Responsibility Analysis by Abstract Interpretation

by

Chaoqiang Deng

A dissertation submitted in partial fulfillment

of the requirements for the degree of

Doctor of Philosophy

Department of Computer Science

Courant Institute of Mathematical Sciences

New York University

January, 2021

Professor Patrick Cousot

Acknowledgments

I would like to express my most sincere gratitude to my advisor Patrick Cousot for his continuous support, patience, motivation, encouragement, and immense knowledge. Without his help, I could not survive from the PhD program and complete this dissertation. Besides my advisor, I want to thank the rest of my committee: Kedar Namjoshi, for his insightful comments and suggestions, but also for the extremely enjoyable internships and collaborations at Bell Labs; Xavier Rival, for spending what must have been quite a chunk of time in reading through my dissertation, as well as the stimulating discussions before and after my defense; Thomas Wies, for the invaluable suggestions and questions, as well as his great help throughout my PhD journey; Benjamin Goldberg, for his precious encouragement and guidance from the DQE to the final defense.

I am thankful to all my colleagues during my internships and my time at New York University for the wonderful times we shared. In addition, I would like to thank all my friends who gave me the necessary distraction from my research and made my life in New York more enjoyable.

Finally, my deep gratitude to my family for their unparalleled love, support and sacrifices. I am forever indebted to my parents for selflessly encouraging me to explore new directions in life and seek my own destiny.

Abstract

Given a behavior of interest, automatically determining the corresponding responsible entity (or say, the root cause) is a task of critical importance in various scientific fields, especially in the program static analysis. Classical static analysis techniques (e.g. dependency analysis, taint analysis, slicing, etc.) assist programmers in narrowing down the scope of responsibility, but none of them can explicitly identify the responsible entity. Meanwhile, the causality analysis is generally not pertinent for analyzing programs, and the structural equations model (SEM) of actual causality misses some information inherent in programs (e.g. temporal information, and whether an entity is free to make choices or not), making the corresponding program analysis imprecise.

In this dissertation, inspired by a classic forest fire example used in defining causality, a novel definition of responsibility based on the abstraction of trace semantics is proposed, which is expressive and generic to cope with both program analyses and tasks in other scientific fields. Briefly speaking, an action a_{R} is responsible for behavior $\mathcal{B}$ in a certain trace, if and only if a_{R} is free to make choices, and such a choice is the first one that ensures the occurrence of $\mathcal{B}$ in that trace. Such a definition makes use of the information regarding the temporal ordering of actions, as well as whether an action has free choices or not. In addition, our definition of responsibility takes into account the

cognizance of observer, which, to the best of our knowledge, is a new innovative idea in program analysis. Compared to current dependency and causality analysis methods, the responsibility analysis is demonstrated to be more precise in many examples.

Furthermore, this dissertation proposes a sound framework of abstract responsibility analysis, which allows a balance between cost and precision to solve the undecidable problem of responsibility. Essentially, the abstract analysis builds a trace partitioning automaton by an iteration of over-approximating forward reachability analysis with trace partitioning and under-approximating/over-approximating backward impossible failure accessibility analysis, and determines the bounds of potentially responsible entities along paths in the automaton. Unlike the concrete responsibility analysis identifies exactly a single action as the responsible entity along every concrete trace, the abstract analysis may lose some precision and find multiple actions potentially responsible along each automaton path. However, the soundness is preserved, and every responsible entity in the concrete is guaranteed to be also found responsible in the abstract.

Table of contents

List of Figures

List of Figures

List of Tables

List of Tables

Introduction

"Everybody is responsible for the fate of the world."
Gu Yanwu (1613 -1682)

This well-known aphorism from an ancient Chinese philosopher encourages ordinary people (not only the ruling class) to take the responsibility for the prosperity of society. Yet, such a positive spirit does not help in solving specific problems in various scientific fields, since usually what people really want is to narrow down or even exactly specify the cause of every behavior of interest. For instance, when studying the cause of pollution in a certain river, environmentalists shall not blame on the natural environment, but explicitly point out which factory along the river is responsible for the pollution; for a detective, instead of ascribing a certain crime to the whole society, his job is to determine the culprit responsible for the crime; similarly, when analyzing the reason of a program behavior (e.g. an error) during a certain execution, blaming on the whole program or a large slice of the program is trivially correct but not of practical use, and the programmer is eager to learn exactly which action (e.g. user input/random number generator/system setting/variable initialization) is responsible for the behavior of interest.

In this dissertation, we focus on program analyses, and our objective is to give a generic definition of responsibility and design a comprehensive framework of responsi-

bility analysis, which could automatically determine the responsible entity (or say, the root cause) of any behavior of interest. Contrary to accountability mechanisms [32, 16, 28] that track down perpetrators after the fact, we want to detect the responsible entity and configure its permission before deploying the program, which is of great importance for the potentially insecure behavior in safety and security critical systems. Due to the massive scale of modern software, it is virtually impossible to identify responsible entities manually. The only possible solution is to design a static analysis of responsibility, which can examine all possible executions of a program without executing them.

The cornerstone of designing such an analysis is to define responsibility in programming languages. It is surprising to notice that, although the concepts of causality and responsibility have been long studied in various contexts (law sciences [58], artificial intelligence [57], statistical and quantum mechanics, biology, social sciences, etc. [1]), none of these definitions is fully pertinent for programming languages. Take the actual cause [47, 48] as an example, its structural equations model (SEM) [60] is not suitable for representing programs: the value of each endogenous variable in the model is fixed once it is set by the equations or some external action, while the value of program variables can be assigned for unbounded number of times during the execution. In addition, the SEM cannot make use of the temporal information or whether an entity is free to make choices, which plays an indispensable role in determining responsibility.

There do exist techniques analyzing the influence relationships in computer programs, such as dependency analysis [19, 39, 15], taint analysis [12] and program slicing [45], which help in narrowing down the scope of possible locations of responsible entities. However, no matter whether adopting semantic or syntactic methods, these techniques

are not precise enough to explicitly identify the responsibility.

In order to solve the above problems, this dissertation proposes a novel definition of responsibility, which is expressive and generic to handle various programming languages. Roughly speaking, an action a_{R} is responsible for a given behavior $\mathcal{B}$ in a certain trace, if and only if the action a_{R} can make choices at its discretion (e.g. an input action from external subjects is assumed to have free choices on the input value), and such a choice is the first one that guarantees the occurrence of $\mathcal{B}$ in that trace. Such a definition of responsibility is an abstract interpretation [3, 4] of the program trace semantics, taking into account both the temporal ordering of actions and the information regarding whether an action has free choices or not. Moreover, an innovative idea of cognizance is adopted in this definition, which allows analyzing responsibility from the perspective of various observers. Compared to current dependency/causality analysis techniques, our definition of responsibility is more generic and precise.

Besides defining the responsibility in programming languages, another major challenge encountered is to design an abstract static analysis of responsibility. Since the concrete trace semantics used in the definition of responsibility is uncomputable in general, it is necessary to have a sound over-approximation of it, and here we propose to adopt the trace partitioning automaton that is constructed by over-approximating forward reachability analysis with trace partitioning [14, 43]. Together with the under-approximating/over-approximating backward impossible failure accessibility analysis introduced in this dissertation, we present a sound framework of abstract responsibility analysis, which determines the possible range of responsible entities along paths in the automaton. Although the abstract analysis loses precision to some extent, the sound-

ness is preserved, i.e. it is guaranteed that every action that is found responsible in the concrete must be also determined responsible in the abstract.

The application of responsibility analysis is pervasive. Although the implementation of an automatic responsibility analyzer is not provided here, we have demonstrated its effectiveness by examples including access control, negative balance / buffer overflow, division by zero / login attack, and information leakage.

To sum up, the main contributions of this dissertation are:

- A completely new definition of responsibility based on the abstract interpretation of trace semantics is introduced, which is more generic and precise than current dependency/causality analysis techniques;
- To the best of our knowledge, the observer's cognizance is adopted in program analysis for the first time, which allows analyzing the responsibility from the perspective of different observers;
- A sound framework of the abstract responsibility analysis is proposed, which essentially consists of an iteration of over-approximating forward reachability analysis with trace partitioning and under/over-approximating backward impossible failure accessibility analysis.

Specifically, in this dissertation, part I introduces some preliminary definitions and techniques, including the syntax and semantics of a transition system (chapter 1), the over-approximating forward reachability analysis and under/over-approximating backward impossible failure accessibility analysis (chapter 2), the trace partitioning domain and automata (chapter 3). Part II proposes the responsibility analysis in the concrete, in which an informal but intuitive characterization of responsibility is given in chapter 4,

the definition of responsibility is formalized in chapter 5, and the applications of responsibility analysis are exemplified in chapter 6. Part III presents the responsibility analysis in the abstract, including the user specification of behaviors and cognizance in the abstract (chapter 7) and a detailed framework of abstract responsibility analysis (chapter 8), which utilizes the forward/backward analyses from part I.

For the sake of coherence, it is recommended to read chapter 1 followed by part II and part III, and refer to chapter 2 or 3 when any unfamiliar notations or techniques are encountered (e.g. backward impossible failure accessibility analysis, forward reachability analysis with trace partitioning).

Part I

Preliminaries

PART I. PRELIMINARIES

In this part, we introduce some definitions and techniques that will be used in the rest of this dissertation.

Chapter 1 introduces the syntax and semantics of a transition system, which is generic to model programs written in various languages. This dissertation focuses on numeric programs, and we specifically consider a very simple programming language that features assignments, conditionals and while loops. An introductory example of access control written in this simple language is given, and it is used throughout the whole dissertation to illustrate the framework of concrete/abstract responsibility analysis.

Chapter 2 recalls some key concepts and notations in the abstract interpretation framework, and presents an over-approximating forward reachability analysis that automatically infers program invariants, which is a well studied problem in the program analysis and verification. In addition, we discuss the dual problem that has been rarely explored: the backward impossible failure accessibility analysis, which infers sufficient preconditions for a given postcondition (program property) to hold. An under-approximating backward impossible failure accessibility analysis was proposed by Miné, and similarly we propose an over-approximating backward impossible failure accessibility analysis.

Chapter 3 discusses the trace partitioning abstract domain proposed by Rival and Mauborgne, introduces a new partitioning directive based on environment properties, and proposes the trace partitioning automaton, which improves the precision of forward reachability analysis and makes determining responsibility in the abstract possible.

It is worth noting that the forward reachability analysis with trace partitioning and the backward accessibility analysis discussed in this part are the cornerstones of abstract responsibility analyses in part III.

Chapter 1

Program Syntax and Semantics

In this dissertation, programs are modeled as transition systems, providing a language-independent small-step operational semantics that is generic to handle various programming languages (including the simple language introduced in this chapter, which is similar to the C language and used by all examples throughout this dissertation).

1.1 Program Syntax

Transition Systems. $\mathbb{V}$ is the set of all possible values. $\mathbb{X}$ is the set of variables. $\mathbb{M}$ is the set of environments (i.e. stores, or memory states), each of which maps all the variables to their values at a specific time during the execution of the program. $\mathbb{L}$ is the set of program points (i.e. control states); specially, $\ell^i \in \mathbb{L}$ is the initial program point (i.e. the entry control state of the program), and $\ell^f \in \mathbb{L}$ is the final program point (i.e. the exit control state of the program). $\mathbb{S} = \mathbb{L} \times \mathbb{M}$ is the set of states, each of which is a pair of a program point $\ell \in \mathbb{L}$ and an environment $\rho \in \mathbb{M}$. Specially, $\mathbb{S}^i \in \wp(\mathbb{S})$

denotes the set of initial states, which can be implemented as $\mathbb{S}^i = \{\ell^i\} \times \mathbb{M}$ in practice; $\mathbb{S}^f \in \wp(\mathbb{S})$ denotes the set of final states, which is implemented as $\mathbb{S}^f = \{\ell^f\} \times \mathbb{M}$ and represents correct program termination; and ω denotes the error state, which represents the incorrect program termination (e.g. division by zero). By abuse of notation, ω also denotes the error in expression evaluations and the error environment. $\mathbb{A}$ is the set of all actions (i.e. atomic instructions) in the program, e.g. assignments, boolean tests, skip, external inputs, random number generations, variable initialization, etc.

v	$\in$	$\mathbb{V}$			values
x	$\in$	$\mathbb{X}$			variables
ρ	$\in$	$\mathbb{M}$	$\triangleq$	$\mathbb{X} \mapsto \mathbb{V}$	environments (memory states)
ℓ	$\in$	$\mathbb{L}$			program points (control states, labels)
s	$\in$	$\mathbb{S}$	$\triangleq$	$\mathbb{L} \times \mathbb{M}$	states
a	$\in$	$\mathbb{A}$			actions (atomic instructions)

Figure 1.1: Transition System Domains

The *transition relation* can be defined as $\rightarrow \in \wp(\mathbb{S} \times \mathbb{A} \times \mathbb{S})$, such that $\langle s,\ a,\ s' \rangle \in \rightarrow$ (or, $s \xrightarrow{a} s'$) denotes an atomic step from one state s to another state s' after executing the action a. Alternatively, we can omit the action a, and define the transition relation as $\rightarrow \in \wp(\mathbb{S} \times \mathbb{S})$, such that an atomic step from s to s' is denoted as $s \rightarrow s'$. In order to be consistent with the notations used in the trace partitioning abstract domain [43], here we adopt the latter definition of transition relation, and the omitted actions can be easily retrieved from the program source code. It is assumed that there is no outgoing transition from final states or the error state ($\forall s \in \mathbb{S}^f \cup \{\omega\}.\ \forall s' \in \mathbb{S}.\ s \not\rightarrow s'$).

A *transition system* (or, program) $\mathrm{P} = \langle \mathbb{S}^i,\ \rightarrow \rangle$ is defined as a pair of the set of initial states and the transition relation, which is generic to represent programs written in vari-

ous languages. Moreover, it is worthwhile to note that the above definition of transition system can also cope with interprocedural programs, if we generalize the control states to include both the syntactic program point and the calling stack. However, for the sake of simplicity, this dissertation does not take interprocedural programs into consideration.

A Simple Language. This dissertation focuses on numeric programs. In order to formalize the forward reachability analysis and backward accessibility analysis introduced in chapter 2, here we instantiate the transition system by considering a simple programming language in Fig.1.2, which features assignments, conditional tests, and while loops. It is similar to the language used in [34], except the ternary operation (or conditional operation) "*bexpr* ? *expr* : *expr*", which can be equivalently represented by a conditional test. More precisely, in this language, $\mathbb{X}$ is a finite fixed set of real-valued variables (i.e. the set of possible values $\mathbb{V} = \mathbb{R}$ are real numbers, and can be further restricted to integers), *expr* denotes numerical expressions, and *bexpr* denotes boolean expressions. Besides, an interval $[a; b]$ returns a random number between the left bound a and the right bound b, which facilitates representing non-determinism directly in the language. Specially, when $a = b$, $[a; b]$ denotes the constant number a. In addition, it is assumed that each atomic statement is associated with a unique program point ℓ from $\mathbb{L}$.

Every program written in this simple language can be modeled by a transition system, in which each action is either an assignment $x := expr$ or a boolean test *bexpr*. In addition, as shown in Fig.1.3, for every (numerical or boolean) expression *e*, its semantics $[\![e]\!]\rho$ is defined as the set of all possible (numerical or boolean) values that *e* may take in a given environment ρ (t denotes true, while f denotes false); for each action *a*, we define an *environment transfer function* $\tau\{\!|\, a \,|\!\} \in \wp(\mathbb{M}) \mapsto \wp(\mathbb{M} \cup \{\omega\})$, which maps a

prog	::=	*stat*	program
stat	::=	$x := expr$	assignment: $x \in \mathbb{X}$
	|	if (*bexpr*) {*stat*} else {*stat*}	conditional test
	|	while (*bexpr*) {*stat*}	while loop
	|	assert (*bexpr*)	assertion
	|	*stat*; *stat*	sequential statements
expr	::=	$[a; b]$	interval: $a, b \in \mathbb{R} \cup \{-\infty, \infty\}$
	|	x	variable $x \in \mathbb{X}$
	|	$-expr$	unary operation
	|	$expr \cdot expr$	binary operation: $\cdot \in \{+, -, \times, /\}$
	|	$bexpr\ ?\ expr : expr$	ternary operation
bexpr	::=	$expr \bowtie expr$	comparison: $\bowtie \in \{<, \leq, >, \geq, =, \neq\}$
	|	$bexpr \vee bexpr$	logical or operation
	|	$bexpr \wedge bexpr$	logical and operation
	|	$\neg bexpr$	logical negation operation

Figure 1.2: The Syntax of a Simple Language

set of environments before a to the set of reachable environments after it, including the error state ω if the execution of a encounters an error. From these environment transfer functions, the corresponding transition relation $\rightarrow$ can be easily derived: for any atomic action of the form ${}^{\ell}a^{\ell'}$, the transition relation is $\{\langle \ell,\ \rho\rangle \rightarrow \langle \ell',\ \rho'\rangle \mid \rho, \rho' \in \mathbb{M} \wedge \rho' \in \tau\{\!|\ a\ |\!\}(\{\rho\})\} \cup \{\langle \ell,\ \rho\rangle \rightarrow \omega \mid \rho \in \mathbb{M} \wedge \omega \in \tau\{\!|\ a\ |\!\}(\{\rho\})\}$; for any program P, its transition relation is the union of transition relations defined for all its atomic actions.

