \\
 & (h,t) \models \mathrm{x} \\
= & \quad \%\ \ Def.\ 26 \\
 & ((h : w \rightsquigarrow exp), t) \models \mathrm{x}
\end{array}
$$

- $exp_0 = \mathrm{x}'$:

  $\mathrm{x} \equiv w$

$$
\begin{array}{ll}
 & (h,t) \models \mathrm{x}'\,[exp/w] \\
= & \quad \%\ \ Def.\ 22 \\
 & (h,t) \models exp' \\
= & \quad \%\ \ Def.\ 26 \\
 & ((h : w \rightsquigarrow exp), t) \models \mathrm{x}'
\end{array}
$$

  $\mathrm{x} \not\equiv w$

$$
\begin{array}{ll}
 & (h,t) \models \mathrm{x}'\,[exp/w] \\
= & \quad \%\ \ Def.\ 22 \\
 & (h,t) \models \mathrm{x}' \\
= & \quad \%\ \ Def.\ 26 \\
 & ((h : w \rightsquigarrow exp), t) \models \mathrm{x}'
\end{array}
$$

- $exp_0 = \grave{\mathrm{x}}$:

  $\mathrm{x} \equiv w$

$$
\begin{array}{ll}
 & (h,t) \models \grave{\mathrm{x}}\,[exp/w] \\
= & \quad \%\ \ Def.\ 22 \\
 & (h,t) \models \grave{exp} \\
= & \quad \%\ \ Def.\ 26 \\
 & ((h : w \rightsquigarrow exp), t) \models \grave{\mathrm{x}}
\end{array}
$$

$\mathrm{x} \not\equiv w$

$$
\begin{array}{rl}
 & (h,t) \models \grave{\mathrm{x}}\,[exp/w] \\
= & \quad \%\ \ Def.\ 22 \\
 & (h,t) \models \mathrm{x} \\
= & \quad \%\ \ Def.\ 26 \\
 & ((h : w \leadsto exp), t) \models \grave{\mathrm{x}}
\end{array}
$$

- $exp_0 \equiv exp_1 + exp_2$

$$
\begin{array}{rl}
 & (h,t) \models (exp_1 + exp_2)\,[exp/w] \\
= & \quad \%\ \ Def.\ 22 \\
 & (h,t) \models exp_1\,[exp/w] + exp_2\,[exp/w] \\
= & \quad \%\ \ Def.\ 20 \\
 & (h,t) \models exp_1\,[exp/w] + (h,t) \models exp_2\,[exp/w] \\
= & \quad \%\ \ Induction \\
 & ((h : w \leadsto exp), t) \models exp_1 + ((h : w \leadsto exp), t) \models exp_2 \\
= & \quad \%\ \ Def.\ 20 \\
 & ((h : w \leadsto exp), t) \models exp_1 + exp_2
\end{array}
$$

$b \quad (h,t) \models exp_0\,[rexp/n] = ((h : n \leadsto rexp), t) \models exp_0$

Proof by induction on structure of exp_0

- $exp_0 = \mu$:

$$
\begin{array}{rl}
 & (h,t) \models \mu\,[rexp/n] \\
= & \quad \%\ \ Def.\ 23 \\
 & (h,t) \models \mu \\
= & \quad \%\ \ Def.\ 26\ and\ 20 \\
 & ((h : n \leadsto rexp), t) \models \mu
\end{array}
$$

- $exp_0 = n_0$:

$n_0 \equiv n$

$$
\begin{array}{rl}
 & (h,t) \models n_0\,[rexp/n] \\
= & \quad \%\ \ Def.\ 23 \\
 & (h,t) \models rexp \\
= & \quad \%\ \ Def.\ 26 \\
 & ((h : n \leadsto rexp), t) \models n_0
\end{array}
$$

$n_0 \not\equiv n$

$$
\begin{array}{rl}
 & (h,t) \models n_0\,[rexp/n] \\
= & \quad \%\ \ Def.\ 23 \\
 & (h,t) \models n_0 \\
= & \quad \%\ \ Def.\ 26 \\
 & ((h : n \leadsto rexp), t) \models n_0
\end{array}
$$

- $exp_0 = n'_0$:

  $n_0 \equiv n$

$$\begin{array}{ll} & (h,t) \models n'_0\,[rexp/n] \\ = & \quad \%\ \ Def.\ 23 \\ & (h,t) \models rexp' \\ = & \quad \%\ \ Def.\ 26 \\ & ((h : n \rightsquigarrow rexp), t) \models n'_0 \end{array}$$

  $n_0 \not\equiv n$

$$\begin{array}{ll} & (h,t) \models n'_0\,[rexp/n] \\ = & \quad \%\ \ Def.\ 23 \\ & (h,t) \models n'_0 \\ = & \quad \%\ \ Def.\ 26 \\ & ((h : n \rightsquigarrow rexp), t) \models n'_0 \end{array}$$

- $exp_0 = \grave{n}_0$:

  $n_0 \equiv n$

$$\begin{array}{ll} & (h,t) \models \grave{n}_0\,[rexp/n] \\ = & \quad \%\ \ Def.\ 23 \\ & (h,t) \models \grave{r}exp \\ = & \quad \%\ \ Def.\ 26 \\ & ((h : n \rightsquigarrow rexp), t) \models \grave{n}_0 \end{array}$$

  $n_0 \not\equiv n$

$$\begin{array}{ll} & (h,t) \models \grave{n}_0\,[rexp/n] \\ = & \quad \%\ \ Def.\ 23 \\ & (h,t) \models \grave{n}_0 \\ = & \quad \%\ \ Def.\ 26 \\ & ((h : n \rightsquigarrow rexp), t) \models \grave{n}_0 \end{array}$$

- $exp_0 = w$:

$$\begin{array}{ll} & (h,t) \models w\,[rexp/n] \\ = & \quad \%\ \ Def.\ 23 \\ & (h,t) \models w \\ = & \quad \%\ \ Def.\ 26 \\ & ((h : n \rightsquigarrow rexp), t) \models w \end{array}$$

- $exp_0 = w'$:

$$\begin{array}{ll} & (h,t) \models w'\,[rexp/n] \\ = & \quad \%\ \ Def.\ 23 \\ & (h,t) \models w' \\ = & \quad \%\ \ Def.\ 26 \\ & ((h : n \rightsquigarrow rexp), t) \models w' \end{array}$$

- $exp_0 = \grave{}w$:

$$
\begin{array}{ll}
 & (h,t) \models \grave{}w\,[rexp/n] \\
= & \quad \%\ \ Def.\ 23 \\
 & (h,t) \models \grave{}w \\
= & \quad \%\ \ Def.\ 26 \\
 & ((h : n \rightsquigarrow rexp), t) \models \grave{}w
\end{array}
$$

- $exp_0 \equiv exp_1 + exp_2$

$$
\begin{array}{ll}
 & (h,t) \models (exp_1 + exp_2)\,[rexp/n] \\
= & \quad \%\ \ Def.\ 23 \\
 & (h,t) \models exp_1\,[rexp/n] + exp_2\,[rexp/n] \\
= & \quad \%\ \ Def.\ 20 \\
 & (h,t) \models exp_1\,[rexp/n] + (h,t) \models exp_2\,[rexp/n] \\
= & \quad \%\ \ Induction \\
 & ((h : n \rightsquigarrow rexp), t) \models exp_1 + ((h : n \rightsquigarrow rexp), t) \models exp_2 \\
= & \quad \%\ \ Def.\ 20 \\
 & ((h : n \rightsquigarrow rexp), t) \models exp_1 + exp_2
\end{array}
$$

$c \quad (h,t) \models evexp_0\,[evexp/\epsilon] = ((h : \epsilon \rightsquigarrow evexp), t) \models evexp_0$

Proof by induction on structure of $evexp_0$*:*

- $evexp_0 = \lambda$:

$$
\begin{array}{ll}
 & (h,t) \models \lambda\,[evexp/\epsilon] \\
= & \quad \%\ \ Def.\ 24 \\
 & (h,t) \models \lambda \\
= & \quad \%\ \ Def.\ 26\ and\ 20 \\
 & ((h : \epsilon \rightsquigarrow evexp), t) \models \lambda
\end{array}
$$

- $evexp_0 = \mathbf{a}?$:

$$
\begin{array}{ll}
 & (h,t) \models \mathbf{a}?\,[evexp/\epsilon] \\
= & \quad \%\ \ Def.\ 24 \\
 & (h,t) \models \mathbf{a}? \\
= & \quad \%\ \ Def.\ 26\ and\ 20 \\
 & ((h : \epsilon \rightsquigarrow evexp), t) \models \mathbf{a}?
\end{array}
$$

- $evexp_0 = \mathbf{a}!$:

$$
\begin{array}{ll}
 & (h,t) \models \mathbf{a}!\,[evexp/\epsilon] \\
= & \quad \%\ \ Def.\ 24 \\
 & (h,t) \models \mathbf{a}! \\
= & \quad \%\ \ Def.\ 26\ and\ 20 \\
 & ((h : \epsilon \rightsquigarrow evexp), t) \models \mathbf{a}!
\end{array}
$$

- $evexp_0 = \mathbf{i}$:

$$\begin{array}{ll} & (h,t) \models \mathbf{i}\,[evexp/\epsilon] \\ = & \quad \%\ \ Def.\ 24 \\ & (h,t) \models \mathbf{i} \\ = & \quad \%\ \ Def.\ 26\ and\ 20 \\ & ((h : \epsilon \rightsquigarrow evexp), t) \models \mathbf{i} \end{array}$$

- $evexp_0 = \mathbf{e}$:

$$\begin{array}{ll} & (h,t) \models \mathbf{e}\,[evexp/\epsilon] \\ = & \quad \%\ \ Def.\ 24 \\ & (h,t) \models \mathbf{e} \\ = & \quad \%\ \ Def.\ 26\ and\ 20 \\ & ((h : \epsilon \rightsquigarrow evexp), t) \models \mathbf{e} \end{array}$$

- $evexp_0 = \epsilon_0$:
  $\epsilon_0 \equiv \epsilon$

$$\begin{array}{ll} & (h,t) \models \epsilon_0\,[evexp/\epsilon] \\ = & \quad \%\ \ Def.\ 24 \\ & (h,t) \models evexp \\ = & \quad \%\ \ Def.\ 26 \\ & ((h : \epsilon \rightsquigarrow evexp), t) \models \epsilon_0 \end{array}$$

  $\epsilon_0 \not\equiv \epsilon$

$$\begin{array}{ll} & (h,t) \models \epsilon_0\,[evexp/\epsilon] \\ = & \quad \%\ \ Def.\ 24 \\ & (h,t) \models \epsilon_0 \\ = & \quad \%\ \ Def.\ 26 \\ & ((h : \epsilon \rightsquigarrow evexp), t) \models \epsilon_0 \end{array}$$

- $evexp_0 = \epsilon_0'$:
  $\epsilon_0 \equiv \epsilon$

$$\begin{array}{ll} & (h,t) \models \epsilon_0'\,[evexp/\epsilon] \\ = & \quad \%\ \ Def.\ 24 \\ & (h,t) \models evexp' \\ = & \quad \%\ \ Def.\ 26 \\ & ((h : \epsilon \rightsquigarrow evexp), t) \models \epsilon_0' \end{array}$$

  $\epsilon_0 \not\equiv \epsilon$

$$\begin{array}{ll} & (h,t) \models \epsilon_0'\,[evexp/\epsilon] \\ = & \quad \%\ \ Def.\ 24 \\ & (h,t) \models \epsilon_0' \\ = & \quad \%\ \ Def.\ 26 \\ & ((h : \epsilon \rightsquigarrow evexp), t) \models \epsilon_0' \end{array}$$

- $evexp_0 = `\epsilon_0$:
  $\epsilon_0 \equiv \epsilon$

$$
\begin{array}{ll}
 & (h,t) \models `\epsilon_0\,[evexp/\epsilon] \\
= & \quad \%\ \ Def.\ 24 \\
 & (h,t) \models `evexp \\
= & \quad \%\ \ Def.\ 26 \\
 & ((h : \epsilon \rightsquigarrow evexp), t) \models `\epsilon_0
\end{array}
$$

$\epsilon_0 \not\equiv \epsilon$

$$
\begin{array}{ll}
 & (h,t) \models `\epsilon_0\,[evexp/\epsilon] \\
= & \quad \%\ \ Def.\ 24 \\
 & (h,t) \models \epsilon_0 \\
= & \quad \%\ \ Def.\ 26 \\
 & ((h : \epsilon \rightsquigarrow evexp), t) \models `\epsilon_0
\end{array}
$$

$d \quad (h,t) \models p\,[exp/w]$ *iff* $((h : w \rightsquigarrow exp), t) \models p$