Consider the following example that is used throughout this dissertation.

Example 1 (Access Control) *The program in Fig. 1.4 can be interpreted as an access control program for an object o (e.g. a confidential file), such that o can be accessed if and only if*

$$
\begin{array}{rcll}
\tau\{\!|\, a \,|\!\} & \in & \wp(\mathbb{M}) \mapsto \wp(\mathbb{M} \cup \{\omega\}) & \text{Environment Transfer Function} \\
\tau\{\!|\, \chi := e \,|\!\}\mathrm{M} & \triangleq & \{\rho[\chi \mapsto v] \mid \rho \in \mathrm{M} \wedge v \in [\![e]\!]\rho\} \cup \{\omega \mid \exists \rho \in \mathrm{M}.\ \omega \in [\![e]\!]\rho\} & \\
\tau\{\!|\, b \,|\!\}\mathrm{M} & \triangleq & \{\rho \mid \rho \in \mathrm{M} \wedge \mathrm{t} \in [\![b]\!]\rho\} \cup \{\omega \mid \exists \rho \in \mathrm{M}.\ \omega \in [\![b]\!]\rho\} &
\end{array}
$$

$$
\begin{array}{rcll}
[\![expr]\!] & \in & \mathbb{M} \mapsto \wp(\mathbb{R} \cup \{\omega\}) & \text{Numerical Expression Semantics} \\
[\![[a;b]]\!]\rho & \triangleq & \{v \in \mathbb{R} \mid a \leq v \leq b\} & \\
[\![\chi]\!]\rho & \triangleq & \{\rho(\chi)\} & \\
[\![-e]\!]\rho & \triangleq & \{-v \mid v \in [\![e]\!]\rho\} & \\
[\![e_1 \cdot e_2]\!]\rho & \triangleq & \{v_1 \cdot v_2 \mid v_1 \in [\![e_1]\!]\rho \wedge v_2 \in [\![e_2]\!]\rho \wedge (v_2 \neq 0 \vee \cdot \neq /)\} \cup & \\
 & & \{\omega \mid 0 \in [\![e_2]\!] \wedge \cdot = /\} & \\
[\![b\ ?\ e_1 : e_2]\!]\rho & \triangleq & \{v \in [\![e_1]\!]\rho \mid \mathrm{t} \in [\![b]\!]\rho\} \cup \{v \in [\![e_2]\!]\rho \mid \mathrm{f} \in [\![b]\!]\rho\} \cup \{\omega \mid \omega \in [\![b]\!]\rho\} &
\end{array}
$$

$$
\begin{array}{rcll}
[\![bexpr]\!] & \in & \mathbb{M} \mapsto \wp(\{\mathrm{t}, \mathrm{f}, \omega\}) & \text{Boolean Expression Semantics} \\
[\![e_1 \bowtie e_2]\!]\rho & \triangleq & \{\mathrm{t} \mid \exists v_1 \in [\![e_1]\!]\rho, v_2 \in [\![e_2]\!]\rho.\ v_1 \bowtie v_2\} \cup & \\
 & & \{\mathrm{f} \mid \exists v_1 \in [\![e_1]\!]\rho, v_2 \in [\![e_2]\!]\rho.\ v_1 \not\bowtie v_2\} \cup & \\
 & & \{\omega \mid \omega \in [\![e_1]\!]\rho \cup [\![e_2]\!]\rho\} & \\
[\![b_1 \vee b_2]\!]\rho & \triangleq & \{\mathrm{t} \mid \mathrm{t} \in [\![b_1]\!]\rho \cup [\![b_2]\!]\rho\} \cup \{\mathrm{f} \mid \mathrm{f} \in [\![b_1]\!]\rho \cap [\![b_2]\!]\rho\} \cup & \\
 & & \{\omega \mid \omega \in [\![b_1]\!]\rho \cup [\![b_2]\!]\rho\} & \\
[\![b_1 \wedge b_2]\!]\rho & \triangleq & \{\mathrm{t} \mid \mathrm{t} \in [\![b_1]\!]\rho \cap [\![b_2]\!]\rho\} \cup \{\mathrm{f} \mid \mathrm{f} \in [\![b_1]\!]\rho \cup [\![b_2]\!]\rho\} \cup & \\
 & & \{\omega \mid \omega \in [\![b_1]\!]\rho \cup [\![b_2]\!]\rho\} & \\
[\![\neg b]\!]\rho & \triangleq & \{\mathrm{t} \mid \mathrm{f} \in [\![b]\!]\rho\} \cup \{\mathrm{f} \mid \mathrm{t} \in [\![b]\!]\rho\} \cup \{\omega \mid \omega \in [\![b]\!]\rho\} &
\end{array}
$$

Figure 1.3: The Environment Transfer Functions and Expression Semantics

both two administrators approve the access and the permission type of o from system settings is greater than or equal to "read only". For the sake of clarity, it is assumed that in this example the evaluation of an interval returns only integers (hence $\mathbb{V} = \mathbb{N}$ *in this example), and the analysis is similar to analyzing real numbers. Specifically, in line 2 and 4, the variable i1 and i2 assigned by a non-deterministic integer from* $[-1; 2]$ *is used to mimic external inputs that correspond to the decisions of two independent admins, where a positive value (i.e.* 1 *or* 2*)*

represents approving the access to o*, while* 0 *or a negative value (i.e.* -1*) represents rejecting the access; in line 6, the variable typ assigned by a non-deterministic integer from* $[1; 2]$ *is used to mimic the action of reading the permission type of* o *specified in the system settings (e.g. we can assume that* 1 *represents "read only", and* 2 *represents "read and write", which is similar to the file permissions system in Unix); in line 8, the access to* o *succeeds only when the value of acs is strictly positive (i.e.* 1 *or* 2*), which guarantees that both admins approve the access and the permission type of* o *is at least as high as "read only".* □

ℓ_1 : *apv* $:= 1$; //Approval: positive - yes, zero or negative - no
ℓ_2 : *i1* $:=$ [-1; 2]; //Input from 1st admin
ℓ_3 : *apv* $:= (i1 \leq 0)$? -1 : *apv*;
ℓ_4 : *i2* $:=$ [-1; 2]; //Input from 2nd admin
ℓ_5 : *apv* $:= (apv \geq 1 \wedge i2 \leq 0)$? -1 : *apv*;
ℓ_6 : *typ* $:= [1; 2]$; //Input from system settings
ℓ_7 : *acs* $:=$ *apv* $\times$ *typ*;
ℓ_8 : //Access the object o here, and it fails when *acs* ≤ 0

Figure 1.4: Access Control Program Example

To represent the above program as a transition system, we have: the set of program points $\mathbb{L} = \{\ell_1, \ell_2, \ell_3, \ell_4, \ell_5, \ell_6, \ell_7, \ell_8\}$; the set of variables $\mathbb{X} = \{apv, i1, i2, typ, acs\}$; the set of environments $\mathbb{M} = \mathbb{X} \mapsto \mathbb{Z}$, where $\mathbb{Z}$ is the set of integers; the set of states $\mathbb{S} = \mathbb{L} \times \mathbb{M}$, the set of initial states $\mathbb{S}^i = \{\ell_1\} \times \mathbb{M}$, and the set of final states $\mathbb{S}^f = \{\ell_8\} \times \mathbb{M}$. Moreover, the transition relation is defined as follows:

$$
\begin{aligned}
\rightarrow \;=\; & \{\langle\langle \ell_1,\, \rho\rangle,\, \langle \ell_2,\, \rho'\rangle\rangle \mid \rho' \in \tau\{\!|\, apv := 1 \,|\!\}(\{\rho\})\} \cup \\
& \{\langle\langle \ell_2,\, \rho\rangle,\, \langle \ell_3,\, \rho'\rangle\rangle \mid \rho' \in \tau\{\!|\, i1 := [-1; 2] \,|\!\}(\{\rho\})\} \cup \\
& \{\langle\langle \ell_3,\, \rho\rangle,\, \langle \ell_4,\, \rho'\rangle\rangle \mid \rho' \in \tau\{\!|\, apv := (i1 \leq 0)\ ?\ -1 : apv \,|\!\}(\{\rho\})\} \cup \\
& \{\langle\langle \ell_4,\, \rho\rangle,\, \langle \ell_5,\, \rho'\rangle\rangle \mid \rho' \in \tau\{\!|\, i2 := [-1; 2] \,|\!\}(\{\rho\})\} \cup
\end{aligned}
$$

$$\{\langle\langle \ell_5,\ \rho\rangle,\ \langle \ell_6,\ \rho'\rangle\rangle \mid \rho' \in \tau\{\!|\ \mathit{apv} := (\mathit{apv} \geq 1 \wedge \mathit{i2} \leq 0)\ ?\ \text{-}1 : \mathit{apv}\ |\!\}(\{\rho\})\} \cup$$
$$\{\langle\langle \ell_6,\ \rho\rangle,\ \langle \ell_7,\ \rho'\rangle\rangle \mid \rho' \in \tau\{\!|\ \mathit{typ} := [1;2]\ |\!\}(\{\rho\})\} \cup$$
$$\{\langle\langle \ell_7,\ \rho\rangle,\ \langle \ell_8,\ \rho'\rangle\rangle \mid \rho' \in \tau\{\!|\ \mathit{acs} := \mathit{apv} \times \mathit{typ}\ |\!\}(\{\rho\})\}.$$

1.2 Program Semantics

Traces. For any program (i.e. transition system), an execution is represented by a finite or infinite sequence of states, which is called as a *trace*; the program semantics is a set of such executions, and a trace property is a set of traces that have this property.

In the following, we write $\sigma = s_0 \cdots s_{n-1}$ to denote a finite trace of exactly length n, where the $(i+1)^{th}$ state $s_i = \langle \ell_i,\ \rho_i\rangle \in \mathbb{S}$ along the trace is denoted as $\sigma_{[i]}$; equivalently, such a finite trace of length n can be represented as a mapping from natural numbers in $[0, n-1]$ to states. Similarly, we write $\sigma = s_0 \cdots s_i \cdots$ to denote an infinite trace that does not terminate, and such a trace can be equivalently represented as a mapping from all natural numbers to states. Specially, ε denotes the empty trace. In addition, by abuse of notation, we say a state s belongs to a trace σ (i.e. $s \in \sigma$), if there exists a natural number $i \in \mathbb{N}$ such that $\sigma_{[i]} = s$.

σ	$\in$	$\mathbb{S}^+$	$\triangleq$ $\bigcup_{n \geqslant 1}([0, n-1] \mapsto \mathbb{S})$	finite traces
σ	$\in$	$\mathbb{S}^*$	$\triangleq$ $\{\varepsilon\} \cup \mathbb{S}^+$	empty or finite traces
σ	$\in$	$\mathbb{S}^\infty$	$\triangleq$ $\mathbb{N} \mapsto \mathbb{S}$	infinite traces
σ	$\in$	$\mathbb{S}^{+\infty}$	$\triangleq$ $\mathbb{S}^+ \cup \mathbb{S}^\infty$	finite or infinite traces
σ	$\in$	$\mathbb{S}^{*\infty}$	$\triangleq$ $\{\varepsilon\} \cup \mathbb{S}^{+\infty}$	empty or finite or infinite traces

For any trace σ, its length $|\sigma|$ is the number of states in σ. Specially, the length of the empty trace $|\varepsilon|$ is 0; for an infinite trace σ, its length $|\sigma|$ is denoted as ∞.

The *concatenation* of a finite trace $\sigma = s_0 \cdots s_{n-1}$ and a state s is simply defined by juxtaposition σs such that $\sigma s = s_0 \cdots s_{n-1} s$; the *concatenation* of a finite trace $\sigma = s_0 \cdots s_{n-1}$ and a transition $\tau = s_{n-1} \xrightarrow{a} s_n$ is denoted as $\sigma\tau$ such that $\sigma\tau = s_0 \cdots s_{n-1} s_n$; the *concatenation* of a finite traces $\sigma = s_0 \cdots s_{n-1}$ and another (finite or infinite) trace $\sigma' = s'_0 \cdots$ is denoted as $\sigma\sigma'$ such that $\sigma\sigma' = s_0 \cdots s_{n-1} s'_0 \cdots$; the *concatenation* of an infinite trace σ and another trace (or a state, or a transition) is the same as σ itself.

A trace σ is said to be $\preceq$ - less than or equal to another trace σ', if and only if, σ is a prefix of σ'. Besides, for any set $\mathcal{T}$ of traces, we define a function $\mathsf{Pref}(\mathcal{T})$ that returns the prefixes of traces in $\mathcal{T}$.

$$
\begin{array}{rcll}
\sigma \preceq \sigma' & \triangleq & |\sigma| \leqslant |\sigma'| \wedge \forall\, 0 \leqslant i < |\sigma| : \sigma_{[i]} = \sigma'_{[i]} & \text{ordering of traces} \\
\mathsf{Pref} & \in & \wp(\mathbb{S}^{*\infty}) \mapsto \wp(\mathbb{S}^{*\infty}) & \text{prefixes of traces} \\
\mathsf{Pref}(\mathcal{T}) & \triangleq & \{\sigma' \in \mathbb{S}^{*\infty} \mid \exists \sigma \in \mathcal{T}.\ \sigma' \preceq \sigma\} &
\end{array}
$$

Trace semantics. For a program $\mathrm{P} = \langle \mathbb{S}^i, \rightarrow \rangle$, a valid *intermediate (partial) trace* σ is a finite or infinite trace, along which every two successive states are bounded by the transition relation $\rightarrow$. The *intermediate (partial) trace semantics* $[\![\mathrm{P}]\!]^{\mathsf{It}} \in \wp(\mathbb{S}^{*\infty})$ is the set of all valid intermediate traces for P, i.e. $[\![\mathrm{P}]\!]^{\mathsf{It}} \triangleq \{s_0 \cdots s_{n-1} \in \mathbb{S}^* \mid \forall i \in [0, n-2].\ s_i \rightarrow s_{i+1}\} \cup \{s_0 \cdots s_i \cdots \in \mathbb{S}^\infty \mid \forall i \in \mathbb{N}.\ s_i \rightarrow s_{i+1}\}$. This semantics is a formal description of the executions of P, which start from any state, and stop at any time or do not ever stop.

A valid *prefix trace* σ is a finite or infinite trace, such that it starts from an initial state $s \in \mathbb{S}^i$ and every two successive states along the trace are related by the transition relation $\rightarrow$. The *prefix trace semantics* $[\![\mathrm{P}]\!]^{\mathsf{Pref}} \in \wp(\mathbb{S}^{*\infty})$ of P is the set of valid prefix traces, i.e. $[\![\mathrm{P}]\!]^{\mathsf{Pref}} \triangleq \{s_0 \cdots s_{n-1} \in \mathbb{S}^* \mid s_0 \in \mathbb{S}^i \wedge \forall i \in [0, n-2].\ s_i \rightarrow s_{i+1}\} \cup \{s_0 \cdots s_i \cdots \in \mathbb{S}^\infty \mid s_0 \in \mathbb{S}^i \wedge \forall i \in \mathbb{N}.\ s_i \rightarrow s_{i+1}\}$. This semantics is a formal description of the executions

of P, which start from any initial state, and stop at any time or do not ever stop.

A valid *maximal trace* σ is a finite or infinite trace, such that it starts from an initial state $s \in \mathbb{S}^i$, every two successive states along the trace are related by the transition relation $\rightarrow$, and either it terminates at a final state $s' \in \mathbb{S}^f$ or the error state ω, or it does not ever terminate. The *maximal trace semantics* $[\![\mathrm{P}]\!]^{\mathsf{Max}} \in \wp(\mathbb{S}^{*\infty})$ of P is the set of valid prefix traces, i.e. $[\![\mathrm{P}]\!]^{\mathsf{Max}} \triangleq \{s_0 \cdots s_{n-1} \in \mathbb{S}^* \mid s_0 \in \mathbb{S}^i \wedge \forall i \in [0, n-2].\, s_i \rightarrow s_{i+1} \wedge s_{n-1} \in \mathbb{S}^f \cup \{\omega\}\} \cup \{s_0 \cdots s_i \cdots \in \mathbb{S}^\infty \mid s_0 \in \mathbb{S}^i \wedge \forall i \in \mathbb{N}.\, s_i \rightarrow s_{i+1}\}$. This semantics is a formal description of the executions of P, which start from any initial state, and stop only at final states or crash or last forever. It is not hard to see that $[\![\mathrm{P}]\!]^{\mathsf{Max}} \subseteq [\![\mathrm{P}]\!]^{\mathsf{Pref}} \subseteq [\![\mathrm{P}]\!]^{\mathsf{It}}$. In addition, the prefix trace semantics $[\![\mathrm{P}]\!]^{\mathsf{Pref}}$ is an abstraction of the maximal trace semantics $[\![\mathrm{P}]\!]^{\mathsf{Max}}$ via the function Pref, i.e. $[\![\mathrm{P}]\!]^{\mathsf{Pref}} = \mathsf{Pref}([\![\mathrm{P}]\!]^{\mathsf{Max}})$.

Specifically, for any program written in the simple language described in Fig. 1.2, its intermediate/prefix/maximal trace semantics can be defined by structural induction/deduction on the program syntax, with the assistance of the environment transfer function defined for every atomic instruction in Fig. 1.3. Here we omit the structural definitions, and refer to chapter 16 of [2] for more information.

Example 2 (Access Control, Continued) *Consider the access control program in Fig. 1.4 again, it is obvious that there is no valid infinite trace and it is impossible to reach the error state ω, thus a valid maximal trace must start from the initial point ℓ_1 and terminate at the final point ℓ_8. By the definition of $\rightarrow$ given in Example 1, it is not hard to construct the corresponding maximal trace semantics:* $[\![\mathrm{P}]\!]^{\mathsf{Max}} = \{\langle \ell_1,\ \rho_1\rangle\langle \ell_2,\ \rho_2\rangle\langle \ell_3,\ \rho_3\rangle\langle \ell_4,\ \rho_4\rangle\langle \ell_5,\ \rho_5\rangle\langle \ell_6,\ \rho_6\rangle\langle \ell_7,\ \rho_7\rangle\langle \ell_8,\ \rho_8\rangle \mid (\rho_1 \in \mathbb{M}) \wedge (\rho_2 = \rho_1[\mathit{apv} \mapsto 1]) \wedge (\rho_3 = \rho_2[\mathit{i1} \mapsto v_1] \wedge v_1 \in \{\text{-}1, 0, 1, 2\}) \wedge (\rho_4 = \rho_3[\mathit{apv} \mapsto ((\rho_3(\mathit{i1}) <= 0)?\text{-}1 : \rho_3(\mathit{apv}))]) \wedge (\rho_5 = \rho_4[\mathit{i2} \mapsto v_2] \wedge$

$v_2 \in \{\text{-}1, 0, 1, 2\}) \wedge (\rho_6 = \rho_5[\mathit{apv} \mapsto ((\rho_5(\mathit{apv}) >= 1 \wedge \rho_5(\mathit{i2}) <= 0)?\text{-}1 : \rho_5(\mathit{apv}))]) \wedge (\rho_7 = \rho_6[\mathit{typ} \mapsto v_3] \wedge v_3 \in \{1, 2\}) \wedge (\rho_8 = \rho_7[\mathit{acs} \mapsto \rho_7(\mathit{apv}) * \rho_7(\mathit{typ})])\}$.

Along every valid maximal trace, there are three inputs, where $[\text{-}1; 2]$ *has four choices of integer values, and* $[1; 2]$ *two choices of integer values. Therefore,* $[\![\mathrm{P}]\!]^{\mathsf{Max}}$ *can be represented by 32 separate paths, each of which denotes a set of valid maximal traces such that they share the same inputs and the only difference comes from the initial environments.*

In addition, the intermediate trace semantics $[\![\mathrm{P}]\!]^{\mathsf{It}}$ *and prefix trace semantics* $[\![\mathrm{P}]\!]^{\mathsf{Pref}}$ *can be easily obtained from the transition relation* $\rightarrow$ *too, hence are omitted here. Moreover, a trace property "the access to o fails" can be represented by a set of maximal traces in which the value of acs is less than or equal to 0 at point* ℓ_8*, i.e.* $\{\sigma \in [\![\mathrm{P}]\!]^{\mathsf{Max}} \mid \exists \rho \in \mathbb{M}.\ \sigma_{[7]} = \langle \ell_8, \rho\rangle \wedge \rho(\mathit{acs}) <= 0\}$. □

Chapter 2

Forward Reachability Analysis and Backward Accessibility Analysis

Abstract interpretation [3, 4, 2] is a mathematical theory to reason on computer programs, more precisely on the executions of computer programs running on a computer. It formalizes formal methods and allows to discuss the guarantees they provide such as soundness (the conclusions about programs are always correct under suitable explicitly stated hypotheses), completeness (all true facts are provable), or incompleteness (showing the limits of applicability of the formal method). Abstract interpretation is mainly applied to design semantics, proof methods, and static analysis of programs. The semantics of programs formally defines all their possible executions at various levels of abstraction. Proof methods can be used to prove (manually or using theorem provers) that the semantics of a program satisfy some specification, that is a property of executions defining what programs are supposed to do. Static analyzers are programs that are able to automatically extract properties of programs semantics (i.e. of their executions)

using only the program text, without running the programs they analyze on a computer.

This chapter presents some notations and techniques in the abstract interpretation framework, which will be referenced in part III. To be more precise, section 2.1 reviews some key concepts of abstract interpretation, and section 2.2 introduces the abstract domain of environments and invariants. In section 2.3, we define the classic forward (possible success) reachability semantics of a program as an abstraction of the trace semantics, and sketch the design of an over-approximating abstract forward reachability analysis, which can automatically infer program invariants. In section 2.4, the backward impossible failure accessibility semantics is defined as the adjoint of forward reachability semantics, which specifies the sufficient precondition for a given postcondition to hold. Compared with the classic forward reachability analysis, the abstract backward impossible failure accessibility analysis has not been well studied yet, and there are few literature on this topic. We summarize the under-approximating abstract backward analysis proposed by Miné [34, 42], and propose a similar over-approximating abstract backward analysis, both of which will be used to determine responsibility in the abstract. In addition, for the sake of completeness, in section 2.5 we also briefly discuss the backward possible success accessibility semantics (which is the conjugate of backward impossible failure accessibility semantics) and the forward impossible failure reachability semantics (which is the adjoint of backward possible success accessibility semantics).

2.1 Basic Notations in Abstract Interpretation

Posets. A *partially ordered set* (i.e. *poset*) $\langle \mathcal{D}, \sqsubseteq \rangle$ is a set $\mathcal{D}$ equipped with a partial order $\sqsubseteq$ that is (1) reflexive: $\forall x \in \mathcal{D}.\ x \sqsubseteq x$; (2) antisymmetric: $\forall x, y \in \mathcal{D}.\ ((x \sqsubseteq y) \wedge (y \sqsubseteq$

$x)) \Rightarrow (x = y)$; and (3) transitive: $\forall x, y, z \in \mathcal{D}.\ ((x \sqsubseteq y) \wedge (y \sqsubseteq z)) \Rightarrow (x \sqsubseteq z)$. Let $S \in \wp(\mathcal{D})$ be a subset of the poset $\langle \mathcal{D}, \sqsubseteq \rangle$, then the *least upper bound* (or *lub, join*) of S (if any) is denoted as $\sqcup S$ such that $\forall x \in S.\ x \sqsubseteq \sqcup S$ and $\forall u \in S.\ (\forall x \in S.\ x \sqsubseteq u) \Rightarrow \sqcup S \sqsubseteq u$, and the *greatest lower bound* (or *glb, meet*) of S (if any) is denoted as $\sqcap S$ such that $\forall x \in S.\ \sqcap S \sqsubseteq x$ and $\forall l \in S.\ (\forall x \in S.\ l \sqsubseteq x) \Rightarrow l \sqsubseteq \sqcap S$. The poset $\mathcal{D}$ has a *supremum* (or *top*) $\top$ if and only if $\top = \sqcup \mathcal{D} \in \mathcal{D}$, and has an *infimum* (or *bottom*) $\bot$ if and only if $\bot = \sqcap \mathcal{D} \in \mathcal{D}$.

Preorder and Equivalence Relation. A *preorder* $\preceq$ is a binary relation that is reflexive and transitive, but not necessarily antisymmetric. Then $x \sim y \triangleq x \preceq y \wedge y \preceq x$ is a *equivalence relation* that is reflexive, symmetric ($\forall x, y \in \mathcal{D}.\ x \sim y \Rightarrow y \sim x$), and transitive. For any equivalence relation $\sim$, the *equivalence class* of $x \in \mathcal{D}$ is defined as $[x]_\sim \triangleq \{y \in \mathcal{D} \mid y \sim x\}$. The *quotient set* $\mathcal{D}|_\sim$ of $\mathcal{D}$ by the equivalence relation $\sim$ is the partition of $\mathcal{D}$ into a set of equivalence classes, i.e. $\mathcal{D}|_\sim \triangleq \{[x]_\sim \mid x \in \mathcal{D}\}$. In addition, the preorder $\preceq$ on $\mathcal{D}$ can be extended to a relation $\preceq_\sim$ on the quotient set $\mathcal{D}|_\sim$ such that $[x]_\sim \preceq_\sim [y]_\sim \Leftrightarrow \exists x' \in [x]_\sim, y' \in [y]_\sim.\ x' \preceq y'$. Thus, if $\preceq$ is a preorder on $\mathcal{D}$, then $\preceq_\sim$ is a partial order on the corresponding quotient set $\mathcal{D}|_\sim$.

CPO and Lattices. A *complete partial order* (i.e. *CPO*) is a poset $\langle \mathcal{D}, \sqsubseteq, \bot, \sqcup \rangle$ with infimum $\bot$ such that any denumerable ascending chain $\{x_i \in \mathcal{D} \mid i \in \mathbb{N}\}$ has a least upper bound $\sqcup_{i \in \mathbb{N}}\ x_i \in \mathcal{D}$. A *lattice* is a poset $\langle \mathcal{D}, \sqsubseteq, \sqcup, \sqcap \rangle$ such that every pair of elements x, y has a least upper bound $x \sqcup y$ and a greatest lower bound $x \sqcap y$ in $\mathcal{D}$, thus every finite subset of $\mathcal{D}$ has a least upper bound and a greatest lower bound. A *complete lattice* $\langle \mathcal{D}, \sqsubseteq, \bot, \top, \sqcup, \sqcap \rangle$ is a lattice in which any arbitrary (possibly infinite)

subset $S \in \wp(\mathcal{D})$ has a least upper bound $\sqcup S$, hence a complete lattice has a supremum $\top = \sqcup \mathcal{D}$ and an infimum $\bot = \sqcup \emptyset$.

Galois Connections and Abstraction. In the abstract interpretation framework, Galois connections are used to formalize the correspondence between concrete properties (e.g. sets of traces) and abstract properties (e.g. sets of reachable states) in case there is always a most precise abstract property over-approximating any concrete property. Given two posets $\langle \mathcal{D}, \sqsubseteq \rangle$ (called the *concrete domain*) and $\langle \mathcal{D}^\sharp, \sqsubseteq^\sharp \rangle$ (called the *abstract domain*), the pair $\langle \alpha, \gamma \rangle$ of functions $\alpha \in \mathcal{D} \mapsto \mathcal{D}^\sharp$ (called the *abstraction function* or lower/left adjoint) and $\gamma \in \mathcal{D}^\sharp \mapsto \mathcal{D}$ (called the *concretization function* or upper/right adjoint) forms a *Galois connection* if and only if $\forall x \in \mathcal{D}.\, \forall y^\sharp \in \mathcal{D}^\sharp.\, \alpha(x) \sqsubseteq^\sharp y^\sharp \Leftrightarrow x \sqsubseteq \gamma(y^\sharp)$. Such a Galois connection is denoted as:

$$\langle \mathcal{D}, \sqsubseteq \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathcal{D}^\sharp, \sqsubseteq^\sharp \rangle.$$

The above definition of Galois connections is equivalent to have α and γ such that: (1) α is increasing (monotonic); (2) γ is increasing (monotonic); (3) $\gamma \circ \alpha$ is extensive (i.e. $\forall x \in \mathcal{D}.\, x \sqsubseteq \gamma(\alpha(x))$); (4) $\alpha \circ \gamma$ is reductive (i.e. $\forall y^\sharp \in \mathcal{D}.\, y^\sharp \sqsubseteq \alpha(\gamma(y^\sharp))$).

The intuition of Galois connections is that the concrete properties in $\mathcal{D}$ are approximated by abstract properties in $\mathcal{D}^\sharp$: $\alpha(x)$ is the best (most precise) sound over-approximation of x in the abstract domain $\mathcal{D}$, and $\gamma(y^\sharp)$ is the least precise element of $\mathcal{D}$ that can be over-approximated by $y^\sharp$. The abstraction of a concrete property $x \in \mathcal{D}$ is said to be *exact* whenever $\gamma(\alpha(x)) = x$, which means that the abstraction $\alpha(x)$ of property x loses no information at all. In addition, we say that $y^\sharp \in \mathcal{D}^\sharp$ is a *sound abstraction* of $x \in \mathcal{D}$ if and only if $x \sqsubseteq \gamma(y^\sharp)$.

Fixpoints. For a poset $\langle \mathcal{D}, \sqsubseteq \rangle$, a *fixpoint* of a function (or transformer) $f \in \mathcal{D} \mapsto \mathcal{D}$ is an element $x \in \mathcal{D}$ such that $f(x) = x$. We denote $\text{lfp}^{\sqsubseteq} f$ as the *least fixpoint* of f, and $\text{gfp}^{\sqsubseteq} f$ as the *greatest fixpoint* of f, if they do exist. $\text{lfp}^{\sqsubseteq}_{a} f$ is the least fixpoint of f, which is $\sqsubseteq$ - greater than or equal to $a \in \mathcal{D}$, if any. Dually, $\text{gfp}^{\sqsubseteq}_{a} f$ is the greatest fixpoint of f, which is $\sqsubseteq$ - less than or equal to $a \in \mathcal{D}$. When the partial order $\sqsubseteq$ is understood from the context, it can be omitted, and we write $\text{lfp}\, f$ or $\text{gfp}\, f$.

(**Tarski Fixpoint Theorem** [59]) An increasing function $f \in \mathcal{D} \mapsto \mathcal{D}$ on a complete lattice $\langle \mathcal{D}, \sqsubseteq, \bot, \top, \sqcup, \sqcap \rangle$ has a least fixpoint $\text{lfp}^{\sqsubseteq} f = \sqcap \{x \in \mathcal{D} \mid f(x) \sqsubseteq x\}$.

(**David Park Conjugate Fixpoint Theorem** [8, 9]) Let S be a set, $f \in \wp(S) \mapsto \wp(S)$ be a $\subseteq$-increasing function on the complete lattice $\langle \wp(S), \subseteq, \emptyset, S, \cup, \cap \rangle$, and $\neg X \triangleq S \backslash X$ be the set complement. If we define $\tilde{f} \triangleq X \mapsto \neg f(\neg X)$, then $\text{gfp}^{\subseteq} f = \neg \text{lfp}^{\subseteq} \tilde{f}$.

Fixpoint Abstraction. All kinds of program semantics can be expressed as fixpoints of increasing transformers in posets. Given an abstraction $\langle \mathcal{D}, \sqsubseteq \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathcal{D}^\sharp, \sqsubseteq^\sharp \rangle$ of a concrete domain $\mathcal{D}$ into an abstract domain $\mathcal{D}^\sharp$ and an increasing concrete transformer $f \in \mathcal{D} \mapsto \mathcal{D}$, we would like to abstract the semantics expressed as $\text{lfp}^{\sqsubseteq} f$ in the concrete domain into a least fixpoint $\text{lfp}^{\sqsubseteq^\sharp} f^\sharp$ in the abstract domain, where $f^\sharp \in \mathcal{D}^\sharp \mapsto \mathcal{D}^\sharp$ is an abstract transformer. If $\alpha(\text{lfp}^{\sqsubseteq} f) = \text{lfp}^{\sqsubseteq^\sharp} f^\sharp$, this abstraction is exact; if $\alpha(\text{lfp}^{\sqsubseteq} f) \sqsubset^\sharp \text{lfp}^{\sqsubseteq^\sharp} f^\sharp$, we get an over-approximation of $\text{lfp}^{\sqsubseteq} f$, but the abstraction is still sound.

Let the concrete domain $\langle \mathcal{D}, \sqsubseteq, \bot, \top, \sqcup, \sqcap \rangle$ and the abstract domain $\langle \mathcal{D}^\sharp, \sqsubseteq^\sharp, \bot^\sharp, \top^\sharp, \sqcup^\sharp, \sqcap^\sharp \rangle$ be two complete lattices, $\langle \mathcal{D}, \sqsubseteq \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathcal{D}^\sharp, \sqsubseteq^\sharp \rangle$ be a Galois connection between the two domains, $f \in \mathcal{D} \mapsto \mathcal{D}$ and $f^\sharp \in \mathcal{D}^\sharp \mapsto \mathcal{D}^\sharp$ be increasing transformers. If $\alpha \circ f \circ \gamma \mathbin{\dot{\sqsubseteq}^\sharp} f^\sharp$ (where $\dot{\sqsubseteq}^\sharp$ is defined pointwise such that $f^\sharp \dot{\sqsubseteq}^\sharp g^\sharp \Leftrightarrow \forall x^\sharp \in \mathcal{D}^\sharp.\ f^\sharp(x^\sharp) \sqsubseteq^\sharp g^\sharp(x^\sharp)$), then we have $\text{lfp}^{\sqsubseteq} f \sqsubseteq^\sharp \gamma(\text{lfp}^{\sqsubseteq^\sharp} f^\sharp)$.

Fixpoint Approximation by Extrapolation with Widening. In the case where the abstract domain has infinite increasing chains (e.g. in interval domain, polyhedron domain, octagon domain, etc.), the sequences of abstract iterations are not guaranteed to terminate in finitely many steps. In [3], a widening operator is introduced to replace the abstract join operator such that the iteration convergence is guaranteed.