Proof by induction on structure of p*:*

- $p = \mathbf{true}$:

$$
\begin{array}{ll}
 & (h,t) \models \mathbf{true}\,[exp/w] \\
= & \quad \%\ \ Def.\ 25 \\
 & (h,t) \models \mathbf{true} \\
= & \quad \%\ \ Def.\ 26 \\
 & ((h : w \rightsquigarrow exp), t) \models \mathbf{true}
\end{array}
$$

- $p = (exp_1 = exp_2)$:

$$
\begin{array}{ll}
 & (h,t) \models (exp_1 = exp_2)\,[exp/w] \\
= & \quad \%\ \ Def.\ 25 \\
 & (h,t) \models exp_1\,[exp/w] = exp_2\,[exp/w] \\
= & \quad \%\ \ Def.\ 20 \\
 & (h,t) \models exp_1\,[exp/w] = (h,t) \models exp_2\,[exp/w] \\
= & \quad \%\ \ Lemma\ 2a \\
 & ((h : w \rightsquigarrow exp), t) \models exp_1 = ((h : w \rightsquigarrow exp), t) \models exp_2 \\
= & \quad \%\ \ Def.\ 20 \\
 & ((h : w \rightsquigarrow exp), t) \models exp_1 = exp_2
\end{array}
$$

- $p = (exp_1 < exp_2)$:

$$
\begin{array}{ll}
 & (h,t) \models (exp_1 < exp_2)\,[exp/w] \\
= & \quad \%\ \ Def.\ 25 \\
 & (h,t) \models exp_1\,[exp/w] < exp_2\,[exp/w] \\
= & \quad \%\ \ Def.\ 20 \\
 & (h,t) \models exp_1\,[exp/w] < (h,t) \models exp_2\,[exp/w] \\
= & \quad \%\ \ Lemma\ refsu.lea \\
 & ((h : w \rightsquigarrow exp), t) \models exp_1 < ((h : w \rightsquigarrow exp), t) \models exp_2 \\
= & \quad \%\ \ Def.\ 20 \\
 & ((h : w \rightsquigarrow exp), t) \models exp_1 < exp_2
\end{array}
$$

- $p = (evexp_1 = evexp_2)$:

$$
\begin{array}{ll}
 & (h,t) \models (evexp_1 = evexp_2)\,[exp/w] \\
= & \quad \%\ \ Def.\ 25 \\
 & (h,t) \models evexp_1 = evexp_2 \\
= & \quad \%\ \ Def.\ 20 \\
 & (h,t) \models evexp_1 = (h,t) \models evexp_2 \\
= & \quad \%\ \ Def.\ 26 \\
 & ((h : w \rightsquigarrow exp), t) \models evexp_1 = ((h : w \rightsquigarrow exp), t) \models evexp_2 \\
= & \quad \%\ \ Def.\ 20 \\
 & ((h : w \rightsquigarrow exp), t) \models evexp_1 = evexp_2
\end{array}
$$

- $p = \neg p_1$:

$$
\begin{array}{ll}
 & (h,t) \models (\neg p_1)\,[exp/w] \\
= & \quad \%\ \ Def.\ 25 \\
 & (h,t) \models \neg(p_1\,[exp/w]) \\
= & \quad \%\ \ Def.\ 20 \\
 & not\ \ (h,t) \models p_1\,[exp/w] \\
= & \quad \%\ \ Induction \\
 & not\ \ ((h : w \rightsquigarrow exp), t) \models p_1 \\
= & \quad \%\ \ Def.\ 20 \\
 & ((h : w \rightsquigarrow exp), t) \models \neg p_1
\end{array}
$$

- $p = p_1 \vee p_2$:

$$
\begin{array}{ll}
 & (h,t) \models (p_1 \vee p_2)\,[exp/w] \\
= & \quad \%\ \ Def.\ 25 \\
 & (h,t) \models (p_1\,[exp/w] \vee p_2\,[exp/w]) \\
= & \quad \%\ \ Def.\ 20 \\
 & (h,t) \models p_1\,[exp/w]\ \ or\ \ (h,t) \models p_2\,[exp/w] \\
= & \quad \%\ \ Induction \\
 & ((h : w \rightsquigarrow exp), t) \models p_1\ \ or\ \ ((h : w \rightsquigarrow exp), t) \models p_2 \\
= & \quad \%\ \ Def.\ 20 \\
 & ((h : w \rightsquigarrow exp), t) \models p_1 \vee p_2
\end{array}
$$

- $p = p_1 \; \widehat{\mathcal{U}} \; p_2$:

$$
\begin{array}{ll}
 & (h,t) \models (p_1 \; \widehat{\mathcal{U}} \; p_2) \, [exp/w] \\
= & \quad \% \;\; Def. \; 25 \\
 & (h,t) \models (p_1 \, [exp/w] \;\; \widehat{\mathcal{U}} \; p_2 \, [exp/w]) \\
= & \quad \% \;\; Def. \; 20 \\
 & \exists t_0 > t : (h,t_0) \models p_2 \, [exp/w] \;\; and \; \forall t_1 \in (t,t_0) : (h,t_1) \models p_1 \, [exp/w] \\
= & \quad \% \;\; Induction \\
 & \exists t_0 > t : ((h : w \rightsquigarrow exp), t_0) \models p_2 \\
 & and \; \forall t_1 \in (t,t_0) : ((h : w \rightsquigarrow exp), t_1) \models p_1 \\
= & \quad \% \;\; Def. \; 20 \\
 & ((h : w \rightsquigarrow exp), t) \models p_1 \; \widehat{\mathcal{U}} \; p_2
\end{array}
$$

- $p = p_1 \; \widehat{\mathcal{S}} \; p_2$:

$$
\begin{array}{ll}
 & (h,t) \models (p_1 \; \widehat{\mathcal{S}} \; p_2) \, [exp/w] \\
= & \quad \% \;\; Def. \; 25 \\
 & (h,t) \models (p_1 \, [exp/w] \;\; \widehat{\mathcal{S}} \; p_2 \, [exp/w]) \\
= & \quad \% \;\; Def. \; 20 \\
 & \exists t_0 < t : (h,t_0) \models p_2 \, [exp/w] \;\; and \; \forall t_1 \in (t_0,t) : (h,t_1) \models p_1 \, [exp/w] \\
= & \quad \% \;\; Induction \\
 & \exists t_0 < t : ((h : w \rightsquigarrow exp), t_0) \models p_2 \\
 & and \; \forall t_1 \in (t_0,t) : ((h : w \rightsquigarrow exp), t_1) \models p_1 \\
= & \quad \% \;\; Def. \; 20 \\
 & ((h : w \rightsquigarrow exp), t) \models p_1 \; \widehat{\mathcal{S}} \; p_2
\end{array}
$$

- $p = \exists \mathrm{x}.p_1$ *for* $\mathrm{x} \notin var(exp) \cup \{w\}$:

$$
\begin{array}{ll}
 & (h,t) \models (\exists \mathrm{x}.p_1) \, [exp/w] \\
= & \quad \% \;\; Def. \; 25 \\
 & (h,t) \models \exists \mathrm{x}.(p_1 \, [exp/w]) \\
= & \quad \% \;\; Def. \; 20 \\
 & \exists h_1 : h_1 \; \mathrm{x}\text{-}variant \; of \, h \;\; and \;\; (h_1,t) \models p_1 \, [exp/w] \\
= & \quad \% \;\; Induction \\
 & \exists h_1 : h_1 \; \mathrm{x}\text{-}variant \; of \, h \;\; and \;\; ((h_1 : w \rightsquigarrow exp), t) \models p_1 \\
= & \quad \% \;\; h_2 = (h_1 : w \rightsquigarrow exp), h_3 = (h : w \rightsquigarrow exp) \\
 & \qquad\;\; h_1 \; \mathrm{x}\text{-}variant \;\; of \, h \;\; iff \;\; h_2 \; \mathrm{x}\text{-}variant \;\; of \, h_3 \\
 & \exists h_2 : h_2 \; \mathrm{x}\text{-}variant \; of \, h_3 \;\; and \;\; (h_2,t) \models p_1 \\
= & \quad \% \;\; Def. \; 20 \\
 & ((h : w \rightsquigarrow exp), t) \models \exists \mathrm{x}.p_1
\end{array}
$$

- $p = \exists \epsilon . p_1$:

$$
\begin{array}{ll}
 & (h,t) \models (\exists \epsilon . p_1)\,[exp/w] \\
= & \quad \%\ \ Def.\ 25 \\
 & (h,t) \models \exists \epsilon . (p_1\,[exp/w]) \\
= & \quad \%\ \ Def.\ 20 \\
 & \exists h_1 : h_1\ \epsilon\text{-}variant\ \ of\ h\ \ and\ (h_1,t) \models p_1\,[exp/w] \\
= & \quad \%\ \ Induction \\
 & \exists h_1 : h_1\ \epsilon\text{-}variant\ \ of\ h\ \ and\ ((h_1 : w \rightsquigarrow exp),t) \models p_1 \\
= & \quad \%\ \ h_2 = (h_1 : w \rightsquigarrow exp), h_3 = (h : w \rightsquigarrow exp) \\
 & \qquad\ \ h_1\ \epsilon\text{-}variant\ \ of\ h\ \ iff\ \ h_2\ \epsilon\text{-}variant\ \ of\ h_3 \\
 & \exists h_2 : h_2\ \epsilon\text{-}variant\ \ of\ h_3\ \ and\ (h_2,t) \models p_1 \\
= & \quad \%\ \ Def.\ 20 \\
 & ((h : w \rightsquigarrow exp),t) \models \exists \epsilon . p_1
\end{array}
$$

- $p = \exists n . p_1$:

$$
\begin{array}{ll}
 & (h,t) \models (\exists n . p_1)\,[exp/w] \\
= & \quad \%\ \ Def.\ 25 \\
 & (h,t) \models \exists n . (p_1\,[exp/w]) \\
= & \quad \%\ \ Def.\ 20 \\
 & \exists h_1 : h_1\ n\text{-}variant\ \ of\ h\ \ and\ (h_1,t) \models p_1\,[exp/w] \\
= & \quad \%\ \ Induction \\
 & \exists h_1 : h_1\ n\text{-}variant\ \ of\ h\ \ and\ ((h_1 : w \rightsquigarrow exp),t) \models p_1 \\
= & \quad \%\ \ h_2 = (h_1 : w \rightsquigarrow exp), h_3 = (h : w \rightsquigarrow exp) \\
 & \qquad\ \ h_1\ n\text{-}variant\ \ of\ h\ \ iff\ \ h_2\ n\text{-}variant\ \ of\ h_3 \\
 & \exists h_2 : h_2\ n\text{-}variant\ \ of\ h_3\ \ and\ (h_2,t) \models p_1 \\
= & \quad \%\ \ Def.\ 20 \\
 & ((h : w \rightsquigarrow exp),t) \models \exists n . p_1
\end{array}
$$

e $\quad (h,t) \models p\,[rexp/n]$ *iff* $((h : n \rightsquigarrow rexp),t) \models p$

Proof by induction on structure of p:

- $p = \mathbf{true}$:

$$
\begin{array}{ll}
 & (h,t) \models \mathbf{true}\,[rexp/n] \\
= & \quad \%\ \ Def.\ 25 \\
 & (h,t) \models \mathbf{true} \\
= & \quad \%\ \ Def.\ 26 \\
 & ((h : n \rightsquigarrow rexp),t) \models \mathbf{true}
\end{array}
$$

- $p = (exp_1 = exp_2)$:

$$\begin{array}{ll} & (h,t) \models (exp_1 = exp_2)\,[rexp/n] \\ = & \quad \%\ \ Def.\ 25 \\ & (h,t) \models exp_1\,[rexp/n] = exp_2\,[rexp/n] \\ = & \quad \%\ \ Def.\ 20 \\ & (h,t) \models exp_1\,[rexp/n] = (h,t) \models exp_2\,[rexp/n] \\ = & \quad \%\ \ Lemma\ 2b \\ & ((h:n \rightsquigarrow rexp),t) \models exp_1 = ((h:n \rightsquigarrow rexp),t) \models exp_2 \\ = & \quad \%\ \ Def.\ 20 \\ & ((h:n \rightsquigarrow rexp),t) \models exp_1 = exp_2 \end{array}$$

- $p = (exp_1 < exp_2)$:

$$\begin{array}{ll} & (h,t) \models (exp_1 < exp_2)\,[rexp/n] \\ = & \quad \%\ \ Def.\ 25 \\ & (h,t) \models exp_1\,[rexp/n] < exp_2\,[rexp/n] \\ = & \quad \%\ \ Def.\ 20 \\ & (h,t) \models exp_1\,[rexp/n] < (h,t) \models exp_2\,[rexp/n] \\ = & \quad \%\ \ Lemma\ 2b \\ & ((h:n \rightsquigarrow rexp),t) \models exp_1 < ((h:n \rightsquigarrow rexp),t) \models exp_2 \\ = & \quad \%\ \ Def.\ 20 \\ & ((h:n \rightsquigarrow rexp),t) \models exp_1 < exp_2 \end{array}$$