A *widening* is a binary operator $\triangledown \in (\mathcal{D}^\sharp \times \mathcal{D}^\sharp) \mapsto \mathcal{D}^\sharp$ on the abstract domain $\mathcal{D}^\sharp$ such that: (1) $\forall x^\sharp, y^\sharp \in \mathcal{D}^\sharp.\ x^\sharp \sqsubseteq^\sharp x^\sharp \triangledown y^\sharp \wedge y^\sharp \sqsubseteq^\sharp x^\sharp \triangledown y^\sharp$; (2) for any sequence $(x_i^\sharp)_{i\in\mathbb{N}}$, the sequence $(y_i^\sharp)_{i\in\mathbb{N}}$ defined as $y_0^\sharp = x_0^\sharp$ and $\forall i \in \mathbb{N}.\ y_{i+1}^\sharp = y_i^\sharp \triangledown x_{i+1}^\sharp$ converges in finite time. The following theorem shows that we can compute a sound over-approximation of concrete semantics expressed by a least fixpoint in a finite number of iterations with widening operators.

(**Cousot and Cousot Upward Iteration with Widening Theorem** [3, 5]) Given a concretization function $\gamma \in \mathcal{D}^\sharp \mapsto \mathcal{D}$, we assume that the abstract transformer $f^\sharp \in \mathcal{D}^\sharp \mapsto \mathcal{D}^\sharp$ is a sound abstraction of the concrete transformer $f \in \mathcal{D} \mapsto \mathcal{D}$ (i.e. $f \circ \gamma \sqsubseteq \gamma \circ f^\sharp$). Let $x \in \mathcal{D}$, $x^\sharp \in \mathcal{D}^\sharp$ such that $x \sqsubseteq \gamma(x^\sharp)$. Then, the sequence $(y_i^\sharp)_{i\in\mathbb{N}}$ defined as $y_0^\sharp = x^\sharp$ and $\forall i \in \mathbb{N}.\ y_{i+1}^\sharp = y_i^\sharp \triangledown f^\sharp(y_i^\sharp)$ is ultimately stationary and its limit $\lim (y_i^\sharp)_{i\in\mathbb{N}}$ is a sound approximation of $\mathrm{lfp}_x\ f$, that is to say, $\mathrm{lfp}_x\ f \sqsubseteq \gamma(\lim (y_i^\sharp)_{i\in\mathbb{N}})$.

Fixpoint Approximation by Interpolation with Narrowing. Suppose the limit of the sequence $(y_i^\sharp)_{i\in\mathbb{N}}$ is $y_n^\sharp$ such that $y_n^\sharp \triangledown f^\sharp(y_n^\sharp) = y_n^\sharp$. In many cases, $y_n^\sharp$ is a strict post-fixpoint of the function $f^\sharp$ (i.e. $f^\sharp(y_n^\sharp) \sqsubset^\sharp y_n^\sharp$), thus the over-approximation $y_n^\sharp$ can be refined by applying $f^\sharp$ for a few more times without using the widening $\triangledown$, and get a new sequence $(z_i^\sharp)_{i\in\mathbb{N}}$ that is defined as $z_0^\sharp = y_n^\sharp$ and $\forall i \in \mathbb{N}.\ z_{i+1}^\sharp = f^\sharp(z_i^\sharp)$. However, such a sequence may not terminate, since the abstract domain $\in \mathcal{D}^\sharp$ could have infinite

decreasing chains. To guarantee the termination of this refinement, a narrowing operator is proposed in [3].

A *narrowing* is a binary operator $\triangle \in (\mathcal{D}^\sharp \times \mathcal{D}^\sharp) \mapsto \mathcal{D}^\sharp$ on the abstract domain $\mathcal{D}^\sharp$ such that: (1) $\forall x^\sharp, y^\sharp \in \mathcal{D}^\sharp.\ y^\sharp \sqsubseteq^\sharp x^\sharp \Rightarrow y^\sharp \sqsubseteq^\sharp (x^\sharp \triangle y^\sharp) \sqsubseteq^\sharp x^\sharp$; (2) for any sequence $(x_i^\sharp)_{i\in\mathbb{N}}$, the sequence $(y_i^\sharp)_{i\in\mathbb{N}}$ defined as $y_0^\sharp = x_0^\sharp$ and $\forall i \in \mathbb{N}.\ y_{i+1}^\sharp = y_i^\sharp \triangle x_{i+1}^\sharp$ converges in finite time. The following theorem shows that we can refine an over-approximation of a fixpoint by decreasing iterations with narrowing operators.

(**Cousot and Cousot Downward Iteration with Narrowing Theorem** [3, 5]) Given a concretization function $\gamma \in \mathcal{D}^\sharp \mapsto \mathcal{D}$, we assume that the abstract transformer $f^\sharp \in \mathcal{D}^\sharp \mapsto \mathcal{D}^\sharp$ is a sound abstraction of the concrete transformer $f \in \mathcal{D} \mapsto \mathcal{D}$ (i.e. $f \circ \gamma \sqsubseteq \gamma \circ f^\sharp$). Let $x \in \mathcal{D}$, $y^\sharp \in \mathcal{D}^\sharp$ such that $\mathrm{lfp}_x\ f \sqsubseteq \gamma(y^\sharp)$. Then, the sequence $(z_i^\sharp)_{i\in\mathbb{N}}$ defined as $z_0^\sharp = y^\sharp$ and $\forall i \in \mathbb{N}.\ z_{i+1}^\sharp = z_i^\sharp \triangle f^\sharp(z_i^\sharp)$ is ultimately stationary, and its limit $\lim (z_i^\sharp)_{i\in\mathbb{N}}$ is a sound approximation of $\mathrm{lfp}_x\ f$ that is more precise than $y^\sharp$. That is to say, $\mathrm{lfp}_x\ f \sqsubseteq \gamma(\lim (z_i^\sharp)_{i\in\mathbb{N}}) \sqsubseteq \gamma(y^\sharp)$.

2.2 Abstract Domains

The concrete trace semantics of transition systems introduced in Section 1.2 is not computable in general, thus we propose to abstract sets of concrete traces into invariants. In order to accomplish that, this section introduces the abstract environment domain, the concrete invariant domain and the abstract invariant domain.

2.2.1 Abstract Environment Domain

Let $\langle \mathcal{D}^\sharp_{\mathbb{M}}, \sqsubseteq^\sharp_{\mathbb{M}}, \bot^\sharp_{\mathbb{M}}, \top^\sharp_{\mathbb{M}}, \sqcup^\sharp_{\mathbb{M}}, \sqcap^\sharp_{\mathbb{M}} \rangle$ be an *abstract environment domain*, and $\gamma_{\mathbb{M}} \in \mathcal{D}^\sharp_{\mathbb{M}} \mapsto \wp(\mathbb{M})$ be the corresponding concretization function that associates each abstract element $\mathrm{M}^\sharp \in \mathcal{D}^\sharp_{\mathbb{M}}$ to the set of concrete environments it represents. In particular, $\mathcal{D}^\sharp_{\mathbb{M}}$ features an infimum $\bot^\sharp_{\mathbb{M}}$ and a supremum $\top^\sharp_{\mathbb{M}}$ such that $\gamma_{\mathbb{M}}(\bot^\sharp_{\mathbb{M}}) = \emptyset$ and $\gamma_{\mathbb{M}}(\top^\sharp_{\mathbb{M}}) = \mathbb{M}$, and an abstract join operator $\sqcup^\sharp_{\mathbb{M}}$ that soundly approximates the concrete join operator $\cup$ (more precisely, $\forall \mathrm{M}, \mathrm{M}' \in \wp(\mathbb{M}), \mathrm{M}^\sharp, \mathrm{M}^{\sharp\prime} \in \mathcal{D}^\sharp_{\mathbb{M}}.\ (\mathrm{M} \subseteq \gamma_{\mathbb{M}}(\mathrm{M}^\sharp) \wedge \mathrm{M}' \subseteq \gamma_{\mathbb{M}}(\mathrm{M}^{\sharp\prime})) \Rightarrow \mathrm{M} \cup \mathrm{M}' \subseteq \gamma_{\mathbb{M}}(\mathrm{M}^\sharp \sqcup^\sharp_{\mathbb{M}} \mathrm{M}^{\sharp\prime})$).

This dissertation focuses on the analysis of numerical programs, and takes three popular abstract domains that can express constraints on program variables as examples. The *interval domain* introduced in [6] bounds the value of numerical variables by minimal and maximal values between which all reachable values of a variable must stand, and each abstract element in this domain can be defined as a mapping from program variables to intervals (e.g. $x \in [l, h] \wedge y \in [l', h']$). It is a simple but useful domain, and it has been applied not only to prove the absence of integers or array index overflows but also to detect unseen inputs of neural networks [49]. However, the interval domain is not expressive enough to be useful for a relational reachability analysis, in which the constraints involving more than one variable are needed. One example of relational abstractions is the *polyhedra domain* introduced in [7] that can express conjunctions of affine inequalities on variables. In this domain, an abstract element (i.e. polyhedron) is defined as a finite set of affine constraints of form $\vec{a} \cdot \vec{x} \geq b$ (e.g. $2 * x - 3 * y + 5 * z \geq 4$), where $\vec{x}$ denotes the vector of all variables, $\vec{a}$ denotes a vector of coefficients and b denotes a constant. In addition, strict inequalities are supported in current polyhedron domain

[21, 41, 10] . Another example is the *octagon domain* introduced in [31, 18, 38], which restricts the affine constraints used in the polyhedron domain to unit binary inequality constraints of form $\pm x_1 \pm x_2 \leq c$ (e.g. $x - y \leq 0$). The above three numerical domains are similar semantically in that they infer conjunctions of inequality constraints and represent convex sets, but they are based on different algorithms and achieve different trade-offs between precision and efficiency. Operators in the interval domain have a linear cost in the number of variables, while octagon operators have a cubic cost. The cost of polyhedra is unbounded in theory (since it can construct arbitrarily many constraints), but it is exponential in practice [56, 42].

It is assumed that, for every concrete environment transfer function $\mathrm{F} \in \wp(\mathbb{M}) \mapsto \wp(\mathbb{M})$ specified for atomic actions in the program (e.g. $\tau\{\!|\, x := \mathit{expr} \,|\!\}$ and $\tau\{\!|\, \mathit{bexpr} \,|\!\}$ for the simple language described in Fig.1.3), the abstract environment domain $\mathcal{D}^\sharp_\mathbb{M}$ (e.g. interval/polyhedron/octagon) provides a sound abstract function $\mathrm{F}^\sharp \in \mathcal{D}^\sharp_\mathbb{M} \mapsto \mathcal{D}^\sharp_\mathbb{M}$, such that the soundness condition $\forall \mathrm{M}^\sharp \in \mathcal{D}^\sharp_\mathbb{M}.\ (\mathrm{F} \circ \gamma_\mathbb{M})(\mathrm{M}^\sharp) \subseteq (\gamma_\mathbb{M} \circ \mathrm{F}^\sharp)(\mathrm{M}^\sharp)$ holds.

In addition, it is worth noting that, in some abstract domains, we have an abstraction function $\alpha_\mathbb{M} \in \wp(\mathbb{M}) \mapsto \mathcal{D}^\sharp_\mathbb{M}$ such that $\alpha_\mathbb{M}$ and $\gamma_\mathbb{M}$ form a Galois connection $\langle \wp(\mathbb{M}), \subseteq \rangle \underset{\alpha_\mathbb{M}}{\overset{\gamma_\mathbb{M}}{\leftrightarrows}} \langle \mathcal{D}^\sharp_\mathbb{M}, \sqsubseteq^\sharp_\mathbb{M} \rangle$. In this case, every concrete element $\mathrm{M} \subseteq \mathbb{M}$ (i.e. every set of concrete environments) has a best abstraction $\alpha_\mathbb{M}(\mathrm{M}) \in \mathcal{D}^\sharp_\mathbb{M}$, and every function $\mathrm{F} \in \wp(\mathbb{M}) \mapsto \wp(\mathbb{M})$ in the concrete domain has also a best abstraction $\alpha_\mathbb{M} \circ \mathrm{F} \circ \gamma_\mathbb{M} \in \mathcal{D}^\sharp_\mathbb{M} \mapsto \mathcal{D}^\sharp_\mathbb{M}$. Specifically, the interval and octagon domain have this desirable property, while the polyhedron domain does not.

Example 3 (Access Control, Continued) *For the access control program in Fig. 1.4, it is sufficient to use the interval domain as $\mathcal{D}^\sharp_\mathbb{M}$ to express environment properties such as "the*

access to o fails" (i.e. the value of acs is less than or equal to 0 *at point* ℓ_8*), since no relational constraints on variables are required. To be more precise, the abstract environment element* $\mathrm{M}^\sharp = \mathit{apv} \in [\text{-}\infty, \infty] \wedge \mathit{i1} \in [\text{-}\infty, \infty] \wedge \mathit{i2} \in [\text{-}\infty, \infty] \wedge \mathit{typ} \in [\text{-}\infty, \infty] \wedge \mathit{acs} \in [\text{-}\infty, 0]$ *represents the set of environments* $\gamma_{\mathbb{M}}(\mathrm{M}^\sharp) = \{\rho \in \mathbb{M} \mid \rho(\mathit{acs}) \leq 0\}$*, in which the value of variable acs is less than or equal to 0 while the values of other variables are arbitrary. Similarly, an environment property "the access to o succeeds" (i.e. the value of acs is greater than or equal to* 1 *at point* ℓ_8*) can be over-approximated by* $\mathrm{M}^{\sharp\prime} = \mathit{apv} \in [\text{-}\infty, \infty] \wedge \mathit{i1} \in [\text{-}\infty, \infty] \wedge \mathit{i2} \in [\text{-}\infty, \infty] \wedge \mathit{typ} \in [\text{-}\infty, \infty] \wedge \mathit{acs} \in [1, \infty]$. □

2.2.2 Concrete Invariant Domain

For any set $\mathcal{T}$ of concrete traces (which can be either the program semantics or a trace property), we would like to abstract it into an invariant, which collects the set of environments for each program point that are visited by traces in $\mathcal{T}$. Hence, the *concrete invariant domain* $\mathcal{D}_{\mathbb{I}}$ is defined as $\langle \mathbb{L} \mapsto \wp(\mathbb{M}),\ \dot{\subseteq} \rangle$, and there exists a Galois connection between concrete traces and the concrete invariant domain $\mathcal{D}_{\mathbb{I}}$.

$$\langle \wp(\mathbb{S}^{*\infty}),\ \subseteq \rangle \underset{\alpha_{\mathbb{I}}}{\overset{\gamma_{\mathbb{I}}}{\leftrightarrows}} \langle \mathbb{L} \mapsto \wp(\mathbb{M}),\ \dot{\subseteq} \rangle.$$

where $\dot{\subseteq}$ is the pointwise inclusion relation, and $\alpha_{\mathbb{I}}$ and $\gamma_{\mathbb{I}}$ are defined as:

$$\begin{array}{rcll} \alpha_{\mathbb{I}} & \in & \wp(\mathbb{S}^{*\infty}) \mapsto (\mathbb{L} \mapsto \wp(\mathbb{M})) & \text{concrete invariant abstraction} \\ \alpha_{\mathbb{I}}(\mathcal{T})\ell & \triangleq & \{\rho \in \mathbb{M} \mid \exists \sigma \in \mathcal{T}.\ \langle \ell,\ \rho \rangle \in \sigma\} & \\ \gamma_{\mathbb{I}} & \in & (\mathbb{L} \mapsto \wp(\mathbb{M})) \mapsto \wp(\mathbb{S}^{*\infty}) & \text{concrete invariant concretization} \\ \gamma_{\mathbb{I}}(\mathsf{I}) & \triangleq & \{\sigma \in \mathbb{S}^{*\infty} \mid \forall \langle \ell,\ \rho \rangle \in \sigma.\ \rho \in \mathsf{I}(\ell)\} & \end{array}$$

Proof. For any $\mathcal{T} \in \wp(\mathbb{S}^{*\infty})$ and $\mathsf{I} \in \mathbb{L} \mapsto \wp(\mathbb{M})$, we can prove that

$$\alpha_{\mathbb{I}}(\mathcal{T}) \dot{\subseteq} \mathsf{I}$$

$$\Leftrightarrow \forall \ell \in \mathbb{L}.\ \alpha_{\mathbb{I}}(\mathcal{T})\ell \subseteq \mathsf{I}(\ell) \qquad \text{⟅def. } \dot{\subseteq}\text{⟆}$$

$$\Leftrightarrow \forall \ell \in \mathbb{L}.\ \{\rho \in \mathbb{M} \mid \exists \sigma \in \mathcal{T}.\ \langle \ell,\ \rho\rangle \in \sigma\} \subseteq \mathsf{I}(\ell) \qquad \text{⟅def. } \alpha_{\mathbb{I}}(S)\ell\text{⟆}$$

$$\Leftrightarrow \forall \ell \in \mathbb{L}.\ \forall \rho \in \mathbb{M}.\ (\exists \sigma \in \mathcal{T}.\ \langle \ell,\ \rho\rangle \in \sigma) \Rightarrow \rho \in \mathsf{I}(\ell) \qquad \text{⟅def. } \subseteq\text{⟆}$$

$$\Leftrightarrow \forall \ell \in \mathbb{L}.\ \forall \rho \in \mathbb{M}.\ \forall \sigma \in \mathbb{S}^{*\infty}.\ (\sigma \in \mathcal{T} \wedge \langle \ell,\ \rho\rangle \in \sigma) \Rightarrow \rho \in \mathsf{I}(\ell) \qquad \text{⟅def. } \exists\text{⟆}$$

$$\Leftrightarrow \forall \sigma \in \mathcal{T}.\ \forall \langle \ell,\ \rho\rangle \in \sigma.\ \rho \in \mathsf{I}(\ell) \qquad \text{⟅def. } \forall \text{ and } \Rightarrow\text{⟆}$$

$$\Leftrightarrow \mathcal{T} \subseteq \{\sigma \in \mathbb{S}^{*\infty} \mid \forall \langle \ell,\ \rho\rangle \in \sigma.\ \rho \in \mathsf{I}(\ell)\} \qquad \text{⟅def. } \subseteq\text{⟆}$$

$$\Leftrightarrow \mathcal{T} \subseteq \gamma_{\mathbb{I}}(\mathsf{I}) \qquad \text{⟅def. } \gamma_{\mathbb{I}}\text{⟆}$$

By the above property, we have proved that $\alpha_{\mathbb{I}}$ and $\gamma_{\mathbb{I}}$ form a Galois connection. □

2.2.3 Abstract Invariant Domain

The concrete invariants introduced above can be further abstracted into abstract invariants, in which every set of concrete environments is represented by an abstract element in $\mathcal{D}^{\sharp}_{\mathbb{M}}$. Here we define the abstract invariant domain $\mathcal{D}^{\sharp}_{\mathbb{I}}$ as $\langle \mathbb{L} \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}}, \dot{\sqsubseteq}^{\sharp}_{\mathbb{M}}\rangle$, where the program points are mapped to abstract elements in $\mathcal{D}^{\sharp}_{\mathbb{M}}$, and $\dot{\sqsubseteq}^{\sharp}_{\mathbb{M}}$ is the pointwise ordering induced by $\sqsubseteq^{\sharp}_{\mathbb{M}}$ (i.e. $\forall \mathsf{I}^{\sharp}, \mathsf{I}^{\sharp\prime} \in \mathcal{D}^{\sharp}_{\mathbb{I}}.\ \mathsf{I}^{\sharp} \dot{\sqsubseteq}^{\sharp}_{\mathbb{M}} \mathsf{I}^{\sharp\prime} \Leftrightarrow (\forall \ell \in \mathbb{L}.\ \mathsf{I}^{\sharp}(\ell) \sqsubseteq^{\sharp}_{\mathbb{M}} \mathsf{I}^{\sharp\prime}(\ell))$). The corresponding concretization function $\dot{\gamma}_{\mathbb{M}}$ to the concrete invariant domain is:

$$\begin{array}{rcll} \dot{\gamma}_{\mathbb{M}} & \in & (\mathbb{L} \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}}) \mapsto (\mathbb{L} \mapsto \wp(\mathbb{M})) & \text{abstract invariant concretization} \\ \dot{\gamma}_{\mathbb{M}}(\mathsf{I}^{\sharp})\ell & \triangleq & \gamma_{\mathbb{M}}(\mathsf{I}^{\sharp}(\ell)) & \end{array}$$

Similar to the abstract environment domain, $\mathcal{D}^{\sharp}_{\mathbb{I}}$ features an infimum $\bot^{\sharp}_{\mathbb{I}} \triangleq \lambda \ell \in \mathbb{L}.\ \bot^{\sharp}_{\mathbb{M}}$ and a supremum $\top^{\sharp}_{\mathbb{I}} \triangleq \lambda \ell \in \mathbb{L}.\ \top^{\sharp}_{\mathbb{M}}$ such that $\dot{\gamma}_{\mathbb{M}}(\bot^{\sharp}_{\mathbb{I}}) = \lambda \ell \in \mathbb{L}.\ \emptyset$ and $\dot{\gamma}_{\mathbb{M}}(\top^{\sharp}_{\mathbb{I}}) = \lambda \ell \in \mathbb{L}.\ \mathbb{M}$. When the environment abstraction $\alpha_{\mathbb{M}} \in \wp(\mathbb{M}) \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}}$

does exist (e.g. in the interval or octagon domain), we can construct the corresponding pointwise abstraction function $\dot{\alpha}_{\mathbb{M}}$ for the abstract invariant domain:

$$\begin{array}{rcll} \dot{\alpha}_{\mathbb{M}} & \in & (\mathbb{L} \mapsto \wp(\mathbb{M})) \mapsto (\mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}) & \text{abstract invariant abstraction} \\ \dot{\alpha}_{\mathbb{M}}(\mathsf{I})\ell & \triangleq & \alpha_{\mathbb{M}}(\mathsf{I}(\ell)) & \end{array}$$

Furthermore, we can build a combination of Galois connections:

$$\langle \wp(\mathbb{S}^{*\infty}),\ \subseteq \rangle \underset{\alpha_{\mathbb{I}}}{\overset{\gamma_{\mathbb{I}}}{\leftrightarrows}} \langle \mathbb{L} \mapsto \wp(\mathbb{M}),\ \dot{\subseteq} \rangle \underset{\dot{\alpha}_{\mathbb{M}}}{\overset{\dot{\gamma}_{\mathbb{M}}}{\leftrightarrows}} \langle \mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}},\ \dot{\sqsubseteq}^\sharp_{\mathbb{M}} \rangle.$$

such that an abstract invariant $\mathsf{I}^\sharp \in \mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}$ over-approximates a set of concrete traces $\gamma_{\mathbb{I}} \circ \dot{\gamma}_{\mathbb{M}}(\mathsf{I}^\sharp) = \{\sigma \in \mathbb{S}^{*\infty} \mid \forall \langle \ell,\ \rho \rangle \in \sigma.\ \rho \in \gamma_{\mathbb{M}}(\mathsf{I}^\sharp(\ell))\}$. Specially, the bottom $\bot^\sharp_{\mathbb{I}}$ represents the empty set of concrete traces ($\gamma_{\mathbb{I}} \circ \dot{\gamma}_{\mathbb{M}}(\bot^\sharp_{\mathbb{I}}) = \emptyset$) and the top$\top^\sharp_{\mathbb{I}}$ represents the set of all possible traces ($\gamma_{\mathbb{I}} \circ \dot{\gamma}_{\mathbb{M}}(\bot^\sharp_{\mathbb{I}}) = \mathbb{S}^{*\infty}$).

Example 4 (Access Control, Continued) *For the access control program in Fig.1.4, its maximal trace semantics* $[\![\mathrm{P}]\!]^{\mathsf{Max}}$ *given in Example 2 can be over-approximated by an abstract invariant* $\mathsf{I}^\sharp \in \mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}$ *such that:* $\mathsf{I}^\sharp(\ell_1) = \top^\sharp_{\mathbb{M}} = apv \in [\text{-}\infty, \infty] \wedge i1 \in [\text{-}\infty, \infty] \wedge i2 \in [\text{-}\infty, \infty] \wedge typ \in [\text{-}\infty, \infty] \wedge acs \in [\text{-}\infty, \infty]$,

$\mathsf{I}^\sharp(\ell_2) = apv \in [1, 1] \wedge i1 \in [\text{-}\infty, \infty] \wedge i2 \in [\text{-}\infty, \infty] \wedge typ \in [\text{-}\infty, \infty] \wedge acs \in [\text{-}\infty, \infty]$,

$\mathsf{I}^\sharp(\ell_3) = apv \in [1, 1] \wedge i1 \in [\text{-}1, 2] \wedge i2 \in [\text{-}\infty, \infty] \wedge typ \in [\text{-}\infty, \infty] \wedge acs \in [\text{-}\infty, \infty]$,

$\mathsf{I}^\sharp(\ell_4) = apv \in [\text{-}1, 1] \wedge i1 \in [\text{-}1, 2] \wedge i2 \in [\text{-}\infty, \infty] \wedge typ \in [\text{-}\infty, \infty] \wedge acs \in [\text{-}\infty, \infty]$,

$\mathsf{I}^\sharp(\ell_5) = apv \in [\text{-}1, 1] \wedge i1 \in [\text{-}1, 2] \wedge i2 \in [\text{-}1, 2] \wedge typ \in [\text{-}\infty, \infty] \wedge acs \in [\text{-}\infty, \infty]$,

$\mathsf{I}^\sharp(\ell_6) = apv \in [\text{-}1, 1] \wedge i1 \in [\text{-}1, 2] \wedge i2 \in [\text{-}1, 2] \wedge typ \in [\text{-}\infty, \infty] \wedge acs \in [\text{-}\infty, \infty]$,

$\mathsf{I}^\sharp(\ell_7) = apv \in [\text{-}1, 1] \wedge i1 \in [\text{-}1, 2] \wedge i2 \in [\text{-}1, 2] \wedge typ \in [1, 2] \wedge acs \in [\text{-}\infty, \infty]$,

$\mathsf{I}^\sharp(\ell_8) = apv \in [\text{-}1, 1] \wedge i1 \in [\text{-}1, 2] \wedge i2 \in [\text{-}1, 2] \wedge typ \in [1, 2] \wedge acs \in [\text{-}2, 2]$.

In addition, the concrete trace property "the access to o fails" is over-approximated by another abstract invariant $\mathsf{I}^{\sharp\prime} \in \mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}$ *such that its abstract environment element attached*

to every program point is the same as $\mathsf{I}^\sharp$ *defined above, except the value bound of acs at point* ℓ_8 *is refined to* $[\text{-}2, 0]$. *More precisely, when* $\ell = \ell_8$, $\mathsf{I}^{\sharp\prime}(\ell) = \mathit{apv} \in [0,1] \wedge \mathit{i1} \in [0,1] \wedge \mathit{i2} \in [0,1] \wedge \mathit{typ} \in [1,2] \wedge \mathit{acs} \in [\text{-}2, 0]$*; otherwise,* $\mathsf{I}^{\sharp\prime}(\ell) = \mathsf{I}^\sharp(\ell)$. □

2.3 Forward Reachability Analysis

Given a program P, the corresponding forward reachability semantics specifies the set of states that are possibly reachable at any program point for all executions of the program. Section 2.3.1 formalizes a variant of the classic forward reachability (invariant) semantics, which is defined as an abstraction of the program's intermediate trace semantics. Section 2.3.2 briefly presents an abstract forward reachability analysis that soundly over-approximates the concrete forward reachability semantics.

2.3.1 Forward Reachability Semantics

Classic Forward Reachability Semantics. In the literature, usually the forward reachability semantics of a program is defined as an abstraction of its prefix trace semantics, which attaches to each program point a set of environments that are possibly encountered during any execution from a given set of initial environments. More precisely, given a set of initial environments $\mathrm{M}^i \in \wp(\mathbb{M})$, the forward reachability semantics $\mathcal{S}_{\vec{\tau}}[\![\mathrm{P}]\!](\mathrm{M}^i) \in \mathbb{L} \mapsto \wp(\mathbb{M})$ is defined as a mapping from each program point ℓ to a set of environments at ℓ that are reachable from M^i. The formal definition is given as below, where $\langle \ell^i,\ \rho^i \rangle \sigma \langle \ell,\ \rho \rangle$ denotes the concatenation of an initial state $\langle \ell^i,\ \rho^i \rangle$, a (possibly empty) finite trace σ and a state $\langle \ell,\ \rho \rangle$. Specially, if σ is empty and $\langle \ell,\ \rho \rangle$ is

equal to $\langle \ell^i,\ \rho^i \rangle$, then $\langle \ell^i,\ \rho^i \rangle \sigma \langle \ell,\ \rho \rangle$ represents a trace with only one state $\langle \ell^i,\ \rho^i \rangle$.

$$\begin{array}{rcll} \mathcal{S}_{\overrightarrow{r}}[\![\mathrm{P}]\!] & \in & \wp(\mathbb{M}) \mapsto (\mathbb{L} \mapsto \wp(\mathbb{M})) & \text{classic forward reachability semantics} \\ \mathcal{S}_{\overrightarrow{r}}[\![\mathrm{P}]\!](\mathrm{M}^i)\ell & \triangleq & \{\rho \in \mathbb{M} \mid \exists \sigma \in \mathbb{S}^*, \rho^i \in \mathrm{M}^i.\ \langle \ell^i,\ \rho^i \rangle \sigma \langle \ell,\ \rho \rangle \in [\![\mathrm{P}]\!]^{\mathsf{Pref}}\} & \end{array}$$

The classic forward reachability semantics defined above specifies an invariant property of the program executions. If the set of initial environments M^i is taken as a precondition, then $\mathcal{S}_{\overrightarrow{r}}[\![\mathrm{P}]\!](\mathrm{M}^i)\ell$ is an invariant at ℓ, which holds if and when the execution of P starting with an initial state satisfying M^i reaches program point ℓ. Such a forward reachability semantics is quite useful in verifying program correctness.

Forward (Possible Success) Reachability Semantics In order to build a Galois connection between the forward reachability semantics and the backward accessibility semantics (defined in Section 2.4) and facilitate the trace partitioning by invariants during the forward reachability analysis (introduced later in Chapter 3), here we define a variant of forward reachability semantics, in which the considered execution traces are not required to start from the initial point ℓ^i.

To be more precise, instead of collecting reachable states from a set of initial environments M^i, here the precondition $\mathsf{I}_{\mathsf{pre}} \in \mathbb{L} \mapsto \wp(\mathbb{M})$ is specified by sets of environments attached to any (not necessarily initial) program point, and the forward (possible success) reachability semantics $\mathcal{S}_{\overrightarrow{ps}}[\![\mathrm{P}]\!]$ collects all the reachable states in the intermediate execution traces, which start from states satisfying the precondition $\mathsf{I}_{\mathsf{pre}}$.

$$\begin{array}{rcll} \mathcal{S}_{\overrightarrow{ps}}[\![\mathrm{P}]\!] & \in & (\mathbb{L} \mapsto \wp(\mathbb{M})) \mapsto (\mathbb{L} \mapsto \wp(\mathbb{M})) & \text{forward reachability semantics} \\ \mathcal{S}_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{pre}})\ell' & \triangleq & \{\rho' \in \mathbb{M} \mid \exists \sigma \in \mathbb{S}^*, \ell \in \mathbb{L}, \rho \in \mathsf{I}_{\mathsf{pre}}(\ell).\ \langle \ell,\ \rho \rangle \sigma \langle \ell',\ \rho' \rangle \in [\![\mathrm{P}]\!]^{\mathsf{It}}\} & \end{array}$$

Given a precondition $\mathsf{I}_{\mathsf{pre}} \in \mathbb{L} \mapsto \wp(\mathbb{M})$, the forward (possible success) reachability semantics $\mathcal{S}_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{pre}})\ell$ specifies an invariant at each point ℓ, which holds if and when

an execution of P starting with a state satisfying $\mathsf{I}_{\mathsf{pre}}$ reaches the point ℓ.

In order to distinguish from the classic forward reachability semantics and the forward impossible failure reachability semantics introduced in section 2.5, the semantics $\mathcal{S}_{\overrightarrow{ps}}[\![\mathrm{P}]\!]$ defined above is formally named "*forward possible success reachability semantics*". Nevertheless, in the rest of this dissertation, the notation of *forward reachability semantics* (where "possible success" or its abbreviation "ps" is omitted) refers to $\mathcal{S}_{\overrightarrow{ps}}[\![\mathrm{P}]\!]$.

It is easy to see that the classic forward reachability semantics $\mathcal{S}_{\overrightarrow{r}}[\![\mathrm{P}]\!] \in \wp(\mathbb{M}) \mapsto (\mathbb{L} \mapsto \wp(\mathbb{M}))$ is an abstraction of our definition $\mathcal{S}_{\overrightarrow{ps}}[\![\mathrm{P}]\!] \in (\mathbb{L} \mapsto \wp(\mathbb{M})) \mapsto (\mathbb{L} \mapsto \wp(\mathbb{M}))$, and $\mathcal{S}_{\overrightarrow{r}}[\![\mathrm{P}]\!](\mathrm{M}^i)$ is equal to $\mathcal{S}_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{pre}})$ if $\mathsf{I}_{\mathsf{pre}} = \lambda \ell \in \mathbb{L}.\ (\ell == \ell^i)\ ?\ \mathrm{M}^i : \emptyset$.