- $p = (evexp_1 = evexp_2)$:

$$\begin{array}{ll} & (h,t) \models (evexp_1 = evexp_2)\,[rexp/n] \\ = & \quad \%\ \ Def.\ 25 \\ & (h,t) \models evexp_1 = evexp_2 \\ = & \quad \%\ \ Def.\ 20 \\ & (h,t) \models evexp_1 = (h,t) \models evexp_2 \\ = & \quad \%\ \ Def.\ 26 \\ & ((h:n \rightsquigarrow rexp),t) \models evexp_1 = ((h:n \rightsquigarrow rexp),t) \models evexp_2 \\ = & \quad \%\ \ Def.\ 20 \\ & ((h:n \rightsquigarrow rexp),t) \models evexp_1 = evexp_2 \end{array}$$

- $p = \neg p_1$:

$$\begin{array}{ll} & (h,t) \models (\neg p_1)\,[rexp/n] \\ = & \quad \%\ \ Def.\ 25 \\ & (h,t) \models \neg(p_1\,[rexp/n]) \\ = & \quad \%\ \ Def.\ 20 \\ & not\ (h,t) \models p_1\,[rexp/n] \\ = & \quad \%\ \ Induction \\ & not\ ((h:n \rightsquigarrow rexp),t) \models p_1 \\ = & \quad \%\ \ Def.\ 20 \\ & ((h:n \rightsquigarrow rexp),t) \models \neg p_1 \end{array}$$

- $p = p_1 \vee p_2$:

$$
\begin{array}{ll}
 & (h,t) \models (p_1 \vee p_2)\,[rexp/n] \\
= & \quad \% \;\; Def.\ 25 \\
 & (h,t) \models (p_1\,[rexp/n] \vee p_2\,[rexp/n]) \\
= & \quad \% \;\; Def.\ 20 \\
 & (h,t) \models p_1\,[rexp/n] \;\; or \;\; (h,t) \models p_2\,[rexp/n] \\
= & \quad \% \;\; Induction \\
 & ((h : n \rightsquigarrow rexp), t) \models p_1 \;\; or \;\; ((h : n \rightsquigarrow rexp), t) \models p_2 \\
= & \quad \% \;\; Def.\ 20 \\
 & ((h : n \rightsquigarrow rexp), t) \models p_1 \vee p_2
\end{array}
$$

- $p = p_1 \;\widehat{\mathcal{U}}\; p_2$:

$$
\begin{array}{ll}
 & (h,t) \models (p_1 \;\widehat{\mathcal{U}}\; p_2)\,[rexp/n] \\
= & \quad \% \;\; Def.\ 25 \\
 & (h,t) \models (p_1\,[rexp/n] \;\widehat{\mathcal{U}}\; p_2\,[rexp/n]) \\
= & \quad \% \;\; Def.\ 20 \\
 & \exists t_0 > t : (h,t_0) \models p_2\,[rexp/n] \;\; and \;\; \forall t_1 \in (t,t_0) : (h,t_1) \models p_1\,[rexp/n] \\
= & \quad \% \;\; Induction \\
 & \exists t_0 > t : ((h : n \rightsquigarrow rexp), t_0) \models p_2 \\
 & and \;\; \forall t_1 \in (t,t_0) : ((h : n \rightsquigarrow rexp), t_1) \models p_1 \\
= & \quad \% \;\; Def.\ 20 \\
 & ((h : n \rightsquigarrow rexp), t) \models p_1 \;\widehat{\mathcal{U}}\; p_2
\end{array}
$$

- $p = p_1 \;\widehat{\mathcal{S}}\; p_2$:

$$
\begin{array}{ll}
 & (h,t) \models (p_1 \;\widehat{\mathcal{S}}\; p_2)\,[rexp/n] \\
= & \quad \% \;\; Def.\ 25 \\
 & (h,t) \models (p_1\,[rexp/n] \;\widehat{\mathcal{S}}\; p_2\,[rexp/n]) \\
= & \quad \% \;\; Def.\ 20 \\
 & \exists t_0 < t : (h,t_0) \models p_2\,[rexp/n] \;\; and \;\; \forall t_1 \in (t_0,t) : (h,t_1) \models p_1\,[rexp/n] \\
= & \quad \% \;\; Induction \\
 & \exists t_0 < t : ((h : n \rightsquigarrow rexp), t_0) \models p_2 \\
 & and \;\; \forall t_1 \in (t_0,t) : ((h : n \rightsquigarrow rexp), t_1) \models p_1 \\
= & \quad \% \;\; Def.\ 20 \\
 & ((h : n \rightsquigarrow rexp), t) \models p_1 \;\widehat{\mathcal{S}}\; p_2
\end{array}
$$

- $p = \exists \mathrm{x}.p_1$:

$$
\begin{array}{ll}
 & (h,t) \models (\exists \mathrm{x}.p_1)\,[rexp/n] \\
= & \quad \%\ \ Def.\ 25 \\
 & (h,t) \models \exists \mathrm{x}.(p_1\,[rexp/n]) \\
= & \quad \%\ \ Def.\ 20 \\
 & \exists h_1 : h_1 \ \mathrm{x}\text{-}variant\ of\ h\ and\ (h_1,t) \models p_1\,[rexp/n] \\
= & \quad \%\ \ Induction \\
 & \exists h_1 : h_1 \ \mathrm{x}\text{-}variant\ of\ h\ and\ ((h_1 : n \leadsto rexp),t) \models p_1 \\
= & \quad \%\ \ h_2 = (h_1 : n \leadsto rexp), h_3 = (h : n \leadsto rexp) \\
 & \qquad h_1\ \mathrm{x}\text{-}variant\ of\ h\ iff\ h_2\ \mathrm{x}\text{-}variant\ of\ h_3 \\
 & \exists h_2 : h_2 \ \mathrm{x}\text{-}variant\ of\ h_3\ and\ (h_2,t) \models p_1 \\
= & \quad \%\ \ Def.\ 20 \\
 & ((h : n \leadsto rexp),t) \models \exists \mathrm{x}.p_1
\end{array}
$$

- $p = \exists \epsilon.p_1$:

$$
\begin{array}{ll}
 & (h,t) \models (\exists \epsilon.p_1)\,[rexp/n] \\
= & \quad \%\ \ Def.\ 25 \\
 & (h,t) \models \exists \epsilon.(p_1\,[rexp/n]) \\
= & \quad \%\ \ Def.\ 20 \\
 & \exists h_1 : h_1 \ \epsilon\text{-}variant\ of\ h\ and\ (h_1,t) \models p_1\,[rexp/n] \\
= & \quad \%\ \ Induction \\
 & \exists h_1 : h_1 \ \epsilon\text{-}variant\ of\ h\ and\ ((h_1 : n \leadsto rexp),t) \models p_1 \\
= & \quad \%\ \ h_2 = (h_1 : n \leadsto rexp), h_3 = (h : n \leadsto rexp) \\
 & \qquad h_1\ \epsilon\text{-}variant\ of\ h\ iff\ h_2\ \epsilon\text{-}variant\ of\ h_3 \\
 & \exists h_2 : h_2 \ \epsilon\text{-}variant\ of\ h_3\ and\ (h_2,t) \models p_1 \\
= & \quad \%\ \ Def.\ 20 \\
 & ((h : n \leadsto rexp),t) \models \exists \epsilon.p_1
\end{array}
$$

- $p = \exists n_0.p_1$: *for* $n_0 \notin varrexp \cup \{n\}$

$$
\begin{array}{ll}
 & (h,t) \models (\exists n_0.p_1)\,[rexp/n] \\
= & \quad \%\ \ Def.\ 25 \\
 & (h,t) \models \exists n_0.(p_1\,[rexp/n]) \\
= & \quad \%\ \ Def.\ 20 \\
 & \exists h_1 : h_1 \ n_0\text{-}variant\ of\ h\ and\ (h_1,t) \models p_1\,[rexp/n] \\
= & \quad \%\ \ Induction \\
 & \exists h_1 : h_1 \ n_0\text{-}variant\ of\ h\ and\ ((h_1 : n \leadsto rexp),t) \models p_1 \\
= & \quad \%\ \ h_2 = (h_1 : n \leadsto rexp), h_3 = (h : n \leadsto rexp) \\
 & \qquad h_1\ n_0\text{-}variant\ of\ h\ iff\ h_2\ n_0\text{-}variant\ of\ h_3 \\
 & \exists h_2 : h_2 \ n_0\text{-}variant\ of\ h_3\ and\ (h_2,t) \models p_1 \\
= & \quad \%\ \ Def.\ 20 \\
 & ((h : n \leadsto rexp),t) \models \exists n_0.p_1
\end{array}
$$

$f \quad h, t) \models p\,[evexp/\epsilon]$ *iff* $((h : \epsilon \rightsquigarrow evexp), t) \models p$

Proof by induction on structure of p:

- $p = \mathbf{true}$*:*

$$
\begin{aligned}
& (h, t) \models \mathbf{true}\,[evexp/\epsilon] \\
= \quad & \quad \%\ \ Def.\ 25 \\
& (h, t) \models \mathbf{true} \\
= \quad & \quad \%\ \ Def.\ 26 \\
& ((h : \epsilon \rightsquigarrow evexp), t) \models \mathbf{true}
\end{aligned}
$$

- $p = (exp_1 = exp_2)$*:*

$$
\begin{aligned}
& (h, t) \models (exp_1 = exp_2)\,[evexp/\epsilon] \\
= \quad & \quad \%\ \ Def.\ 25 \\
& (h, t) \models exp_1 = exp_2 \\
= \quad & \quad \%\ \ Def.\ 20 \\
& (h, t) \models exp_1 = (h, t) \models exp_2 \\
= \quad & \quad \%\ \ Def.\ 26 \\
& ((h : \epsilon \rightsquigarrow evexp), t) \models exp_1 = ((h : \epsilon \rightsquigarrow evexp), t) \models exp_2 \\
= \quad & \quad \%\ \ Def.\ 20 \\
& ((h : \epsilon \rightsquigarrow evexp), t) \models exp_1 = exp_2
\end{aligned}
$$

- $p = (exp_1 < exp_2)$*:*

$$
\begin{aligned}
& (h, t) \models (exp_1 < exp_2)\,[evexp/\epsilon] \\
= \quad & \quad \%\ \ Def.\ 25 \\
& (h, t) \models exp_1 < exp_2 \\
= \quad & \quad \%\ \ Def.\ 20 \\
& (h, t) \models exp_1 < (h, t) \models exp_2 \\
= \quad & \quad \%\ \ Def.\ 26 \\
& ((h : \epsilon \rightsquigarrow evexp), t) \models exp_1 < ((h : \epsilon \rightsquigarrow evexp), t) \models exp_2 \\
= \quad & \quad \%\ \ Def.\ 20 \\
& ((h : \epsilon \rightsquigarrow evexp), t) \models exp_1 < exp_2
\end{aligned}
$$

- $p = (evexp_1 = evexp_2)$*:*

$$
\begin{aligned}
& (h, t) \models (evexp_1 = evexp_2)\,[evexp/\epsilon] \\
= \quad & \quad \%\ \ Def.\ 25 \\
& (h, t) \models evexp_1\,[evexp_1/\epsilon] = evexp_2\,[evexp_1/\epsilon] \\
= \quad & \quad \%\ \ Def.\ 20 \\
& (h, t) \models evexp_1\,[evexp_1/\epsilon] = (h, t) \models evexp_2\,[evexp_2/\epsilon] \\
= \quad & \quad \%\ \ Lemma\ 2c \\
& ((h : \epsilon \rightsquigarrow evexp), t) \models evexp_1 = ((h : \epsilon \rightsquigarrow evexp), t) \models evexp_2 \\
= \quad & \quad \%\ \ Def.\ 20 \\
& ((h : \epsilon \rightsquigarrow evexp), t) \models evexp_1 = evexp_2
\end{aligned}
$$

- $p = \neg p_1$:

$$
\begin{array}{ll}
 & (h,t) \models (\neg p_1)\,[evexp/\epsilon] \\
= & \quad \%\ \ Def.\ 25 \\
 & (h,t) \models \neg(p_1\,[evexp/\epsilon]) \\
= & \quad \%\ \ Def.\ 20 \\
 & not\ (h,t) \models p_1\,[evexp/\epsilon] \\
= & \quad \%\ \ Induction \\
 & not\ ((h : \epsilon \leadsto evexp), t) \models p_1 \\
= & \quad \%\ \ Def.\ 20 \\
 & ((h : \epsilon \leadsto evexp), t) \models \neg p_1
\end{array}
$$

- $p = p_1 \vee p_2$:

$$
\begin{array}{ll}
 & (h,t) \models (p_1 \vee p_2)\,[evexp/\epsilon] \\
= & \quad \%\ \ Def.\ 25 \\
 & (h,t) \models (p_1\,[evexp/\epsilon] \vee p_2\,[evexp/\epsilon]) \\
= & \quad \%\ \ Def.\ 20 \\
 & (h,t) \models p_1\,[evexp/\epsilon]\ \ or\ \ (h,t) \models p_2\,[evexp/\epsilon] \\
= & \quad \%\ \ Induction \\
 & ((h : \epsilon \leadsto evexp), t) \models p_1\ \ or\ \ ((h : \epsilon \leadsto evexp), t) \models p_2 \\
= & \quad \%\ \ Def.\ 20 \\
 & ((h : \epsilon \leadsto evexp), t) \models p_1 \vee p_2
\end{array}
$$

- $p = p_1\ \widehat{\mathcal{U}}\ p_2$:

$$
\begin{array}{ll}
 & (h,t) \models (p_1\ \widehat{\mathcal{U}}\ p_2)\,[evexp/\epsilon] \\
= & \quad \%\ \ Def.\ 25 \\
 & (h,t) \models (p_1\,[evexp/\epsilon]\ \ \widehat{\mathcal{U}}\ p_2\,[evexp/\epsilon]) \\
= & \quad \%\ \ Def.\ 20 \\
 & \exists t_0 > t : (h,t_0) \models p_2\,[evexp/\epsilon]\ \ and\ \forall t_1 \in (t,t_0) : (h,t_1) \models p_1\,[evexp/\epsilon] \\
= & \quad \%\ \ Induction \\
 & \exists t_0 > t : ((h : \epsilon \leadsto evexp), t_0) \models p_2 \\
 & and\ \forall t_1 \in (t,t_0) : ((h : \epsilon \leadsto evexp), t_1) \models p_1 \\
= & \quad \%\ \ Def.\ 20 \\
 & ((h : \epsilon \leadsto evexp), t) \models p_1\ \widehat{\mathcal{U}}\ p_2
\end{array}
$$

- $p = p_1 \ \widehat{\mathcal{S}} \ p_2$:

$$
\begin{array}{rl}
& (h,t) \models (p_1 \ \widehat{\mathcal{S}} \ p_2)\,[evexp/\epsilon] \\
= & \quad \%\ \ Def.\ 25 \\
& (h,t) \models (p_1\,[evexp/\epsilon] \ \widehat{\mathcal{S}} \ p_2\,[evexp/\epsilon]) \\
= & \quad \%\ \ Def.\ 20 \\
& \exists t_0 < t : (h,t_0) \models p_2\,[evexp/\epsilon] \ \ and\ \forall t_1 \in (t_0,t) : (h,t_1) \models p_1\,[evexp/\epsilon] \\
= & \quad \%\ \ Induction \\
& \exists t_0 < t : ((h : \epsilon \rightsquigarrow evexp), t_0) \models p_2 \\
& and\ \forall t_1 \in (t_0,t) : ((h : \epsilon \rightsquigarrow evexp), t_1) \models p_1 \\
= & \quad \%\ \ Def.\ 20 \\
& ((h : \epsilon \rightsquigarrow evexp), t) \models p_1 \ \widehat{\mathcal{S}} \ p_2
\end{array}
$$

- $p = \exists \mathrm{x}.p_1$:

$$
\begin{array}{rl}
& (h,t) \models (\exists \mathrm{x}.p_1)\,[evexp/\epsilon] \\
= & \quad \%\ \ Def.\ 25 \\
& (h,t) \models \exists \mathrm{x}.(p_1\,[evexp/\epsilon]) \\
= & \quad \%\ \ Def.\ 20 \\
& \exists h_1 : h_1\ \mathrm{x}\text{-}variant\ of\ h\ and\ (h_1,t) \models p_1\,[evexp/\epsilon] \\
= & \quad \%\ \ Induction \\
& \exists h_1 : h_1\ \mathrm{x}\text{-}variant\ of\ h\ and\ ((h_1 : \epsilon \rightsquigarrow evexp), t) \models p_1 \\
= & \quad \%\ \ h_2 = (h_1 : \epsilon \rightsquigarrow evexp), h_3 = (h : \epsilon \rightsquigarrow evexp) \\
& \qquad\quad h_1\ \mathrm{x}\text{-}variant\ of\ h\ iff\ h_2\ \mathrm{x}\text{-}variant\ of\ h_3 \\
& \exists h_2 : h_2\ \mathrm{x}\text{-}variant\ of\ h_3\ and\ (h_2,t) \models p_1 \\
= & \quad \%\ \ Def.\ 20 \\
& ((h : \epsilon \rightsquigarrow evexp), t) \models \exists \mathrm{x}.p_1
\end{array}
$$

- $p = \exists \epsilon_0.p_1$: *for* $\epsilon_0 \notin evar(evexp) \cup \{\epsilon\}$:

$$
\begin{array}{rl}
& (h,t) \models (\exists \epsilon_0.p_1)\,[evexp/\epsilon] \\
= & \quad \%\ \ Def.\ 25 \\
& (h,t) \models \exists \epsilon_0.(p_1\,[evexp/\epsilon]) \\
= & \quad \%\ \ Def.\ 20 \\
& \exists h_1 : h_1\ \epsilon_0\text{-}variant\ of\ h\ and\ (h_1,t) \models p_1\,[evexp/\epsilon] \\
= & \quad \%\ \ Induction \\
& \exists h_1 : h_1\ \epsilon_0\text{-}variant\ of\ h\ and\ ((h_1 : \epsilon \rightsquigarrow evexp), t) \models p_1 \\
= & \quad \%\ \ h_2 = (h_1 : \epsilon \rightsquigarrow evexp), h_3 = (h : \epsilon \rightsquigarrow evexp) \\
& \qquad\quad h_1\ \epsilon_0\text{-}variant\ of\ h\ iff\ h_2\ \epsilon_0\text{-}variant\ of\ h_3 \\
& \exists h_2 : h_2\ \epsilon_0\text{-}variant\ of\ h_3\ and\ (h_2,t) \models p_1 \\
= & \quad \%\ \ Def.\ 20 \\
& ((h : \epsilon \rightsquigarrow evexp), t) \models \exists \epsilon_0.p_1
\end{array}
$$

- $p = \exists n_0 . p_1$:

$$
\begin{array}{ll}
 & (h,t) \models (\exists n.p_1)\,[evexp/\epsilon] \\
= & \quad \%\ \ Def.\ 25 \\
 & (h,t) \models \exists n.(p_1\,[evexp/\epsilon]) \\
= & \quad \%\ \ Def.\ 20 \\
 & \exists h_1 : h_1 \textit{ n-variant of } h \textit{ and } (h_1,t) \models p_1\,[evexp/\epsilon] \\
= & \quad \%\ \ Induction \\
 & \exists h_1 : h_1 \textit{ n-variant of } h \textit{ and } ((h_1 : \epsilon \rightsquigarrow evexp),t) \models p_1 \\
= & \quad \%\ \ h_2 = (h_1 : \epsilon \rightsquigarrow evexp), h_3 = (h : \epsilon \rightsquigarrow evexp) \\
 & \qquad h_1 \textit{ n-variant of } h\ iff\ h_2 \textit{ n-variant of } h_3 \\
 & \exists h_2 : h_2 \textit{ n-variant of } h_3 \textit{ and } (h_2,t) \models p_1 \\
= & \quad \%\ \ Def.\ 20 \\
 & ((h : \epsilon \rightsquigarrow evexp),t) \models \exists n.p_1
\end{array}
$$

A.5 Proof of Lemma 3

Lemma 3
Given a machine in DTL $(B, \mathrm{I} \wedge \Box \mathrm{T})$ *then there exists a semantic machine* $M = (B, I, T)$ *such that* $Comp(M) = Hist(\mathrm{I} \wedge \Box \mathrm{T})$.

Proof 19
Let $I \triangleq \{\sigma \in \Sigma \mid \exists h : \sigma = \theta_h(0) \wedge h \models \mathrm{I}\}$ *and*
let $T \triangleq \{\langle \delta, \sigma_0, \sigma_1 \rangle \in \Delta \times \Sigma^2 \mid \exists h : \exists t : Step_h(t) = \langle \delta, \sigma_0, \sigma_1 \rangle \wedge Step_h(t) \notin STU \wedge h \models \Box \mathrm{T}\}$
then $Hist(\mathrm{I} \wedge \Box \mathrm{T}) = Comp(M)$. *Proof:*

$$
\begin{array}{ll}
 & Hist(\mathrm{I} \wedge \Box \mathrm{T}) \\
= & \quad \%\ \ Def.\ 21 \\
 & \{h \in \mathcal{H} \mid h \models \mathrm{I} \wedge \Box \mathrm{T}\} \\
= & \quad \%\ \ Def.\ 20 \\
 & \{h \in \mathcal{H} \mid h \models \mathrm{I} \wedge \forall t : (h,t) \models \mathrm{T}\} \\
= & \quad \%\ \ Def.\ 28,\ \ def.\ of\ \ I\ and\ T \\
 & \{h \in \mathcal{H} \mid \theta_h(0) \in I \wedge \forall t : Step_h(t) \in \mathrm{STU} \vee Step_h(t) \in T\} \\
= & \quad \%\ \ Def.\ 16 \\
 & Comp(M)
\end{array}
$$

A.6 Proof of Lemma 4

Lemma 4
Given DTL machine specification of a system $(B, \mathrm{I} \wedge \Box \mathrm{T} \wedge \mathrm{L})$ *then there exists a semantic machine specification* $\mathcal{S} = (B, Comp(M) \cap L)$ *such that* $Comp(M) \cap L = Hist(\mathrm{I} \wedge \Box \mathrm{T} \wedge \mathrm{L})$.

Proof 20
Let $I \triangleq \{\sigma \in \Sigma \mid \exists h : \sigma = \theta_h(0) \wedge h \models \mathrm{I}\}$ *and*
let $T \triangleq \{\langle \delta, \sigma_0, \sigma_1 \rangle \in \Delta \times \Sigma^2 \mid \exists h : \exists t : Step_h(t) = \langle \delta, \sigma_0, \sigma_1 \rangle \wedge Step_h(t) \notin STU \wedge h \models \Box \mathrm{T}\}$

and
let $L \triangleq Hist(\mathrm{L})$ *then* $Hist(\mathrm{I} \wedge \Box\mathrm{T} \wedge \mathrm{L}) = Comp(M) \cap L$. *Because of machine closedness* $cl(Comp(M) \cap Hist(\mathrm{L})) = Comp(M)$. *Proof:*

$$
\begin{array}{ll}
 & Hist(\mathrm{I} \wedge \Box\mathrm{T} \wedge \mathrm{L}) \\
= & \quad \%\ \ Def.\ 21 \\
 & \{h \in \mathcal{H} \mid h \models \mathrm{I} \wedge \Box\mathrm{T}\} \cap Hist(\mathrm{L}) \\
= & \quad \%\ \ Def.\ 20 \\
 & \{h \in \mathcal{H} \mid h \models \mathrm{I} \wedge \forall t : (h,t) \models \mathrm{T}\} \cap Hist(\mathrm{L}) \\
= & \quad \%\ \ Def.\ 28,\ \ \mathit{def.\ of}\ \ I,\ T\ \mathit{and}\ L \\
 & \{h \in \mathcal{H} \mid \theta_h(0) \in I \wedge \forall t : Step_h(t) \in \mathrm{STU} \vee Step_h(t) \in T\} \cap L \\
= & \quad \%\ \ Def.\ 16 \\
 & Comp(M) \cap L
\end{array}
$$

A.7 Proof of Lemma 5

Lemma 5 (Properties of $\mathcal{O}$ and $\otimes$)
Given systems (B_1, H_0), (B_1, H_1), (B_2, H_2) *and* (B_2, H_3) *then*

$$
\begin{array}{ll}
(a) & H_0 \subseteq H_1 \ \mathit{implies}\ H_0 \otimes H_2 \subseteq H_1 \otimes H_2 \\
(b) & \mathcal{O}_{\mathrm{X}_{12}}(H_1 \otimes H_2) = \mathcal{O}_{\mathrm{X}_1}(H_1) \otimes \mathcal{O}_{\mathrm{X}_2}(H_2) \\
(c) & H_0 \subseteq H_1 \ \mathit{implies}\ \mathcal{O}_{\mathrm{X}_1}(H_0) \subseteq \mathcal{O}_{\mathrm{X}_1}(H_1) \\
(d) & (H_0 \cap H_1) \otimes (H_2 \cap H_3) \subseteq (H_0 \otimes H_2) \cap (H_1 \otimes H_3)
\end{array}
$$