Forward (Possible Success) Reachability Semantics in Fixpoint Form. The forward reachability semantics $\mathcal{S}_{\overrightarrow{ps}}[\![\mathrm{P}]\!]$ of a program $\mathrm{P} = \langle \mathbb{S}^i,\ \rightarrow \rangle$ can be defined by structural induction on the language-specific syntax of the program, or in the fixpoint form with a concrete forward transfer function $\mathrm{F}_{\overrightarrow{ps}}[\![\mathrm{P}]\!]$:

$$
\begin{array}{rcll}
\mathcal{S}_{\overrightarrow{ps}}[\![\mathrm{P}]\!] & \in & (\mathbb{L} \mapsto \wp(\mathbb{M})) \mapsto (\mathbb{L} \mapsto \wp(\mathbb{M})) & \text{forward reachability semantics} \\
\mathcal{S}_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{pre}}) & \triangleq & \mathrm{lfp}^{\dot{\subseteq}}_{\mathsf{I}_{\mathsf{pre}}}\ \mathrm{F}_{\overrightarrow{ps}}[\![\mathrm{P}]\!] & \\
\mathrm{F}_{\overrightarrow{ps}}[\![\mathrm{P}]\!] & \in & (\mathbb{L} \mapsto \wp(\mathbb{M})) \mapsto (\mathbb{L} \mapsto \wp(\mathbb{M})) & \text{forward transfer function} \\
\mathrm{F}_{\overrightarrow{ps}}[\![\mathrm{P}]\!]\mathsf{I} & \triangleq & \mathsf{I} \mathbin{\dot{\cup}} \lambda \ell' \in \mathbb{L}.\{\rho' \in \mathbb{M} \mid \exists \ell \in \mathbb{L}, \rho \in \mathsf{I}(\ell).\ \langle \ell,\ \rho \rangle \rightarrow \langle \ell',\ \rho' \rangle\} &
\end{array}
$$

where $\dot{\subseteq}$ and $\dot{\cup}$ are pointwise extensions of the standard inclusion relation $\subseteq$ and union operator $\cup$, respectively.

Essentially, the monotonic function $\mathrm{F}_{\overrightarrow{ps}}[\![\mathrm{P}]\!]$ described above can be constructed by combining atomic forward transfer functions, each of which is typically defined for an atomic action (instruction / computation step) in the program and associates a set of environments before the action with the set of environments reachable after the action.

More formally, here we assume that for every pair of program points $\langle \ell,\ \ell' \rangle$ in the program P, an atomic transfer function $\mathrm{F}_{\ell\to\ell'}[\![\mathrm{P}]\!] \in \wp(\mathbb{M}) \mapsto \wp(\mathbb{M})$ is provided such that for any set M of environments at point ℓ, the function $\mathrm{F}_{\ell\to\ell'}[\![\mathrm{P}]\!](\mathrm{M})$ returns the set of environments at point ℓ' that are reachable from M: (1) if $\ell = \ell'$, then $\mathrm{F}_{\ell\to\ell'}[\![\mathrm{P}]\!](\mathrm{M}) = \mathrm{M}$; (2) if $\ell \neq \ell'$ and there is not an atomic action from ℓ to ℓ', then $\mathrm{F}_{\ell\to\ell'}[\![\mathrm{P}]\!](\mathrm{M}) = \emptyset$; and (3) otherwise, there is an atomic action from ℓ to ℓ', then $\mathrm{F}_{\ell\to\ell'}[\![\mathrm{P}]\!](\mathrm{M})$ is the set of environments after executing the action from M. Take the simple language in Fig.1.2 as an example, there are only two types of atomic actions: for an assignment ${}^{\ell_1}x := e^{\ell_2}$, the corresponding atomic transfer function $\mathrm{F}_{\ell_1\to\ell_2}[\![\mathrm{P}]\!](\mathrm{M}) = \tau\{\!|x := e|\!\}\mathrm{M}$, which is defined in Fig. 1.3; similarly, for a boolean test ${}^{\ell_1}b^{\ell_2}$, the corresponding atomic transfer function $\mathrm{F}_{\ell_1\to\ell_2}[\![\mathrm{P}]\!](\mathrm{M}) = \tau\{\!|b|\!\}\mathrm{M}$.

Therefore, the definition of forward transfer function $\mathrm{F}_{\overrightarrow{ps}}[\![\mathrm{P}]\!]$ can be rephrased into:

$$\begin{array}{lcll} \mathrm{F}_{\overrightarrow{ps}}[\![\mathrm{P}]\!] & \in & (\mathbb{L} \mapsto \wp(\mathbb{M})) \mapsto (\mathbb{L} \mapsto \wp(\mathbb{M})) & \text{forward transfer function} \\ \mathrm{F}_{\overrightarrow{ps}}[\![\mathrm{P}]\!]\mathsf{I} & \triangleq & \lambda\ell' \in \mathbb{L}.\ \cup_{\ell\in\mathbb{L}}\, \mathrm{F}_{\ell\to\ell'}[\![\mathrm{P}]\!](\mathsf{I}(\ell)) & \end{array}$$

Example 5 (Access Control, Continued) *Consider the access control program in Fig.1.4 again, the forward transfer function* $\mathrm{F}_{\overrightarrow{ps}}[\![\mathrm{P}]\!]$ *can be derived by combining the following atomic transfer functions:* $\tau\{\!|\ apv := 1\ |\!\}$, $\tau\{\!|\ i1 := [\text{-}1; 2]\ |\!\}$, $\tau\{\!|\ apv := (i1 \leq 0)\,?\,\text{-}1 : apv\ |\!\}$, $\tau\{\!|\ i2 := [\text{-}1; 2]\ |\!\}$, $\tau\{\!|\ apv := (apv \geq 1 \wedge i2 \leq 0)\,?\,\text{-}1 : apv\ |\!\}$, $\tau\{\!|\ typ := [1; 2]\ |\!\}$, *and* $\tau\{\!|acs := apv \times typ|\!\}$. *Then, from a precondition* $\mathsf{I}_{\mathsf{pre}} \in \mathbb{L} \mapsto \wp(\mathbb{M})$ *such that* $\mathsf{I}_{\mathsf{pre}}(\ell_1) = \mathbb{M}$ *and* $\mathsf{I}_{\mathsf{pre}}(\ell) = \emptyset$ *for* $\ell \neq \ell_1$, *we can compute the forward reachability semantics* $\mathcal{S}_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{pre}})$ *by the least fixpoint* $\mathrm{lfp}^{\dot{\subseteq}}_{\mathsf{I}_{\mathsf{pre}}}\ \mathrm{F}_{\overrightarrow{ps}}[\![\mathrm{P}]\!]$, *which is equal to the classic invariant semantics.*

To be more precise, the result $\mathcal{S}_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{pre}})$ *is listed in Table 2.1, in which the constraints on environment like "*$\rho(apv) = 1$*" is written as "*$apv = 1$*" for short.* □

ℓ	$\mathcal{S}_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{pre}})\ell$
ℓ_1	$\mathbb{M}$
ℓ_2	$\{\rho \in \mathbb{M} \mid \mathit{apv} = 1\}$
ℓ_3	$\{\rho \in \mathbb{M} \mid \mathit{apv} = 1 \wedge \mathit{i1} \in \{\text{-}1, 0, 1, 2\}\}$
ℓ_4	$\{\rho \in \mathbb{M} \mid \mathit{apv} = 1 \wedge \mathit{i1} \in \{1, 2\}\} \cup \{\rho \in \mathbb{M} \mid \mathit{apv} = \text{-}1 \wedge \mathit{i1} \in \{\text{-}1, 0\}\}$
ℓ_5	$\{\rho \in \mathbb{M} \mid \mathit{apv} = 1 \wedge \mathit{i1} \in \{1, 2\} \wedge \mathit{i2} \in \{\text{-}1, 0, 1, 2\}\}$ $\cup \{\rho \in \mathbb{M} \mid \mathit{apv} = \text{-}1 \wedge \mathit{i1} \in \{\text{-}1, 0\} \wedge \mathit{i2} \in \{\text{-}1, 0, 1, 2\}\}$
ℓ_6	$\{\rho \in \mathbb{M} \mid \mathit{apv} = 1 \wedge \mathit{i1} \in \{1, 2\} \wedge \mathit{i2} \in \{1, 2\}\}$ $\cup \{\rho \in \mathbb{M} \mid \mathit{apv} = \text{-}1 \wedge \mathit{i1} \in \{1, 2\} \wedge \mathit{i2} \in \{\text{-}1, 0\}\}$ $\cup \{\rho \in \mathbb{M} \mid \mathit{apv} = \text{-}1 \wedge \mathit{i1} \in \{\text{-}1, 0\} \wedge \mathit{i2} \in \{\text{-}1, 0, 1, 2\}\}$
ℓ_7	$\{\rho \in \mathbb{M} \mid \mathit{apv} = 1 \wedge \mathit{i1} \in \{1, 2\} \wedge \mathit{i2} \in \{1, 2\} \wedge \mathit{typ} \in \{1, 2\}\}$ $\cup \{\rho \in \mathbb{M} \mid \mathit{apv} = \text{-}1 \wedge \mathit{i1} \in \{1, 2\} \wedge \mathit{i2} \in \{\text{-}1, 0\} \wedge \mathit{typ} \in \{1, 2\}\}$ $\cup \{\rho \in \mathbb{M} \mid \mathit{apv} = \text{-}1 \wedge \mathit{i1} \in \{\text{-}1, 0\} \wedge \mathit{i2} \in \{\text{-}1, 0, 1, 2\} \wedge \mathit{typ} \in \{1, 2\}\}$
ℓ_8	$\{\rho \in \mathbb{M} \mid \mathit{apv} = 1 \wedge \mathit{i1} \in \{1, 2\} \wedge \mathit{i2} \in \{1, 2\} \wedge \mathit{typ} = 1 \wedge \mathit{acs} = 1\}$ $\cup \{\rho \in \mathbb{M} \mid \mathit{apv} = 1 \wedge \mathit{i1} \in \{1, 2\} \wedge \mathit{i2} \in \{1, 2\} \wedge \mathit{typ} = 2 \wedge \mathit{acs} = 2\}$ $\cup \{\rho \in \mathbb{M} \mid \mathit{apv} = \text{-}1 \wedge \mathit{i1} \in \{1, 2\} \wedge \mathit{i2} \in \{\text{-}1, 0\} \wedge \mathit{typ} = 1 \wedge \mathit{acs} = \text{-}1\}$ $\cup \{\rho \in \mathbb{M} \mid \mathit{apv} = \text{-}1 \wedge \mathit{i1} \in \{1, 2\} \wedge \mathit{i2} \in \{\text{-}1, 0\} \wedge \mathit{typ} = 2 \wedge \mathit{acs} = \text{-}2\}$ $\cup \{\rho \in \mathbb{M} \mid \mathit{apv} = \text{-}1 \wedge \mathit{i1} \in \{\text{-}1, 0\} \wedge \mathit{i2} \in \{\text{-}1, 0, 1, 2\} \wedge \mathit{typ} = 1 \wedge \mathit{acs} = \text{-}1\}$ $\cup \{\rho \in \mathbb{M} \mid \mathit{apv} = \text{-}1 \wedge \mathit{i1} \in \{\text{-}1, 0\} \wedge \mathit{i2} \in \{\text{-}1, 0, 1, 2\} \wedge \mathit{typ} = 2 \wedge \mathit{acs} = \text{-}2\}$

Table 2.1: Concrete Forward Reachability Semantics for the Access Control Program

2.3.2 Over-approximating Abstract Forward Reachability Analysis

Although the concrete forward reachability semantics $\mathcal{S}_{\overrightarrow{ps}}[\![\mathrm{P}]\!]$ can be easily computed in the Example 5 (since there is no infinite loops in the access control program and the variable values are bounded integers), it is not computable in general, and an over-approximation is necessary.

Over-approximating Abstract Forward Transfer Function. For the forward transfer function $\mathrm{F}_{\overrightarrow{ps}}[\![\mathrm{P}]\!] \in (\mathbb{L} \mapsto \wp(\mathbb{M})) \mapsto (\mathbb{L} \mapsto \wp(\mathbb{M}))$ on the concrete invariant domain, we need to construct an abstract forward transfer function $\hat{\mathrm{F}}^{\sharp}_{\overrightarrow{ps}}[\![\mathrm{P}]\!] \in (\mathbb{L} \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}}) \mapsto (\mathbb{L} \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}})$ that over-approximates $\mathrm{F}_{\overrightarrow{ps}}[\![\mathrm{P}]\!]$, where the symbol $\hat{}$ denotes over-approximations.

In section 2.2.1, it is assumed that for each transfer function $\mathrm{F}_{\ell\to\ell'}[\![\mathrm{P}]\!] \in \wp(\mathbb{M}) \mapsto \wp(\mathbb{M})$ defined for atomic actions, the abstract environment domain $\mathcal{D}^\sharp_\mathbb{M}$ provides an abstract function $\hat{\mathrm{F}}^\sharp_{\ell\to\ell'}[\![\mathrm{P}]\!] \in \mathcal{D}^\sharp_\mathbb{M} \mapsto \mathcal{D}^\sharp_\mathbb{M}$ such that $\forall \mathrm{M}^\sharp \in \mathcal{D}^\sharp_\mathbb{M}.\ (\mathrm{F}_{\ell\to\ell'}[\![\mathrm{P}]\!] \circ \gamma_\mathbb{M})(\mathrm{M}^\sharp) \subseteq (\gamma_\mathbb{M} \circ \hat{\mathrm{F}}^\sharp_{\ell\to\ell'}[\![\mathrm{P}]\!])(\mathrm{M}^\sharp)$. For instance, the interval/polyhedron/octagon domain provides the over-approximating abstract transfer versions $\tau^\sharp\{\!|\, x := e \,|\!\}$ and $\tau^\sharp\{\!|\, b \,|\!\}$ for $\tau\{\!|\, x := e \,|\!\}$ and $\tau\{\!|\, b \,|\!\}$. Therefore, $\hat{\mathrm{F}}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!]$ can be constructed by the join of $\hat{\mathrm{F}}^\sharp_{\ell\to\ell'}[\![\mathrm{P}]\!]$ functions:

$$\begin{array}{lcll} \hat{\mathrm{F}}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!] & \in & (\mathbb{L} \mapsto \mathcal{D}^\sharp_\mathbb{M}) \mapsto (\mathbb{L} \mapsto \mathcal{D}^\sharp_\mathbb{M}) & \text{abstract forward transfer function} \\ \hat{\mathrm{F}}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!]\mathrm{I}^\sharp & \triangleq & \lambda\ell' \in \mathbb{L}.\ \sqcup^\sharp_{\mathbb{M}\ \ell\in\mathbb{L}}\ \hat{\mathrm{F}}^\sharp_{\ell\to\ell'}[\![\mathrm{P}]\!](\mathrm{I}^\sharp(\ell)) & \end{array}$$

The abstract function $\hat{\mathrm{F}}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!]$ is monotonic and obeys the soundness condition:

$$\forall \mathrm{I}^\sharp \in \mathbb{L} \mapsto \mathcal{D}^\sharp_\mathbb{M}.\ \mathrm{F}_{\overrightarrow{ps}}[\![\mathrm{P}]\!] \circ \dot{\gamma}_\mathbb{M}(\mathrm{I}^\sharp) \mathrel{\dot{\subseteq}} \dot{\gamma}_\mathbb{M} \circ \hat{\mathrm{F}}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathrm{I}^\sharp). \tag{2.1}$$

Proof. We start with the soundness of abstract atomic transfer function $\hat{\mathrm{F}}^\sharp_{\ell\to\ell'}[\![\mathrm{P}]\!]$:

$$\begin{array}{l} \forall \ell, \ell' \in \mathbb{L}.\ \forall \mathrm{M}^\sharp \in \mathcal{D}^\sharp_\mathbb{M}.\ \mathrm{F}_{\ell\to\ell'}[\![\mathrm{P}]\!] \circ \gamma_\mathbb{M}(\mathrm{M}^\sharp) \subseteq \gamma_\mathbb{M} \circ \hat{\mathrm{F}}^\sharp_{\ell\to\ell'}[\![\mathrm{P}]\!](\mathrm{M}^\sharp) \\ \Rightarrow \forall \ell, \ell' \in \mathbb{L}.\ \forall \mathrm{I}^\sharp \in \mathbb{L} \mapsto \mathcal{D}^\sharp_\mathbb{M}.\ \mathrm{F}_{\ell\to\ell'}[\![\mathrm{P}]\!] \circ \gamma_\mathbb{M}(\mathrm{I}^\sharp(\ell)) \subseteq \gamma_\mathbb{M} \circ \hat{\mathrm{F}}^\sharp_{\ell\to\ell'}[\![\mathrm{P}]\!](\mathrm{I}^\sharp(\ell)) \\ \qquad\qquad \text{(by replacing } \mathrm{M}^\sharp \text{ with } \mathrm{I}^\sharp(\ell)\text{)} \\ \Rightarrow \forall \ell' \in \mathbb{L}.\ \forall \mathrm{I}^\sharp \in \mathbb{L} \mapsto \mathcal{D}^\sharp_\mathbb{M}.\ \cup_{\ell\in\mathbb{L}}\ \mathrm{F}_{\ell\to\ell'}[\![\mathrm{P}]\!](\gamma_\mathbb{M}(\mathrm{I}^\sharp(\ell))) \subseteq \gamma_\mathbb{M}(\sqcup^\sharp_{\mathbb{M}\ell\in\mathbb{L}}\ \hat{\mathrm{F}}^\sharp_{\ell\to\ell'}[\![\mathrm{P}]\!](\mathrm{I}^\sharp(\ell))) \\ \qquad\qquad \text{(join on } \ell \in \mathbb{L}\text{, and } \sqcup^\sharp_\mathbb{M} \text{ soundly approximates } \cup\text{)} \\ \Rightarrow \forall \ell' \in \mathbb{L}.\ \forall \mathrm{I}^\sharp \in \mathbb{L} \mapsto \mathcal{D}^\sharp_\mathbb{M}.\ (\mathrm{F}_{\overrightarrow{ps}}[\![\mathrm{P}]\!] \circ \dot{\gamma}_\mathbb{M}(\mathrm{I}^\sharp))(\ell') \ \subseteq\ (\dot{\gamma}_\mathbb{M} \circ \hat{\mathrm{F}}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathrm{I}^\sharp))(\ell') \\ \qquad\qquad \text{(def. } \mathrm{F}_{\overrightarrow{ps}}[\![\mathrm{P}]\!] \text{ and } \hat{\mathrm{F}}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!]\text{)} \\ \Rightarrow \forall \mathrm{I}^\sharp \in \mathbb{L} \mapsto \mathcal{D}^\sharp_\mathbb{M}.\ \mathrm{F}_{\overrightarrow{ps}}[\![\mathrm{P}]\!] \circ \dot{\gamma}_\mathbb{M}(\mathrm{I}^\sharp) \mathrel{\dot{\subseteq}} \dot{\gamma}_\mathbb{M} \circ \hat{\mathrm{F}}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathrm{I}^\sharp) \qquad \text{(def. } \dot{\subseteq}\text{)} \end{array}$$ □