Proof 21

$$(a) \quad H_0 \subseteq H_1 \ \mathit{implies}\ H_0 \otimes H_2 \subseteq H_1 \otimes H_2$$

$$
\begin{array}{ll}
 & h \in H_0 \otimes H_2 \\
= & \quad \%\ \ Def.\ 32 \\
 & \exists h_1 \in H_0, h_2 \in H_2. \otimes (h, h_1, h_2) \\
\rightarrow & \quad \%\ \ H_0 \subseteq H_1 \\
 & \exists h_1 \in H_1, h_2 \in H_2. \otimes (h, h_1, h_2) \\
= & \quad \%\ \ Def.\ 32 \\
 & h \in H_1 \otimes H_2
\end{array}
$$

$$(b) \quad \mathcal{O}_{\mathrm{X}_{12}}(H_1 \otimes H_2) = \mathcal{O}_{\mathrm{X}_1}(H_1) \otimes \mathcal{O}_{\mathrm{X}_2}(H_2)$$

$$
\begin{array}{ll}
 & h \in \mathcal{O}_{\mathrm{X}_{12}}(H_1 \bigotimes H_2) \\
= & \quad \%\ \ Def.\ 30 \\
 & \exists h_3 \in H_1 \bigotimes H_2 : h\ \mathrm{X}_1 \cup \mathrm{X}_2\text{-}variant\ \ of\ h_3 \\
= & \quad \%\ \ Def.\ 32 \\
 & \exists h_1, h_2, h_3 : h_1 \in Obs_1 \wedge h_2 \in Obs_2 \wedge \otimes(h_3, h_1, h_2) \\
 & \wedge h\ \mathrm{X}_1 \cup \mathrm{X}_2\text{-}variant\ \ of\ h_3 \\
= & \quad \%\ \ \psi = \psi_3, \psi_4 = \psi_1, \psi_5 = \psi_2 \\
 & \qquad \theta|^2_{(\mathfrak{Y}\cup\mathfrak{X})\setminus(\mathrm{X}_1\cup\mathrm{X}_2)} = \theta_3|^2_{(\mathfrak{Y}\cup\mathfrak{X})\setminus(\mathrm{X}_1\cup\mathrm{X}_2)}, \\
 & \qquad \theta_4|^2_{(\mathfrak{Y}\cup\mathfrak{X})\setminus\mathrm{X}_1} = \theta_1|^2_{(\mathfrak{Y}\cup\mathfrak{X})\setminus\mathrm{X}_1}, \\
 & \qquad \theta_5|^2_{(\mathfrak{Y}\cup\mathfrak{X})\setminus\mathrm{X}_2} = \theta_2|^2_{(\mathfrak{Y}\cup\mathfrak{X})\setminus\mathrm{X}_2} \\
 & \qquad \theta_3 = \theta_1 = \theta_2, \theta = \theta_4 = \theta_5 \\
 & \exists h_1, h_2, h_4, h_5 : h_1 \in H_1 \wedge h_2 \in H_2 \wedge \otimes(h, h_4, h_5) \\
 & h_4\ \mathrm{X}_1\text{-}variant\ \ of\ h_1 \wedge h_5\ \mathrm{X}_2\text{-}variant\ \ of\ h_2 \\
= & \quad \%\ \ Def.\ 30 \\
 & \exists h_4 \in \mathcal{O}_{\mathrm{X}_1}(H_1), h_5 \in \mathcal{O}_{\mathrm{X}_2}(H_2) : \otimes(h, h_4, h_5) \\
= & \quad \%\ \ Def.\ 32 \\
 & h \in \mathcal{O}_{\mathrm{X}_1}(H_1) \bigotimes \mathcal{O}_{\mathrm{X}_2}(H_2)
\end{array}
$$

(c) $\quad H_0 \subseteq H_1$ *implies* $\mathcal{O}_{\mathrm{X}_1}(H_0) \subseteq \mathcal{O}_{\mathrm{X}_1}(H_1)$

$$
\begin{array}{ll}
 & h \in \mathcal{O}_{\mathrm{X}_1}(H_0) \\
= & \quad \%\ \ Def.\ 30 \\
 & \exists h_1 : h_1 \in H_0 \wedge h\ \mathrm{X}_1\text{-}variant\ \ of\ h_1 \\
\rightarrow & \quad \%\ \ H_0 \subseteq H_1 \\
 & \exists h_1 : h_1 \in H_1 \wedge h\ \mathrm{X}_1\text{-}variant\ \ of\ h_1 \\
= & \quad \%\ \ Def.\ 30 \\
 & h \in \mathcal{O}_{\mathrm{X}_1}(H_1)
\end{array}
$$

(d) $\quad (H_0 \cap H_1) \bigotimes (H_2 \cap H_3) \subseteq (H_0 \bigotimes H_2) \cap (H_1 \bigotimes H_3)$

$$
\begin{array}{ll}
 & h \in (H_0 \cap H_1) \bigotimes (H_2 \cap H_3) \\
= & \quad \%\ \ Def.\ 32 \\
 & \exists h_1, h_2 : h_1 \in (H_0 \cap H_1) \wedge h_2 \in (H_2 \cap H_3) \wedge \otimes(h, h_1, h_2) \\
\rightarrow & \quad \%\ \ Calculus \\
 & \exists h_1, h_2 : h_1 \in H_0 \wedge h_2 \in H_2 \wedge \otimes(h, h_1, h_2) \\
 & \wedge \exists h_1, h_2 : h_1 \in H_1 \wedge h_2 \in H_3 \wedge \otimes(h, h_1, h_2) \\
= & \quad \%\ \ Def.\ 32 \\
 & h \in H_0 \bigotimes H_2 \wedge h \in H_1 \bigotimes H_3
\end{array}
$$

A.8 Proof of Theorem 3

Theorem 3 (Compositional refinement)
Given concrete systems $\mathcal{S}_i = (B_i, H_i)$ $(i = 1, 2)$ *and abstract systems* $\mathcal{S}_j = (B_j, H_j)$ $(j = 3, 4)$ *such that* $\mathfrak{D}(B_1) = \mathfrak{D}(B_3)$ *and* $\mathfrak{D}(B_2) = \mathfrak{D}(B_4)$ *then* $\mathcal{S}_1$ **ref** $\mathcal{S}_3$ *and* $\mathcal{S}_2$ **ref** $\mathcal{S}_4$ *implies* $\mathcal{S}_1 \parallel \mathcal{S}_2$ **ref** $\mathcal{S}_3 \parallel \mathcal{S}_4$.

Proof 22

$$
\begin{array}{ll}
 & \mathcal{S}_1 \parallel \mathcal{S}_2 \ \mathbf{ref}\ \mathcal{S}_3 \parallel \mathcal{S}_4 \\
= & \quad \%\ \ \mathit{Def.}\ 31, 32, \mathfrak{D}(B_1) = \mathfrak{D}(B_3), \mathfrak{D}(B_2) = \mathfrak{D}(B_4) \\
 & \mathcal{O}_{\mathrm{X}_{12}}(H_1 \otimes H_2) \subseteq \mathcal{O}_{\mathrm{X}_{34}}(H_3 \otimes H_4) \\
= & \quad \%\ \ \mathit{Lemma}\ 5(b) \\
 & \mathcal{O}_{\mathrm{X}_1}(H_1) \otimes \mathcal{O}_{\mathrm{X}_2}(H_2) \subseteq \mathcal{O}_{\mathrm{X}_3}(H_3) \otimes \mathcal{O}_{\mathrm{X}_4}(H_4) \\
= & \quad \%\ \ \mathcal{O}_{\mathrm{X}_1}(H_1) \subseteq \mathcal{O}_{\mathrm{X}_3}(H_3)\ \mathit{with\ Lemma}\ 5(a)\ \mathit{gives} \\
 & \qquad\quad \mathcal{O}_{\mathrm{X}_1}(H_1) \otimes \mathcal{O}_{\mathrm{X}_2}(H_2) \subseteq \mathcal{O}_{\mathrm{X}_3}(H_3) \otimes \mathcal{O}_{\mathrm{X}_2}(H_2) \\
 & \qquad\quad \mathcal{O}_{\mathrm{X}_2}(H_2) \subseteq \mathcal{O}_{\mathrm{X}_4}(H_4)\ \mathit{with\ Lemma}\ 5(a)\ \mathit{gives} \\
 & \qquad\quad \mathcal{O}_{\mathrm{X}_3}(H_3) \otimes \mathcal{O}_{\mathrm{X}_2}(H_2) \subseteq \mathcal{O}_{\mathrm{X}_3}(H_3) \otimes \mathcal{O}_{\mathrm{X}_4}(H_4) \\
 & \mathit{true}
\end{array}
$$

A.9 Proof of Lemma 6

Lemma 6
Given DTL machine specification $\mathcal{S} = (B, \mathrm{I} \wedge \Box\mathrm{T} \wedge \mathrm{L})$ *then* $\mathcal{O}_{\mathrm{X}}(\mathit{Hist}(\mathrm{I} \wedge \Box\mathrm{T} \wedge \mathrm{L})) = \mathit{Hist}((\exists \mathrm{X} \,.\, (\mathrm{I} \wedge \Box\mathrm{T} \wedge \mathrm{L})))$

Proof 23

$$
\begin{array}{ll}
 & \mathit{Hist}((\exists \mathrm{X} \,.\, (\mathrm{I} \wedge \Box\mathrm{T} \wedge \mathrm{L}))) \\
= & \quad \%\ \ \mathit{Def.}\ 21 \\
 & \{h \mid h \models (\exists \mathrm{X} \,.\, (\mathrm{I} \wedge \Box\mathrm{T} \wedge \mathrm{L}))\} \\
= & \quad \%\ \ \mathit{Def.}\ 20 \\
 & \{h \mid \exists h_1 : h_1\ \mathrm{X}\text{-}\mathit{variant\ of}\ h \wedge h_1 \models \mathrm{I} \wedge \Box\mathrm{T} \wedge \mathrm{L}\} \\
= & \quad \%\ \ \mathit{Def.}\ 21 \\
 & \{h \mid \exists h_1 : h_1\ \mathrm{X}\text{-}\mathit{variant\ of}\ h \wedge h_1 \in \mathit{Hist}(\mathrm{I} \wedge \Box\mathrm{T} \wedge \mathrm{L})\} \\
= & \quad \%\ \ \mathit{Def.}\ 30 \\
 & \mathcal{O}_{\mathrm{X}}(\mathit{Hist}(\mathrm{I} \wedge \Box\mathrm{T} \wedge \mathrm{L}))
\end{array}
$$

A.10 Proof of Theorem 4

Theorem 4 (Refinement of machine specifications)
Given concrete machine specification $\mathcal{S}_c \triangleq (B_c, \mathrm{I}_c \wedge \Box\mathrm{T}_c \wedge \mathrm{L}_c)$ *where* $B_c \triangleq (B_c^P, (\mathrm{V}_c, \mathrm{X}_c))$ *and abstract machine specification* $\mathcal{S}_a \triangleq (B_a, \mathrm{I}_a \wedge \Box\mathrm{T}_a \wedge \mathrm{L}_a)$ *where* $B_a \triangleq (B_a^P, (\mathrm{V}_a, \mathrm{X}_a))$. *Then* $\mathcal{S}_c$ **refines** $\mathcal{S}_a$ *denoted* $\mathcal{S}_c$ **ref** $\mathcal{S}_a$ *iff*

$$
\begin{array}{l}
\mathfrak{D}(B_c) = \mathfrak{D}(B_a)\ \mathit{and} \\
(\exists \mathrm{X}_c \,.\, (\mathrm{I}_c \wedge \Box\mathrm{T}_c \wedge \mathrm{L}_c)) \ \rightarrow (\exists \mathrm{X}_a \,.\, (\mathrm{I}_a \wedge \Box\mathrm{T}_a \wedge \mathrm{L}_a))
\end{array}
$$

Proof 24

$$
\begin{array}{rl}
& \mathcal{S}_c \textbf{ ref } \mathcal{S}_a \\
= & \quad \% \;\; \mathit{Def.}\ 31 \\
& \mathfrak{O}(B_c) = \mathfrak{O}(B_a) \\
& \mathcal{O}_{\mathrm{X}_c}(\mathit{Hist}(\mathrm{I}_c \wedge \Box\mathrm{T}_c \wedge \mathrm{L}_c)) \subseteq \mathcal{O}_{\mathrm{X}_a}(\mathit{Hist}(\mathrm{I}_a \wedge \Box\mathrm{T}_a \wedge \mathrm{L}_a)) \\
= & \quad \% \;\; \mathit{Lemma}\ 6 \\
& \mathfrak{O}(B_c) = \mathfrak{O}(B_a) \\
& \mathit{Hist}((\exists \mathrm{X}_c\,.\,(\mathrm{I}_c \wedge \Box\mathrm{T}_c \wedge \mathrm{L}_c))) \subseteq \mathit{Hist}((\exists \mathrm{X}_a\,.\,(\mathrm{I}_a \wedge \Box\mathrm{T}_a \wedge \mathrm{L}_a))) \\
= & \quad \% \;\; \mathit{Def.}\ 20 \mathit{\ and\ } 21 \\
& \mathfrak{O}(B_c) = \mathfrak{O}(B_a) \\
& \models (\exists \mathrm{X}_c\,.\,(\mathrm{I}_c \wedge \Box\mathrm{T}_c \wedge \mathrm{L}_c)) \rightarrow (\exists \mathrm{X}_a\,.\,(\mathrm{I}_a \wedge \Box\mathrm{T}_a \wedge \mathrm{L}_a))
\end{array}
$$

A.11 Proof of Theorem 5

Theorem 5 (Semantic merge is almost conjunction)
Given machine system specifications $(B_i, \mathrm{I}_i \wedge \Box\mathrm{T}_i \wedge \mathrm{L}_i)$ *where* $B_i \triangleq ((\mathrm{In}_i, \mathrm{Out}_i), (\mathrm{V}_i, \mathrm{X}_i))$, *for* $i = 1, 2$ *and composed machine system specification as in definition 35, i.e.,* (B, H) *where* $\mathrm{H} \triangleq \exists \epsilon_1, \epsilon_2 . _{B_1^A} \odot_{B_2^A} (\epsilon, \epsilon_1, \epsilon_2) \wedge (\mathrm{I}_1 \wedge \Box\mathrm{T}_1 \wedge \mathrm{L}_1)\,[\epsilon_1/\epsilon] \wedge (\mathrm{I}_2 \wedge \Box\mathrm{T}_2 \wedge \mathrm{L}_2)\,[\epsilon_2/\epsilon]$ *and* $B \triangleq ((\mathrm{In}_1 \setminus \mathrm{Out}_2 \cup \mathrm{In}_2 \setminus \mathrm{Out}_1, \mathrm{Out}_1 \setminus \mathrm{In}_2 \cup \mathrm{Out}_2 \setminus \mathrm{In}_1), (\mathrm{V}_1 \cup \mathrm{V}_2, \mathrm{X}_1 \cup \mathrm{X}_2))$ *then*

$$
\mathit{Hist}(\mathrm{I}_1 \wedge \Box\mathrm{T}_1 \wedge \mathrm{L}_1) \bigotimes \mathit{Hist}(\mathrm{I}_2 \wedge \Box\mathrm{T}_2 \wedge \mathrm{L}_2) = \mathit{Hist}(\mathrm{H})
$$

Proof 25

$$
\begin{array}{rl}
& h \in \mathit{Hist}(\mathrm{H}) \\
= & \quad \% \;\; \mathit{Def.}\ 20 \\
& \exists h_1 : h_1\{\epsilon_1, \epsilon_2\}\text{-}\mathit{variant\ of\ } h \wedge \\
& h_1 \models {}_{B_1^A} \odot_{B_2^A} (\epsilon, \epsilon_1, \epsilon_2) \wedge (\mathrm{I}_1 \wedge \Box\mathrm{T}_1 \wedge \mathrm{L}_1)\,[\epsilon_1/\epsilon] \wedge (\mathrm{I}_2 \wedge \Box\mathrm{T}_2 \wedge \mathrm{L}_2)\,[\epsilon_2/\epsilon] \\
= & \quad \% \;\; \mathit{Def.}\ 20 \mathit{\ and\ } 25 \\
& \exists h_1 : h_1\{\epsilon_1, \epsilon_2\}\text{-}\mathit{variant\ of\ } h \wedge \\
& h_1 \models {}_{B_1^A} \odot_{B_2^A} (\epsilon, \epsilon_1, \epsilon_2) \wedge \\
& (h : \epsilon \rightsquigarrow \epsilon_1) \models \mathrm{I}_1 \wedge \Box\mathrm{T}_1 \wedge \mathrm{L}_1 \wedge \\
& (h : \epsilon \rightsquigarrow \epsilon_2) \models \mathrm{I}_2 \wedge \Box\mathrm{T}_2 \wedge \mathrm{L}_2 \\
= & \quad \% \;\; \theta_1 = \theta, h_3 = (h_1 : \epsilon \rightsquigarrow \epsilon_1), h_4 = (h_1 : \epsilon \rightsquigarrow \epsilon_2), \\
& \qquad \psi_1(t)(\epsilon) = \psi(t)(\epsilon), \psi_1(t)(\epsilon_1) = \psi_3(t)(\epsilon), \psi_1(t)(\epsilon_2) = \psi_4(t)(\epsilon) \\
& \qquad \mathit{i.e.,}\ h_1\{\epsilon_1, \epsilon_2\}\text{-}\mathit{variant\ of\ } h \wedge h_1 \models {}_{B_1^A} \odot_{B_2^A} (\epsilon, \epsilon_1, \epsilon_2) \mathit{\ iff\ } \otimes (h, h_3, h_4) \\
& \exists h_3, h_4 : h_3 \models \mathrm{I}_1 \wedge \Box\mathrm{T}_1 \wedge \mathrm{L}_1 \wedge \\
& h_4 \models \mathrm{I}_2 \wedge \Box\mathrm{T}_2 \wedge \mathrm{L}_2 \wedge \\
& \otimes(h, h_3, h_4) \\
= & \quad \% \;\; \mathit{Def.}\ 21 \\
& h \in \mathit{Hist}(\mathrm{I}_1 \wedge \Box\mathrm{T}_1 \wedge \mathrm{L}_1) \bigotimes \mathit{Hist}(\mathrm{I}_2 \wedge \Box\mathrm{T}_2 \wedge \mathrm{L}_2)
\end{array}
$$

A.12 Proof of Theorem 6

Theorem 6
Given machine specification $\mathcal{S} \triangleq (B, \mathrm{H})$ *and given set of shared variables* $\mathrm{V}_1 \subseteq \mathrm{V}$ *then*

$$Enc_{\mathrm{V}_1}(Hist(\mathrm{H})) = Hist(\mathrm{H} \wedge (\epsilon = \mathbf{e} \Rightarrow \mathrm{V}_1' = \mathrm{V}_1))$$

Proof 26

$$\begin{array}{ll}
 & h \in Enc_{\mathrm{V}_1}(Hist(\mathrm{H})) \\
= & \quad \%\ \ Def.\ 33 \\
 & h \in Hist(\mathrm{H}) \wedge \forall t : \psi(t)(\epsilon) = \mathbf{e} \rightarrow \theta(t)|_{\mathrm{V}_1}^1 = \lim_{t \leftarrow t_1} \theta(t_1)|_{\mathrm{V}_1}^1 \\
= & \quad \%\ \ Semantics.\ of\ (\epsilon = \mathbf{e} \Rightarrow \mathrm{V}_1' = \mathrm{V}_1) \\
 & h \in Hist(\mathrm{H}) \wedge h \in Hist(\epsilon = \mathbf{e} \Rightarrow \mathrm{V}_1' = \mathrm{V}_1) \\
= & \quad \%\ \ Calculus \\
 & h \in Hist(\mathrm{H} \wedge (\epsilon = \mathbf{e} \Rightarrow \mathrm{V}_1' = \mathrm{V}_1))
\end{array}$$

A.13 Proof of Lemma 7

Lemma 7
Given concrete system $\mathcal{S}_c \triangleq (B_c, H_c)$ *and abstract system* $\mathcal{S}_a \triangleq (B_a, H_a)$ *s.t.* $\mathfrak{D}(B_c) = \mathfrak{D}(B_a)$*. If there exists a refinement mapping from* $\mathcal{S}_c$ *to* $\mathcal{S}_a$*, then* $\mathcal{S}_c$ **ref** $\mathcal{S}_a$*.*

Proof 27

$$\begin{array}{ll}
 & \mathcal{S}_c\ \mathbf{ref}\ \mathcal{S}_a \\
= & \quad \%\ \ Def.\ 31 \\
 & \mathfrak{D}(B_c) = \mathfrak{D}(B_a)\ and \\
 & \mathcal{O}_{\mathrm{X}_c}(H_c) \subseteq \mathcal{O}_{\mathrm{X}_a}(H_a) \\
\leftarrow & \quad \%\ \ \mathfrak{D}(B_c) = \mathfrak{D}(B_a) \\
 & \mathcal{O}_{\mathrm{X}_c}(H_c) \subseteq \mathcal{O}_{\mathrm{X}_a}(H_a) \\
\leftarrow & \quad \%\ \ Def.\ 37,\ i.e.\ \mathcal{O}_{\mathrm{X}_a}(f(H_c)) \subseteq \mathcal{O}_{\mathrm{X}_a}(H_a), \mathcal{O}_{\mathrm{X}_c}(H_c) = \mathcal{O}_{\mathrm{X}_a}(f(H_c)) \\
 & true
\end{array}$$

A.14 Proof of Lemma 8

Lemma 8
Given concrete machine specification $\mathcal{S}_c \triangleq (B_c, Comp(M_c) \cap L_c)$ *and given abstract machine specification* $\mathcal{S}_a \triangleq (B_a, Comp(M_a) \cap L_a)$ *s.t.* $\mathfrak{D}(B_c) = \mathfrak{D}(B_a)$*. If there exists a refinement mapping from* $\mathcal{S}_c$ *to* $\mathcal{S}_a$ *then* $\mathcal{S}_c$ **ref** $\mathcal{S}_a$*.*

Proof 28
We first prove the following result:

For all $h_c \in Comp(M_c)$, *there exists a* $h_a \in Comp(M_a)$ *s.t. for all* $t \in \mathbb{R}^{\geq 0}$, $\langle \psi_c(t), \theta_c(t) \rangle = \langle \psi_a(t), \theta(t)_a \rangle$ *and* $f(\theta_c(t)) = \theta_a(t)$.

$$
\begin{array}{ll}
 & h_c \in Comp(M_c) \\
= & \quad \% \quad Def.\ 16 \\
 & \theta_c(0) \in I_c \wedge \\
 & \forall t : \langle \psi_c(t), \theta_c(t), \lim\limits_{t \leftarrow t_1} \theta_c(t_1) \rangle \in T_c \vee (\psi_c(t)(\epsilon) \in \{\lambda, \mathbf{i}, \mathbf{e}\} \wedge \theta_c(t) = \lim\limits_{t \leftarrow t_1} \theta_c(t_1)) \\
\rightarrow & \quad \% \quad Def.\ 38 \\
 & f(\theta_c(0)) \in I_a \\
 & \wedge \forall t : \langle \psi_a(t), f(\theta_c(t)), \lim\limits_{t \leftarrow t_1} f(\theta_c(t_1)) \rangle \in T_a \vee \\
 & \ (\psi_a(t)(\epsilon) \in \{\lambda, \mathbf{i}, \mathbf{e}\} \wedge f(\theta_c(t)) = \lim\limits_{t \leftarrow t_1} f(\theta_c(t_1))) \\
= & \quad \% \quad Def.\ 16 \\
 & h_a \in Comp(M_a) \wedge \forall t : \langle \psi_c(t), \theta_c(t) \rangle = \langle \psi_a(t), \theta(t)_a \rangle \wedge f(\theta_c(t)) = \theta_a(t)
\end{array}
$$

The proof of Lemma 8 is then as follows:

$$
\begin{array}{lll}
 & \mathcal{S}_c \ \mathbf{ref} \ \mathcal{S}_a & \\
= & \quad \% \quad Def.\ 31 & \\
 & \mathfrak{O}(B_c) = \mathfrak{O}(B_a) \ and & \\
 & \mathcal{O}_{\mathrm{X}_c}(Comp(M_c) \cap L_c) \subseteq \mathcal{O}_{\mathrm{X}_a}(Comp(M_a) \cap L_a) & \\
= & \quad \% \quad \mathfrak{O}(B_c) = \mathfrak{O}(B_a) & \\
 & \mathcal{O}_{\mathrm{X}_c}(Comp(M_c) \cap L_c) \subseteq \mathcal{O}_{\mathrm{X}_a}(Comp(M_a) \cap L_a) & \\
\leftarrow & \quad \% \quad From\ Def.\ 37, f(Comp(M_c) \cap L_c) \subseteq L_a & \\
 & \qquad Property\ of\ f, f(Comp(M_c) \cap L_c) \subseteq f(Comp(M_c)), & \\
 & \qquad by\ above\ result,\ f(Comp(M_c)) \subseteq Comp(M_a), & \\
 & \qquad Resulting\ in\ , f(Comp(M_c) \cap L_c) \subseteq Comp(M_a) \cap L_a & \\
 & \qquad From\ Lemma\ 5(c), \mathcal{O}_{\mathrm{X}_a}(f(Comp(M_c) \cap L_c)) \subseteq \mathcal{O}_{\mathrm{X}_a}(Comp(M_a) \cap L_a), & \\
 & \qquad From\ Def.\ 37, \mathcal{O}_{\mathrm{X}_c}(Comp(M_c) \cap L_c) = \mathcal{O}_{\mathrm{X}_a}(f(Comp(M_c) \cap L_c)) & \\
 & true &
\end{array}
$$