By the monotonic property and the soundness condition (2.1) of the abstract forward transfer function $\hat{\mathrm{F}}^{\sharp}_{\overrightarrow{ps}}[\![\mathrm{P}]\!]$, we know that: for any $\mathsf{I}_{\mathsf{pre}} \in \mathbb{L} \mapsto \wp(\mathbb{M})$ and $\mathsf{I}^{\sharp}_{\mathsf{pre}} \in \mathbb{L} \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}}$, if $\mathsf{I}_{\mathsf{pre}} \dot{\subseteq} \dot{\gamma}_{\mathbb{M}}(\mathsf{I}^{\sharp}_{\mathsf{pre}})$, then $\mathrm{lfp}^{\dot{\subseteq}}_{\mathsf{I}_{\mathsf{pre}}} \mathrm{F}_{\overrightarrow{ps}}[\![\mathrm{P}]\!] \dot{\subseteq} \dot{\gamma}_{\mathbb{M}}(\mathrm{lfp}^{\dot{\sqsubseteq}^{\sharp}_{\mathbb{M}}}_{\mathsf{I}^{\sharp}_{\mathsf{pre}}} \hat{\mathrm{F}}^{\sharp}_{\overrightarrow{ps}}[\![\mathrm{P}]\!])$. That is to say, the concrete forward reachability semantics $\mathcal{S}_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{pre}})$ can be soundly over-approximated by the least fixpoint of the abstract forward transfer function $\hat{\mathrm{F}}^{\sharp}_{\overrightarrow{ps}}[\![\mathrm{P}]\!]$.

Widening. In most abstract environment domains (e.g. intervals, polyhedra, octagons), there may exist infinite increasing chains, hence the iteration of $\hat{\mathrm{F}}^{\sharp}_{\overrightarrow{ps}}[\![\mathrm{P}]\!]$ may not converge in finite time. To address this problem, as explained in section 2.1, we need to have a widening operator $\triangledown_{\mathbb{I}} \in (\mathbb{L} \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}}) \times (\mathbb{L} \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}}) \mapsto (\mathbb{L} \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}})$ on the abstract invariant domain, which satisfies the following soundness and termination conditions:

(1) $\forall x^{\sharp}, y^{\sharp} \in \mathbb{L} \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}}.\ \dot{\gamma}_{\mathbb{M}}(x^{\sharp}) \dot{\cup} \dot{\gamma}_{\mathbb{M}}(y^{\sharp}) \dot{\subseteq} \dot{\gamma}_{\mathbb{M}}(x^{\sharp} \triangledown_{\mathbb{I}} y^{\sharp})$;

(2) for any sequence $(x^{\sharp}_i)_{i\in\mathbb{N}}$, the sequence $(y^{\sharp}_i)_{i\in\mathbb{N}}$ defined as $y^{\sharp}_0 = x^{\sharp}_0$ and $\forall i \in \mathbb{N}.\ y^{\sharp}_{i+1} = y^{\sharp}_i \triangledown_{\mathbb{I}} x^{\sharp}_{i+1}$ converges in finite time.

The implementation of $\triangledown_{\mathbb{I}} \in (\mathbb{L} \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}}) \times (\mathbb{L} \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}}) \mapsto (\mathbb{L} \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}})$ naturally follows the widening operator $\triangledown_{\mathbb{M}} \in \mathcal{D}^{\sharp}_{\mathbb{M}} \times \mathcal{D}^{\sharp}_{\mathbb{M}} \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}}$ provided by the abstract environment domain, such that $\mathsf{I}^{\sharp} \triangledown_{\mathbb{I}} \mathsf{I}^{\sharp\prime} \triangleq \lambda \ell \in \mathbb{L}.\ \mathsf{I}^{\sharp}(\ell) \triangledown_{\mathbb{M}} \mathsf{I}^{\sharp\prime}(\ell)$. It is easy to prove such a definition of $\triangledown_{\mathbb{I}}$ obeys the soundness and termination conditions, and we omit it here.

Abstract Forward Reachability Semantics. Given a precondition represented by $\mathsf{I}^{\sharp}_{\mathsf{pre}} \in \mathbb{L} \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}}$, the corresponding concrete reachability semantics $\mathcal{S}_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\dot{\gamma}_{\mathbb{M}}(\mathsf{I}^{\sharp}_{\mathsf{pre}}))$ is the least fixpoint of function $\mathrm{F}_{\overrightarrow{ps}}[\![\mathrm{P}]\!]$ which is greater than or equal to $\dot{\gamma}_{\mathbb{M}}(\mathsf{I}^{\sharp}_{\mathsf{pre}})$. That is to say, $\mathcal{S}_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\dot{\gamma}_{\mathbb{M}}(\mathsf{I}^{\sharp}_{\mathsf{pre}})) = \mathrm{lfp}^{\dot{\subseteq}}_{\dot{\gamma}_{\mathbb{M}}(\mathsf{I}^{\sharp}_{\mathsf{pre}})} \mathrm{F}_{\overrightarrow{ps}}[\![\mathrm{P}]\!]$. By Cousot and Cousot's upward iteration with

widening theorem, $\mathrm{lfp}^{\dot{\subseteq}}_{\dot{\gamma}_{\mathbb{M}}(\mathsf{I}^\sharp_{\mathsf{pre}})} \mathrm{F}_{\overrightarrow{ps}}[\![\mathrm{P}]\!]$ can be soundly over-approximated by the limit of a ultimately stationary sequence $(\mathsf{I}^\sharp_i)_{i\in\mathbb{N}}$, where $\mathsf{I}^\sharp_0 = \mathsf{I}^\sharp_{\mathsf{pre}}$ and $\forall i \in \mathbb{N}.\ \mathsf{I}^\sharp_{i+1} = \mathsf{I}^\sharp_i \ \nabla_{\mathbb{I}}\ \hat{\mathrm{F}}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_i)$.

$$\forall \mathsf{I}^\sharp_{\mathsf{pre}} \in \mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}.\ \mathrm{lfp}^{\dot{\subseteq}}_{\dot{\gamma}_{\mathbb{M}}(\mathsf{I}^\sharp_{\mathsf{pre}})} \mathrm{F}_{\overrightarrow{ps}}[\![\mathrm{P}]\!] \ \dot{\subseteq}\ \dot{\gamma}_{\mathbb{M}}(\mathrm{lim}_{\mathsf{I}^\sharp_{\mathsf{pre}}}\ \lambda \mathsf{I}^\sharp.\ \mathsf{I}^\sharp \ \nabla_{\mathbb{I}}\ \hat{\mathrm{F}}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp)). \tag{2.2}$$

In the rest of this dissertation, the abstract forward reachability semantics $\mathcal{S}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!]$ refers to the following definition, which gives a sound over-approximation of the concrete reachability semantics and can be computed in finite time.

$$\begin{array}{rcll} \mathcal{S}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!] & \in & (\mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}) \mapsto (\mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}) & \text{abstract forward reachability semantics} \\ \mathcal{S}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{pre}}) & \triangleq & \mathrm{lim}_{\mathsf{I}^\sharp_{\mathsf{pre}}}\ \lambda \mathsf{I}^\sharp.\ \mathsf{I}^\sharp \ \nabla_{\mathbb{I}}\ \hat{\mathrm{F}}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp) & \end{array}$$

Example 6 (Access Control, Continued) *For the access control program in Fig.1.4, we use the interval domain as the abstract environment domain $\mathcal{D}^\sharp_{\mathbb{M}}$. Given an abstract precondition $\mathsf{I}^\sharp_{\mathsf{pre}} \in \mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}$ such that $\mathsf{I}^\sharp_{\mathsf{pre}}(\ell_1) = \top^\sharp_{\mathbb{M}}$ and $\mathsf{I}^\sharp_{\mathsf{pre}}(\ell) = \bot^\sharp_{\mathbb{M}}$ for $\ell \neq \ell_1$, the corresponding abstract forward reachability semantics $\mathcal{S}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{pre}})\ell$ is listed in Table 2.2.*

ℓ	$\mathcal{S}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{pre}})\ell$
ℓ_1	$\top^\sharp_{\mathbb{M}}$
ℓ_2	$apv \in [1;1] \wedge i1 \in [-\infty;\infty] \wedge i2 \in [-\infty;\infty] \wedge typ \in [-\infty;\infty] \wedge acs \in [-\infty;\infty]$
ℓ_3	$apv \in [1;1] \wedge i1 \in [-1;2] \wedge i2 \in [-\infty;\infty] \wedge typ \in [-\infty;\infty] \wedge acs \in [-\infty;\infty]$
ℓ_4	$apv \in [-1;1] \wedge i1 \in [-1;2] \wedge i2 \in [-\infty;\infty] \wedge typ \in [-\infty;\infty] \wedge acs \in [-\infty;\infty]$
ℓ_5	$apv \in [-1;1] \wedge i1 \in [-1;2] \wedge i2 \in [-1;2] \wedge typ \in [-\infty;\infty] \wedge acs \in [-\infty;\infty]$
ℓ_6	$apv \in [-1;1] \wedge i1 \in [-1;2] \wedge i2 \in [-1;2] \wedge typ \in [-\infty;\infty] \wedge acs \in [-\infty;\infty]$
ℓ_7	$apv \in [-1;1] \wedge i1 \in [-1;2] \wedge i2 \in [-1;2] \wedge typ \in [1;2] \wedge acs \in [-\infty;\infty]$
ℓ_8	$apv \in [-1;1] \wedge i1 \in [-1;2] \wedge i2 \in [-1;2] \wedge typ \in [1;2] \wedge acs \in [-2;2]$

Table 2.2: Abstract Forward Reachability Semantics for the Access Control Program

Compared with the concrete reachability semantics $\mathcal{S}_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{pre}})\ell$ in Table 2.1, it is obvious that $\mathcal{S}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{pre}})\ell$ is an over-approximation and contains some spurious environments that are not reachable in the concrete (e.g. the value of acs cannot be 0 at ℓ_8 in the concrete). □

2.4 Backward Accessibilty Analysis

Given a precondition on states, the forward reachability analysis collects states that are possibly reachable by the executions from states satisfying the precondition. Inversely, given a postcondition on states, the backward accessibility analysis collects states from which the executions reach states satisfying the postcondition.

In general, there are two types of backward accessibility analysis: (1) the *backward impossible failure accessibility analysis* computes the states, from which the executions can reach only the states satisfying the given postcondition (i.e. it is impossible to reach states that fail the postcondition); (2) the *backward possible success accessibility analysis* computes the states, from which the executions may reach a state satisfying the given postcondition (i.e. it is possible to succeed to reach a state satisfying the postcondition). This section discusses the backward impossible failure accessibility semantics, which is essentially equivalent to the *sufficient condition semantics* in [34, 42]. More precisely, we briefly review the under-approximating abstract analysis introduced by Miné, and propose a new over-approximating abstract backward impossible failure accessibility analysis. Meanwhile, the backward possible success accessibility semantics is not utilized in this dissertation, hence we briefly introduce it in the next section for the sake of completeness, as well as its adjoint (the forward impossible failure reachability semantics).

2.4.1 Backward Impossible Failure Accessibility Semantics

The forward (possible success) reachability semantics $\mathcal{S}_{\overrightarrow{ps}}[\![\mathrm{P}]\!] \in (\mathbb{L} \mapsto \wp(\mathbb{M})) \mapsto (\mathbb{L} \mapsto \wp(\mathbb{M}))$ is the lower adjoint in a Galois connection, and the corresponding upper adjoint is defined as the backward impossible failure accessibility semantics $\mathcal{S}_{\overleftarrow{if}}[\![\mathrm{P}]\!] \in (\mathbb{L} \mapsto$

$\wp(\mathbb{M})) \mapsto (\mathbb{L} \mapsto \wp(\mathbb{M}))$, such that any execution from states satisfying $\mathcal{S}^{\leftarrow}_{if}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{post}})$ can reach only the states satisfying the given postcondition $\mathsf{I}_{\mathsf{post}} \in \mathbb{L} \mapsto \wp(\mathbb{M})$:

$$\langle \mathbb{L} \mapsto \wp(\mathbb{M}),\ \dot{\subseteq} \rangle \underset{\mathcal{S}^{\rightarrow}_{ps}[\![\mathrm{P}]\!]}{\overset{\mathcal{S}^{\leftarrow}_{if}[\![\mathrm{P}]\!]}{\leftrightarrows}} \langle \mathbb{L} \mapsto \wp(\mathbb{M}),\ \dot{\subseteq} \rangle$$

where the definition of $\mathcal{S}^{\leftarrow}_{if}[\![\mathrm{P}]\!]$ is formalized as

$$\begin{array}{rcl} \mathcal{S}^{\leftarrow}_{if}[\![\mathrm{P}]\!] & \in & (\mathbb{L} \mapsto \wp(\mathbb{M})) \mapsto (\mathbb{L} \mapsto \wp(\mathbb{M})) \\ \mathcal{S}^{\leftarrow}_{if}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{post}})\iota & \triangleq & \{\rho \in \mathbb{M} \mid \forall \sigma \in \mathbb{S}^*, \iota' \in \mathbb{L}, \rho' \in \mathbb{M}.\ (\langle \iota,\ \rho \rangle \sigma \langle \iota',\ \rho' \rangle \in [\![\mathrm{P}]\!]^{\mathsf{lt}} \Rightarrow \\ & & \qquad \rho' \in \mathsf{I}_{\mathsf{post}}(\iota'))\} \end{array}$$