A.15 Proof of Theorem 7

Theorem 7 (Compositional relative refinement)
Given concrete systems $\mathcal{S}_i = (B_i, H_i)$ $(i = 1, 2)$ *and given set* W_c *constraining* B_{12} *(the basis of* $\mathcal{S}_1 \parallel \mathcal{S}_2$*). And given abstract systems* $\mathcal{S}_j = (B_j, H_j)$ $(j = 3, 4)$ *and given set* W_a *constraining* B_{34} *(the basis of* $\mathcal{S}_3 \parallel \mathcal{S}_4$*). Then the following holds:*

$$
\begin{array}{ll}
H_1 \bigotimes H_2 \cap W_{c1} \bigotimes W_{c2} \subseteq (H_1 \cap W_{c1}) \bigotimes (H_2 \cap W_{c2}) & \\
W_c \subseteq W_{c1} \bigotimes W_{c2} & \\
W_{a3} \bigotimes W_{a4} \subseteq W_a & W_{ci}\ constraining\ B_i\ (i{=}1{,}2) \\
\mathcal{S}_1 \ {}_{W_{c1}}\mathbf{ref}^{W_{a3}} \ \mathcal{S}_3 & W_{aj}\ constraining\ B_j\ (j{=}3{,}4) \\
\mathcal{S}_2 \ {}_{W_{c2}}\mathbf{ref}^{W_{a4}} \ \mathcal{S}_4 & \\
\hline
\mathcal{S}_1 \parallel \mathcal{S}_2 \ {}_{W_c}\mathbf{ref}^{W_a} \ \mathcal{S}_3 \parallel \mathcal{S}_4 &
\end{array}
$$

Proof 29
Assume agreement on the bases. Then according to Def. 39 and 40 we must infer from the assumptions that $\mathcal{O}_{X_{12}}(H_1 \bigotimes H_2 \cap W_c) \subseteq \mathcal{O}_{X_{34}}(H_3 \bigotimes H_4 \cap W_a)$.

$$
\begin{array}{ll}
 & \mathcal{O}_{X_{12}}(H_1 \bigotimes H_2 \cap W_c) \\
\subseteq & \quad \% \ H_1 \bigotimes H_2 \cap W_{c1} \bigotimes W_{c2} \subseteq (H_1 \cap W_{c1}) \bigotimes (H_2 \cap W_{c2}) \\
 & \quad \ W_c \subseteq W_{c1} \bigotimes W_{c2} \\
 & \quad \ \mathit{Lemma}\ 5(c) \\
 & \mathcal{O}_{X_{12}}((H_1 \cap W_{c1}) \bigotimes (H_2 \cap W_{c2})) \\
\subseteq & \quad \% \ \mathcal{S}_1 \ {}_{W_{c1}}\mathbf{ref}^{W_{a3}} \ \mathcal{S}_3 \\
 & \quad \ \mathcal{S}_2 \ {}_{W_{c2}}\mathbf{ref}^{W_{a4}} \ \mathcal{S}_4 \\
 & \quad \ \mathit{Lemma}\ 5(a),(b) \\
 & \mathcal{O}_{X_{34}}((H_3 \cap W_{a3}) \bigotimes (H_4 \cap W_{a4})) \\
\subseteq & \quad \% \ \mathit{Lemma}\ 5(c),(d) \\
 & \mathcal{O}_{X_{34}}(H_3 \bigotimes H_4 \cap W_{a3} \bigotimes W_{a4}) \\
\subseteq & \quad \% \ W_{a3} \bigotimes W_{a4} \subseteq W_a \\
 & \quad \ \mathit{Lemma}\ 5(c) \\
 & \mathcal{O}_{X_{34}}(H_3 \bigotimes H_4 \cap W_a)
\end{array}
$$

A.16 Proof of Lemma 9

Lemma 9
Given systems $\mathcal{S}_i = (B_i, H_i)$ *and sets* W_i *constraining* B_i $(i = 1, 2)$ *with no restrictions on the event variables. Then the following holds:*

$$(H_1 \cap W_1) \bigotimes (H_2 \cap W_2) = H_1 \bigotimes H_2 \cap W_1 \bigotimes W_2$$

Proof 30
From Lemma 5(d) we infer $(H_1 \cap W_1) \bigotimes (H_2 \cap W_2) \subseteq H_1 \bigotimes H_2 \cap W_1 \bigotimes W_2$ *so we must prove* $H_1 \bigotimes H_2 \cap W_1 \bigotimes W_2 \subseteq (H_1 \cap W_1) \bigotimes (H_2 \cap W_2)$.

$$
\begin{array}{ll}
 & h \in H_1 \bigotimes H_2 \cap W_1 \bigotimes W_2 \\
= & \quad \% \ \mathit{Def}.32 \\
 & \exists h_1, h_2 : h_1 \in H_1 \wedge h_2 \in H_2 \wedge \otimes(h, h_1, h_2) \\
 & \wedge \exists h_3, h_4 : h_3 \in W_1 \wedge h_4 \in W_2 \wedge \otimes(h, h_3, h_4) \\
\rightarrow & \quad \% \ W_i \ \textit{puts no restriction on } \epsilon \textit{ variables}, \theta = \theta_3 = \theta_4 \\
 & \exists h_1, h_2 : h_1 \in H_1 \wedge h_2 \in H_2 \wedge \otimes(h, h_1, h_2) \\
 & \wedge h \in W_1 \wedge h \in W_2 \\
= & \quad \% \ \mathit{Calc}. \\
 & \exists h_1, h_2 : h_1 \in H_1 \wedge h_2 \in H_2 \wedge h \in W_1 \wedge h \in W_2 \wedge \otimes(h, h_1, h_2) \\
\rightarrow & \quad \% \ W_i \ \textit{puts no restriction on } \epsilon \textit{ variables}, \theta = \theta_1 = \theta_2, \\
 & \quad \ W_i \ \textit{constrains } B_i \\
 & \exists h_1, h_2 : h_1 \in H_1 \cap W_1 \wedge h_2 \in H_2 \cap W_2 \wedge \otimes(h, h_1, h_2) \\
= & \quad \% \ \mathit{Def}.\ 32 \\
 & h \in (H_1 \cap W_1) \bigotimes (H_2 \cap W_2)
\end{array}
$$

A.17 Proof of Lemma 10

Lemma 10
Given concrete systems $\mathcal{S}_i = (B_i, H_i)$ $(i = 1, 2)$ and given set W_c constraining B_{12}. And given abstract systems $\mathcal{S}_j = (B_j, H_j)$ $(j = 3, 4)$ and given set W_a constraining B_{34} without restricting the ϵ variables. Then the following holds:

$$\frac{\begin{array}{l} H_1 \bigotimes H_2 \cap W_{c1} \bigotimes W_{c2} \subseteq (H_1 \cap W_{c1}) \bigotimes (H_2 \cap W_{c2}) \\ W_c \subseteq W_{c1} \bigotimes W_{c2} \\ \mathcal{S}_1 \ {}_{W_{c1}}\mathbf{ref}^{\,W_a}\ \mathcal{S}_3 \\ \mathcal{S}_2 \ {}_{W_{c2}}\mathbf{ref}^{\,W_a}\ \mathcal{S}_4 \end{array}}{\mathcal{S}_1 \parallel \mathcal{S}_2 \ {}_{W_c}\mathbf{ref}^{\,W_a}\ \mathcal{S}_3 \parallel \mathcal{S}_4} \qquad W_{ci} \textit{ constraining } B_i \textit{ (i=1,2)}$$

Proof 31
Assume agreement on the bases. Then according to Def. 39 and 40 we must infer from the assumptions that $\mathcal{O}_{\mathrm{X}_{12}}(H_1 \bigotimes H_2 \cap W_c) \subseteq \mathcal{O}_{\mathrm{X}_{34}}(H_3 \bigotimes H_4 \cap W_a)$. We will first prove the following:

$$\mathcal{O}_{\mathrm{X}_{34}}((H_3 \cap W_a) \bigotimes (H_4 \cap W_a)) \subseteq \mathcal{O}_{\mathrm{X}_{34}}(H_3 \bigotimes H_4 \cap W_a)$$

$$\begin{array}{ll}
 & h \in \mathcal{O}_{\mathrm{X}_{34}}((H_3 \cap W_a) \bigotimes (H_4 \cap W_a)) \\
= & \quad \% \ \ Def.\ 30 \\
 & \exists h_1 : h_1 \in (H_3 \cap W_a) \bigotimes (H_4 \cap W_a) \wedge h \ \mathrm{X}_{34}\textit{-variant of } h_1 \\
= & \quad \% \ \ Def.\ 32 \\
 & \exists h_1 : (\exists h_3, h_4 : h_3 \in (H_3 \cap W_a) \wedge h_4 \in (H_4 \cap W_a) \wedge \otimes(h_1, h_3, h_4)) \\
 & \wedge h \ \mathrm{X}_{34}\textit{-variant of } h_1 \\
\rightarrow & \quad \% \ \ \theta_1 = \theta_3 = \theta_4, W_a \textit{ doesn't restrict the } \epsilon \textit{ variables} \\
 & \exists h_1 : (\exists h_3, h_4 : h_3 \in H_3 \wedge h_4 \in H_4 \wedge h_1 \in W_a \wedge \otimes(h_1, h_3, h_4)) \\
 & \wedge h \ \mathrm{X}_{34}\textit{-variant of } h_1 \\
= & \quad \% \ \ Calc. \\
 & \exists h_1 : (\exists h_3, h_4 : h_3 \in H_3 \wedge h_4 \in H_4 \wedge \otimes(h_1, h_3, h_4)) \\
 & \wedge h_1 \in W_a \wedge h \ \mathrm{X}_{34}\textit{-variant of } h_1 \\
= & \quad \% \ \ Def.\ 32 \\
 & \exists h_1 : h_1 \in H_3 \bigotimes H_4 \cap W_a \wedge h \ \mathrm{X}_{34}\textit{-variant of } h_1 \\
= & \quad \% \ \ Def.\ 30 \\
 & h \in \mathcal{O}_{\mathrm{X}_{34}}(H_3 \bigotimes H_4 \cap W_a)
\end{array}$$

The proof of the Lemma is then as follows:

$$
\begin{array}{ll}
& \mathcal{O}_{X_{12}}(H_1 \bigotimes H_2 \cap W_c) \\
\subseteq & \quad \% \;\; H_1 \bigotimes H_2 \cap W_{c1} \bigotimes W_{c2} \subseteq (H_1 \cap W_{c1}) \bigotimes (H_2 \cap W_{c2}) \\
& \qquad W_c \subseteq W_{c1} \bigotimes W_{c2} \\
& \qquad \mathit{Lemma}\ 5(c) \\
& \mathcal{O}_{X_{12}}((H_1 \cap W_{c1}) \bigotimes (H_2 \cap W_{c2})) \\
\subseteq & \quad \% \;\; \mathcal{S}_1 \ {}_{W_{c1}}\mathbf{ref}^{\,W_a}\, \mathcal{S}_3 \\
& \qquad \mathcal{S}_2 \ {}_{W_{c2}}\mathbf{ref}^{\,W_a}\, \mathcal{S}_4 \\
& \qquad \mathit{Lemma}\ 5(a), (b) \\
& \mathcal{O}_{X_{34}}((H_3 \cap W_a) \bigotimes (H_4 \cap W_a)) \\
\subseteq & \quad \% \;\; \mathit{Above\ result} \\
& \mathcal{O}_{X_{34}}(H_3 \bigotimes H_4 \cap W_a)
\end{array}
$$

A.18 Proof of Lemma 11

Lemma 11
Given sets W_i $(i = 1, 2)$ not restricting the ϵ variables then

$$W_1 \bigotimes W_2 = W_1 \cap W_2.$$

Proof 32

$$
\begin{array}{ll}
& h \in W_1 \bigotimes W_2 \\
= & \quad \% \;\; \mathit{Def.}\ 32 \\
& \exists h_1, h_2 : h_1 \in W_1 \wedge h_2 \in W_2 \wedge \otimes(h, h_1, h_2) \\
= & \quad \% \;\; W_i \ \mathit{don't\ restrict}\ \epsilon\ \mathit{variables,\ i.e.} \\
& \qquad \otimes(h, h_1, h_2) \leftrightarrow h = h_1 = h_2 \\
& \exists h_1, h_2 : h_1 \in W_1 \wedge h_2 \in W_2 \wedge h = h_1 = h_2 \\
= & \quad \% \;\; \mathit{Calc.} \\
& h \in W_1 \cap W_2
\end{array}
$$

A.19 Proof of Theorem 8

Theorem 8 (Relative refinement of DTL machine specifications)
Given concrete machine specification $\mathcal{S}_c \triangleq (B_c, \mathrm{I}_c \wedge \Box\mathrm{T}_c \wedge \mathrm{L}_c)$ and DTL formula W_c over B_c and abstract machine specification $\mathcal{S}_a \triangleq (B_a, \mathrm{I}_a \wedge \Box\mathrm{T}_a \wedge \mathrm{L}_a)$ and DTL formula W_a over B_a. Let $\mathrm{G}_c \triangleq \mathrm{I}_c \wedge \Box\mathrm{T}_c \wedge \mathrm{L}_c \wedge \mathrm{W}_c$ and $\mathrm{G}_a \triangleq \mathrm{I}_a \wedge \Box\mathrm{T}_a \wedge \mathrm{L}_a \wedge \mathrm{W}_a$. Then $\mathcal{S}_c \ {}_{\mathit{Hist}(\mathrm{W}_c)}\mathbf{ref}^{\,\mathit{Hist}(\mathrm{W}_a)}\, \mathcal{S}_a$ iff

$$
\begin{array}{l}
\mathfrak{O}(B_c) = \mathfrak{O}(B_a) \ \mathit{and} \\
\models (\exists \mathrm{X}_c \,.\, (\mathrm{G}_c)) \rightarrow (\exists \mathrm{X}_a \,.\, (\mathrm{G}_a))
\end{array}
$$

Proof 33

$$
\begin{array}{ll}
& \mathcal{S}_c \ {}_{Hist(\mathrm{W}_c)}\mathbf{ref}^{\ Hist(\mathrm{W}_a)}\ \mathcal{S}_a \\
= & \quad \% \ \ Def.\ 39 \\
& \mathfrak{O}(B_c) = \mathfrak{O}(B_a) \\
& \mathcal{O}_{\mathrm{X}_c}(Hist(\mathrm{I}_c \wedge \Box\mathrm{T}_c \wedge \mathrm{L}_c) \cap Hist(\mathrm{W}_c)) \\
& \subseteq \mathcal{O}_{\mathrm{X}_a}(Hist(\mathrm{I}_a \wedge \Box\mathrm{T}_a \wedge \mathrm{L}_a) \cap Hist(\mathrm{W}_a)) \\
= & \quad \% \ \ Def.\ 21 \ and \ 20 \\
& \mathfrak{O}(B_c) = \mathfrak{O}(B_a) \\
& \mathcal{O}_{\mathrm{X}_c}(Hist(\mathrm{I}_c \wedge \Box\mathrm{T}_c \wedge \mathrm{L}_c \wedge \mathrm{W}_c)) \subseteq \mathcal{O}_{\mathrm{X}_a}(Hist(\mathrm{I}_a \wedge \Box\mathrm{T}_a \wedge \mathrm{L}_a \wedge \mathrm{W}_a)) \\
= & \quad \% \ \ Theorem\ 4 \\
& \mathfrak{O}(B_c) = \mathfrak{O}(B_a) \\
& \models (\exists \mathrm{X}_c \,.\, (\mathrm{I}_c \wedge \Box\mathrm{T}_c \wedge \mathrm{L}_c \wedge \mathrm{W}_c)) \rightarrow (\exists \mathrm{X}_a \,.\, (\mathrm{I}_a \wedge \Box\mathrm{T}_a \wedge \mathrm{L}_a \wedge \mathrm{W}_a))
\end{array}
$$

A.20 Proof of Theorem 9

Theorem 9 (Relative composition corresponds to semantic merge)
Given machine system specifications $(B_i, \mathrm{I}_i \wedge \Box\mathrm{T}_i \wedge \mathrm{L}_i)$ *where* $B_i \triangleq ((\mathrm{In}_i, \mathrm{Out}_i), (\mathrm{V}_i, \mathrm{X}_i))$, *and given DTL formulae* W_i *over* B_i *for* $i = 1, 2$ *and let* $\overline{W} \triangleq (Hist(\mathrm{W}_c), Hist(\mathrm{W}_a))$ *and given the relative composed system as in Def. 41, i.e.,* (B, H) *where* $B \triangleq ((\mathrm{In}_1 \setminus \mathrm{Out}_2 \cup \mathrm{In}_2 \setminus \mathrm{Out}_1, \mathrm{Out}_1 \setminus \mathrm{In}_2 \cup \mathrm{Out}_2 \setminus \mathrm{In}_1), (\mathrm{V}_1 \cup \mathrm{V}_2, \mathrm{X}_1 \cup \mathrm{X}_2))$ *and* $\mathrm{H} \triangleq \exists \epsilon_1, \epsilon_2 . ({}_{B_1^A} \odot_{B_2^A} (\epsilon, \epsilon_1, \epsilon_2) \wedge (\mathrm{I}_1 \wedge \Box\mathrm{T}_1 \wedge \mathrm{L}_1 \wedge \mathrm{W}_1)\,[\epsilon_1/\epsilon] \wedge (\mathrm{I}_2 \wedge \Box\mathrm{T}_2 \wedge \mathrm{L}_2 \wedge \mathrm{W}_2)\,[\epsilon_2/\epsilon])$ *then*

$$Hist(\mathrm{I}_1 \wedge \Box\mathrm{T}_1 \wedge \mathrm{L}_1) \textcircled{\scriptsize $\overline{W}$} Hist(\mathrm{I}_2 \wedge \Box\mathrm{T}_2 \wedge \mathrm{L}_2) = Hist(\mathrm{H})$$

Proof 34

$$
\begin{array}{ll}
& Hist(\mathrm{I}_1 \wedge \Box\mathrm{T}_1 \wedge \mathrm{L}_1) \textcircled{\scriptsize $\overline{W}$} Hist(\mathrm{I}_2 \wedge \Box\mathrm{T}_2 \wedge \mathrm{L}_2) \\
= & \quad \% \ \ Def.\ 40 \\
& (Hist(\mathrm{I}_1 \wedge \Box\mathrm{T}_1 \wedge \mathrm{L}_1) \cap Hist(\mathrm{W}_1)) \otimes (Hist(\mathrm{I}_2 \wedge \Box\mathrm{T}_2 \wedge \mathrm{L}_2) \cap Hist(\mathrm{W}_2)) \\
= & \quad \% \ \ Def.\ 21 \ and \ 20 \\
& (Hist(\mathrm{I}_1 \wedge \Box\mathrm{T}_1 \wedge \mathrm{L}_1 \wedge \mathrm{W}_1)) \otimes (Hist(\mathrm{I}_2 \wedge \Box\mathrm{T}_2 \wedge \mathrm{L}_2 \wedge \mathrm{W}_2)) \\
= & \quad \% \ \ Theorem\ 5,\ def.\ of\ \ \mathrm{H} \\
& Hist(\mathrm{H})
\end{array}
$$

A.21 Proof of Lemma 12

Lemma 12
Given machines $M \triangleq (B, I, T)$ *and* $M_1 \triangleq (B, I_1, T_1)$. *Define machine* M_2 *as* $(B, I_2, T_2$ *where* I_2 *and* T_2 *are as follows:*

- $I_2 \triangleq I \cap I_1$, *and*
- $T_2 \triangleq T \cap T_1$.

Then $Comp(M_2) = Comp(M) \cap Comp(M_1)$.

Proof 35

$$
\begin{array}{ll}
 & h \in Comp(M) \cap Comp(M_1) \\
= & \quad \%\ \ Def.\ 16 \\
 & \theta(0) \in I \wedge \theta(0) \in I_1 \\
 & (\forall t : Step_h \in T \vee Step_h \in \mathrm{STU}) \wedge (\forall t : Step_h \in T_1 \vee Step_h \in \mathrm{STU}) \\
= & \quad \%\ \ Calculus \\
 & \theta(0) \in I \cap I_1 \\
 & \forall t : Step_h \in T \cap T_2 \vee Step_h \in \mathrm{STU} \\
= & \quad \%\ \ Def.\ 16 \\
 & h \in Comp(M_2)
\end{array}
$$

A.22 Proof of Lemma 13

Lemma 13
Given concrete machine specification $\mathcal{S}_c \triangleq (B_c, Comp(M_c) \cap L_c)$ and set $W_c = Comp(M_{c1}) \cap L_{c1}$, and given abstract machine specification $\mathcal{S}_a \triangleq (B_a, Comp(M_a) \cap L_a)$ and set $W_a = Comp(M_{a1}) \cap L_{a1}$ s.t. $\mathfrak{O}(B_c) = \mathfrak{O}(B_a)$. If there exists a relative refinement mapping from $\mathcal{S}_c$ to $\mathcal{S}_a$ then $\mathcal{S}_c\ {}_{W_c}\mathbf{ref}^{\,W_a}\ \mathcal{S}_a$.

Proof 36
We first prove the following result:
For all $h_c \in Comp(M_c) \cap Comp(M_{c1})$, there exists a $h_a \in Comp(M_a) \cap Comp(M_{a1})$ s.t. for all $t \in \mathbb{R}^{\geq 0}$, $\langle \psi_c(t), \theta_c(t) \rangle = \langle \psi_a(t), \theta(t)_a \rangle$ and $f(\theta_c(t)) = \theta_a(t)$.

$$
\begin{array}{ll}
 & h_c \in Comp(M_c) \cap Comp(M_{c1}) \\
= & \quad \%\ \ Def.\ 16 \\
 & \theta_c(0) \in I_c \cap I_{c1} \wedge \\
 & \forall t : \langle \psi_c(t), \theta_c(t), \lim_{t \leftarrow t_1} \theta_c(t_1) \rangle \in T_c \cap T_{c1} \vee (\psi_c(t)(\epsilon) \in \{\lambda, \mathbf{i}, \mathbf{e}\} \wedge \theta_c(t) = \lim_{t \leftarrow t_1} \theta_c(t_1)) \\
\rightarrow & \quad \%\ \ Def.\ 42 \\
 & f(\theta_c(0)) \in I_a \cap I_{a1} \\
 & \wedge \forall t : \langle \psi_a(t), f(\theta_c(t)), \lim_{t \leftarrow t_1} f(\theta_c(t_1)) \rangle \in T_a \cap T_{a1} \vee \\
 & \quad (\psi_a(t)(\epsilon) \in \{\lambda, \mathbf{i}, \mathbf{e}\} \wedge f(\theta_c(t)) = \lim_{t \leftarrow t_1} f(\theta_c(t_1))) \\
= & \quad \%\ \ Def.\ 16 \\
 & h_a \in Comp(M_a) \cap Comp(M_{a1}) \\
 & \wedge \forall t : \langle \psi_c(t), \theta_c(t) \rangle = \langle \psi_a(t), \theta(t)_a \rangle \wedge f(\theta_c(t)) = \theta_a(t)
\end{array}
$$

The proof of Lemma 13 is then as follows:

$$
\begin{array}{ll}
 & \mathcal{S}_c\ {}_{W_c}\mathbf{ref}^{W_a}\ \mathcal{S}_a \\
= & \quad \%\ \ Def.\ 39, Def.\ W_c\ and\ W_a \\
 & \mathfrak{O}(B_c) = \mathfrak{O}(B_a)\ and \\
 & \mathcal{O}_{\mathrm{X}_c}(Comp(M_c) \cap Comp(M_{c1}) \cap L_c \cap L_{c1}) \\
 & \subseteq \mathcal{O}_{\mathrm{X}_a}(Comp(M_a) \cap Comp(M_{a1}) \cap L_a \cap L_{a1}) \\
= & \quad \%\ \ \mathfrak{O}(B_c) = \mathfrak{O}(B_a) \\
 & \mathcal{O}_{\mathrm{X}_c}(Comp(M_c) \cap Comp(M_{c1}) \cap L_c \cap L_{c1}) \\
 & \subseteq \mathcal{O}_{\mathrm{X}_a}(Comp(M_a) \cap Comp(M_{a1}) \cap L_a \cap L_{a1}) \\
\leftarrow & \quad \%\ \ From\ Def.\ 42, \\
 & \qquad f(Comp(M_c) \cap Comp(M_{c1}) \cap L_c \cap L_{c1}) \subseteq L_a \cap L_{a1} \\
 & \qquad Property\ of\ f, \\
 & \qquad f(Comp(M_c) \cap Comp(M_{c1}) \cap L_c \cap L_{c1}) \subseteq f(Comp(M_c) \cap Comp(M_{c1})), \\
 & \qquad by\ above\ result, \\
 & \qquad f(Comp(M_c) \cap Comp(M_{c1})) \subseteq Comp(M_a) \cap Comp(M_{a1}), \\
 & \qquad Resulting\ in\ , \\
 & \qquad f(Comp(M_c) \cap Comp(M_{c1}) \cap L_c \cap L_{c1}) \\
 & \qquad \subseteq Comp(M_a) \cap Comp(M_{a1}) \cap L_a \cap L_{a1} \\
 & \qquad From\ Lemma\ 5(c), \\
 & \qquad \mathcal{O}_{\mathrm{X}_a}(f(Comp(M_c) \cap Comp(M_{c1}) \cap L_c \cap L_{c1})) \\
 & \qquad \subseteq \mathcal{O}_{\mathrm{X}_a}(Comp(M_a) \cap Comp(M_{a1}) \cap L_a \cap L_{a1}), \\
 & \qquad From\ Def.\ 42, \\
 & \qquad \mathcal{O}_{\mathrm{X}_c}(Comp(M_c) \cap Comp(M_{c1}) \cap L_c \cap L_{c1}) \\
 & \qquad = \mathcal{O}_{\mathrm{X}_a}(f(Comp(M_c) \cap Comp(M_{c1}) \cap L_c \cap L_{c1})) \\
 & true
\end{array}
$$