Proof. For any $\mathsf{I}_{\mathsf{pre}}, \mathsf{I}_{\mathsf{post}} \in \mathbb{L} \mapsto \wp(\mathbb{M})$, we can prove that:

$$\begin{array}{ll} & \mathcal{S}^{\rightarrow}_{ps}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{pre}}) \mathrel{\dot{\subseteq}} \mathsf{I}_{\mathsf{post}} \\ \Leftrightarrow & \forall \iota' \in \mathbb{L}.\ \mathcal{S}^{\rightarrow}_{ps}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{pre}})\iota' \ \subseteq\ \mathsf{I}_{\mathsf{post}}(\iota') & \text{〈def. } \dot{\subseteq}\text{〉} \\ \Leftrightarrow & \forall \iota' \in \mathbb{L}.\ \{\rho' \in \mathbb{M} \mid \exists \sigma \in \mathbb{S}^*, \iota \in \mathbb{L}, \rho \in \mathsf{I}_{\mathsf{pre}}(\iota).\ \langle \iota,\ \rho \rangle \sigma \langle \iota',\ \rho' \rangle \in [\![\mathrm{P}]\!]^{\mathsf{lt}}\} \ \subseteq\ \mathsf{I}_{\mathsf{post}}(\iota') \\ & & \text{〈def. } \mathcal{S}^{\rightarrow}_{ps}[\![\mathrm{P}]\!]\text{〉} \\ \Leftrightarrow & \forall \iota' \in \mathbb{L}.\ \{\rho' \in \mathbb{M} \mid \neg(\forall \sigma \in \mathbb{S}^*, \iota \in \mathbb{L}, \rho \in \mathsf{I}_{\mathsf{pre}}(\iota).\ \langle \iota,\ \rho \rangle \sigma \langle \iota',\ \rho' \rangle \notin [\![\mathrm{P}]\!]^{\mathsf{lt}})\} \ \subseteq \\ & \{\rho' \in \mathbb{M} \mid \rho' \in \mathsf{I}_{\mathsf{post}}(\iota')\} & \text{〈def. } \exists \text{ and } \forall\text{〉} \\ \Leftrightarrow & \forall \iota' \in \mathbb{L}.\ \{\rho' \in \mathbb{M} \mid \forall \sigma \in \mathbb{S}^*, \iota \in \mathbb{L}, \rho \in \mathsf{I}_{\mathsf{pre}}(\iota).\ \langle \iota,\ \rho \rangle \sigma \langle \iota',\ \rho' \rangle \notin [\![\mathrm{P}]\!]^{\mathsf{lt}}\} \ \cup\ \{\rho' \in \\ & \mathbb{M} \mid \rho' \in \mathsf{I}_{\mathsf{post}}(\iota')\} = \mathbb{M} & \text{〈def. } \neg \text{ and } \cup\text{〉} \\ \Leftrightarrow & \forall \iota' \in \mathbb{L}.\ \forall \rho' \in \mathbb{M}.\ (\forall \sigma \in \mathbb{S}^*, \iota \in \mathbb{L}, \rho \in \mathsf{I}_{\mathsf{pre}}(\iota).\ \langle \iota,\ \rho \rangle \sigma \langle \iota',\ \rho' \rangle \notin [\![\mathrm{P}]\!]^{\mathsf{lt}}) \ \vee \rho' \in \\ & \mathsf{I}_{\mathsf{post}}(\iota') & \text{〈def. } \vee\text{〉} \\ \Leftrightarrow & \forall \iota \in \mathbb{L}.\ \forall \rho \in \mathsf{I}_{\mathsf{pre}}(\iota).\ \forall \sigma \in \mathbb{S}^*, \iota' \in \mathbb{L}, \rho' \in \mathbb{M}.\ \langle \iota,\ \rho \rangle \sigma \langle \iota',\ \rho' \rangle \in [\![\mathrm{P}]\!]^{\mathsf{lt}} \ \Rightarrow \rho' \in \\ & \mathsf{I}_{\mathsf{post}}(\iota') & \text{〈def. } \Rightarrow\text{〉} \\ \Leftrightarrow & \forall \iota \in \mathbb{L}.\ \mathsf{I}_{\mathsf{pre}}(\iota) \ \subseteq\ \{\rho \in \mathbb{M} \mid \forall \sigma \in \mathbb{S}^*, \iota' \in \mathbb{L}, \rho' \in \mathbb{M}.\ \langle \iota,\ \rho \rangle \sigma \langle \iota',\ \rho' \rangle \in [\![\mathrm{P}]\!]^{\mathsf{lt}} \ \Rightarrow \\ & \rho' \in \mathsf{I}_{\mathsf{post}}(\iota')\} & \text{〈def. } \subseteq\text{〉} \end{array}$$

$$\Leftrightarrow \forall \ell \in \mathbb{L}.\ \mathsf{I}_{\mathsf{pre}}(\ell) \ \subseteq\ \mathcal{S}^{\leftarrow}_{if}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{post}})\ell \qquad \wr \text{def. } \mathcal{S}^{\leftarrow}_{if}[\![\mathrm{P}]\!] \int$$

$$\Leftrightarrow \mathsf{I}_{\mathsf{pre}} \ \dot{\subseteq}\ \mathcal{S}^{\leftarrow}_{if}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{post}}) \qquad \wr \text{def. } \dot{\subseteq} \int$$

Thus, the forward (possible success) reachability semantics $\mathcal{S}^{\rightarrow}_{ps}[\![\mathrm{P}]\!]$ and the backward impossible failure accessibility semantics $\mathcal{S}^{\leftarrow}_{if}[\![\mathrm{P}]\!]$ form a Galois connection. □

For any postcondition $\mathsf{I}_{\mathsf{post}} \in \mathbb{L} \mapsto \wp(\mathbb{M})$ that can represent a trace property of interest $\gamma_{\mathbb{I}}(\mathsf{I}_{\mathsf{post}})$, the backward impossible failure accessibility semantics $\mathcal{S}^{\leftarrow}_{if}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{post}})$ computes the states from which all the execution traces must have the property $\gamma_{\mathbb{I}}(\mathsf{I}_{\mathsf{post}})$, or say, it infers the sufficient preconditions for the postcondition $\mathsf{I}_{\mathsf{post}}$ to hold. It is of great importance to know that our $\mathcal{S}^{\leftarrow}_{if}[\![\mathrm{P}]\!]$ is essentially equivalent to the sufficient condition semantics introduced in [34, 42].

Backward Impossible Failure Accessibility Semantics in Fixpoint Form. Similar to the forward (possible success) reachability semantics $\mathcal{S}^{\rightarrow}_{ps}[\![\mathrm{P}]\!]$, the backward impossible failure accessibility semantics $\mathcal{S}^{\leftarrow}_{if}[\![\mathrm{P}]\!]$ of a program $\mathrm{P} = \langle \mathbb{S}^i,\ \rightarrow \rangle$ can be also defined in the fixpoint form with a concrete backward transfer function $\mathrm{F}^{\leftarrow}_{if}[\![\mathrm{P}]\!]$:

$$\begin{array}{rcl}
\mathcal{S}^{\leftarrow}_{if}[\![\mathrm{P}]\!] & \in & (\mathbb{L} \mapsto \wp(\mathbb{M})) \mapsto (\mathbb{L} \mapsto \wp(\mathbb{M})) \quad \text{backward IF accessibility semantics} \\
\mathcal{S}^{\leftarrow}_{if}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{post}}) & \triangleq & \mathrm{gfp}^{\dot{\subseteq}}_{\mathsf{I}_{\mathsf{post}}}\ \mathrm{F}^{\leftarrow}_{if}[\![\mathrm{P}]\!] \\
\mathrm{F}^{\leftarrow}_{if}[\![\mathrm{P}]\!] & \in & (\mathbb{L} \mapsto \wp(\mathbb{M})) \mapsto (\mathbb{L} \mapsto \wp(\mathbb{M})) \qquad \text{backward IF transfer function} \\
\mathrm{F}^{\leftarrow}_{if}[\![\mathrm{P}]\!]\mathsf{I} & \triangleq & \mathsf{I} \mathbin{\dot{\cap}} \lambda \ell \in \mathbb{L}.\{\rho \in \mathbb{M} \mid \forall \ell' \in \mathbb{L}, \rho' \in \mathbb{M}.\ \langle \ell,\ \rho \rangle \rightarrow \langle \ell',\ \rho' \rangle \\
& & \qquad\qquad \Rightarrow \rho' \in \mathsf{I}(\ell')\}
\end{array}$$

where $\dot{\subseteq}$ and $\dot{\cap}$ are pointwise extensions of the standard set inclusion relation $\subseteq$ and intersection operator $\cap$, respectively.

As $\mathrm{F}^{\rightarrow}_{ps}[\![\mathrm{P}]\!]$ is constructed by combining atomic forward transfer functions $\mathrm{F}_{\ell \rightarrow \ell'}[\![\mathrm{P}]\!]$, we can construct $\mathrm{F}^{\leftarrow}_{if}[\![\mathrm{P}]\!]$ by atomic backward transfer functions $\mathrm{F}_{\ell \leftarrow \ell'}[\![\mathrm{P}]\!] \in \wp(\mathbb{M}) \mapsto$

$\wp(\mathbb{M})$, which are defined for every pair of program points $\langle \ell, \ell' \rangle$ in the program such that, if there exists a single atomic action from ℓ to ℓ', then executions from environments in $\mathrm{F}_{\ell \leftarrow \ell'}[\![\mathrm{P}]\!]\mathrm{M}$ at point ℓ can only reach environments in M at point ℓ'. To be more precise: (1) if $\ell = \ell'$, then $\mathrm{F}_{\ell \leftarrow \ell'}[\![\mathrm{P}]\!](\mathrm{M}) = \mathrm{M}$; (2) if $\ell \neq \ell'$ and there is not an atomic action from ℓ to ℓ', then $\mathrm{F}_{\ell \leftarrow \ell'}[\![\mathrm{P}]\!](\mathrm{M}) = \mathbb{M}$; and (3) otherwise, there is an atomic action from ℓ to ℓ', then $\mathrm{F}_{\ell \leftarrow \ell'}[\![\mathrm{P}]\!](\mathrm{M})$ is the set of environments at point ℓ that guarantee the environments after executing the atomic action belong to M.

Specifically, for the simple language described in Fig. 1.2, there are only two types of atomic actions, and for each of them we define an atomic backward transfer function. For an assignment ${}^{\ell_1}x := e^{\ell_2}$, the corresponding atomic backward transfer function $\mathrm{F}_{\ell_1 \leftarrow \ell_2}[\![\mathrm{P}]\!](\mathrm{M}) = \overleftarrow{\tau}\{\!|x := e|\!\}\mathrm{M}$, which is defined as:

$$\overleftarrow{\tau}\{\!|x := e|\!\}\mathrm{M} \triangleq \{\rho \in \mathbb{M} \mid \forall v \in [\![e]\!]\rho.\ \rho[x \mapsto v] \in \mathrm{M}\}.$$

Similarly, for a boolean test ${}^{\ell_1}b^{\ell_2}$, the corresponding atomic backward transfer function $\mathrm{F}_{\ell_1 \leftarrow \ell_2}[\![\mathrm{P}]\!](\mathrm{M}) = \overleftarrow{\tau}\{\!|b|\!\}\mathrm{M}$, which is defined as:

$$\overleftarrow{\tau}\{\!|b|\!\}\mathrm{M} \triangleq \mathrm{M} \cup \{\rho \in \mathbb{M} \mid [\![b]\!]\rho = \{\mathrm{f}\}\}.$$

Therefore, the definition of backward transfer function $\mathrm{F}^{\leftarrow}_{if}[\![\mathrm{P}]\!]$ can be rephrased into:

$$\begin{array}{lcll} \mathrm{F}^{\leftarrow}_{if}[\![\mathrm{P}]\!] & \in & (\mathbb{L} \mapsto \wp(\mathbb{M})) \mapsto (\mathbb{L} \mapsto \wp(\mathbb{M})) & \text{backward IF transfer function} \\ \mathrm{F}^{\leftarrow}_{if}[\![\mathrm{P}]\!]\mathsf{I} & \triangleq & \lambda \ell \in \mathbb{L}.\ \cap_{\ell' \in \mathbb{L}} \mathrm{F}_{\ell \leftarrow \ell'}[\![\mathrm{P}]\!](\mathsf{I}(\ell')) & \end{array}$$

Example 7 (Access Control, Continued) *For the access control program in Fig.1.4, the transfer function* $\mathrm{F}^{\leftarrow}_{if}[\![\mathrm{P}]\!]$ *can be constructed by combining the following atomic backward transfer functions:* $\overleftarrow{\tau}\{\!|\ apv := 1\ |\!\}$, $\overleftarrow{\tau}\{\!|\ i1 := [\text{-}1; 2]\ |\!\}$, $\overleftarrow{\tau}\{\!|\ apv := (i1 \leq 0)\,?\,\text{-}1 : apv\ |\!\}$, $\overleftarrow{\tau}\{\!|\ i2 := [\text{-}1; 2]\ |\!\}$, $\overleftarrow{\tau}\{\!|\ apv := (apv \geq 1 \wedge i2 \leq 0)\,?\,\text{-}1 : apv\ |\!\}$, $\overleftarrow{\tau}\{\!|\ typ := [1; 2]\ |\!\}$, *and* $\overleftarrow{\tau}\{\!|acs := apv \times typ|\!\}$.

Suppose we are interested in inferring sufficient preconditions of the trace property "the access to o fails", a simple idea is to specify a postcondition $\mathsf{I}_{\mathsf{post}} \in \mathbb{L} \mapsto \wp(\mathbb{M})$ *such that* $\mathsf{I}_{\mathsf{post}}(\ell_8) = \{\rho \in \mathbb{M} \mid \rho(acs) <= 0\}$ *and* $\mathsf{I}_{\mathsf{post}}(\ell) = \mathbb{M}$ *for* $\ell \neq \ell_8$*, and then compute the corresponding backward accessibility semantics* $\mathcal{S}^{\overleftarrow{}}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{post}})$*. However, such a result is too imprecise. Take the semantics at the point* ℓ_7 *as an example:* $\mathcal{S}^{\overleftarrow{}}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{post}})\ell_7 = \mathsf{I}_{\mathsf{post}}(\ell_7) \cap \mathrm{F}_{\ell_7 \leftarrow \ell_8}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{post}}(\ell_8)) = \mathbb{M} \cap \overleftarrow{\tau}\{\!|\, acs := apv \times typ \,|\!\}(\{\rho \in \mathbb{M} \mid \rho(acs) <= 0\}) = \{\rho \in \mathbb{M} \mid (\rho(apv) <= 0 \wedge \rho(typ) >= 0) \vee (\rho(apv) >= 0 \wedge \rho(typ) <= 0)\}$*. This semantics does provide correct sufficient preconditions of "the access to o fails", but it is not precise enough, since the value of typ is never zero or negative at point* ℓ_7 *in the real executions.*

In order to get a more precise result, the specified postcondition $\mathsf{I}_{\mathsf{post}}$ *can be refined by the intersection with the forward reachability semantics* $\mathcal{S}^{\overrightarrow{}}_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{pre}})$ *computed in Example 5, i.e. we define* $\mathsf{I}'_{\mathsf{post}} = \mathsf{I}_{\mathsf{post}} \dot{\cap} \mathcal{S}^{\overrightarrow{}}_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{pre}})$*, and the semantics* $\mathcal{S}^{\overleftarrow{}}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathsf{I}'_{\mathsf{post}})$ *would be more precise, whose result is listed in table 2.3, and the constraints on environment like "*$\rho(apv) = 1$*" is written as "*$apv = 1$*" for short. It is not hard to see that: at the point* ℓ_1 *or* ℓ_2*, there is no sufficient precondition that can guarantee the property "the access to o fails"; beginning from the point* ℓ_3*, the negative or zero value of i1 guarantees "access failure"; and beginning from the point* ℓ_5*, the negative or zero value of i2 guarantees "access failure".* □

2.4.2 Under-approximating Abstract Backward Impossible Failure Accessibility Analysis

Similar to the forward reachability semantics, the backward impossible failure accessibility semantics may be not computable in the concrete, hence it is necessary to reason

ℓ	$\mathcal{S}^{\leftarrow}_{\overline{if}}[\![\mathrm{P}]\!](\mathsf{I}'_{\mathsf{post}})\ell$
ℓ_1	$\emptyset$
ℓ_2	$\emptyset$
ℓ_3	$\{\rho \in \mathbb{M} \mid \mathit{apv} = 1 \wedge \mathit{i1} \in \{\text{-}1, 0\}\}$
ℓ_4	$\{\rho \in \mathbb{M} \mid \mathit{apv} = \text{-}1 \wedge \mathit{i1} \in \{\text{-}1, 0\}\}$
ℓ_5	$\{\rho \in \mathbb{M} \mid \mathit{apv} = 1 \wedge \mathit{i1} \in \{1, 2\} \wedge \mathit{i2} \in \{\text{-}1, 0\}\}$ $\cup \{\rho \in \mathbb{M} \mid \mathit{apv} = \text{-}1 \wedge \mathit{i1} \in \{\text{-}1, 0\} \wedge \mathit{i2} \in \{\text{-}1, 0, 1, 2\}\}$
ℓ_6	$\{\rho \in \mathbb{M} \mid \mathit{apv} = \text{-}1 \wedge \mathit{i1} \in \{1, 2\} \wedge \mathit{i2} \in \{\text{-}1, 0\}\}$ $\cup \{\rho \in \mathbb{M} \mid \mathit{apv} = \text{-}1 \wedge \mathit{i1} \in \{\text{-}1, 0\} \wedge \mathit{i2} \in \{\text{-}1, 0, 1, 2\}\}$
ℓ_7	$\{\rho \in \mathbb{M} \mid \mathit{apv} = \text{-}1 \wedge \mathit{i1} \in \{1, 2\} \wedge \mathit{i2} \in \{\text{-}1, 0\} \wedge \mathit{typ} \in \{1, 2\}\}$ $\cup \{\rho \in \mathbb{M} \mid \mathit{apv} = \text{-}1 \wedge \mathit{i1} \in \{\text{-}1, 0\} \wedge \mathit{i2} \in \{\text{-}1, 0, 1, 2\} \wedge \mathit{typ} \in \{1, 2\}\}$
ℓ_8	$\{\rho \in \mathbb{M} \mid \mathit{apv} = \text{-}1 \wedge \mathit{i1} \in \{1, 2\} \wedge \mathit{i2} \in \{\text{-}1, 0\} \wedge \mathit{typ} = 1 \wedge \mathit{acs} = \text{-}1\}$ $\cup \{\rho \in \mathbb{M} \mid \mathit{apv} = \text{-}1 \wedge \mathit{i1} \in \{1, 2\} \wedge \mathit{i2} \in \{\text{-}1, 0\} \wedge \mathit{typ} = 2 \wedge \mathit{acs} = \text{-}2\}$ $\cup \{\rho \in \mathbb{M} \mid \mathit{apv} = \text{-}1 \wedge \mathit{i1} \in \{\text{-}1, 0\} \wedge \mathit{i2} \in \{\text{-}1, 0, 1, 2\} \wedge \mathit{typ} = 1 \wedge \mathit{acs} = \text{-}1\}$ $\cup \{\rho \in \mathbb{M} \mid \mathit{apv} = \text{-}1 \wedge \mathit{i1} \in \{\text{-}1, 0\} \wedge \mathit{i2} \in \{\text{-}1, 0, 1, 2\} \wedge \mathit{typ} = 2 \wedge \mathit{acs} = \text{-}2\}$

Table 2.3: Concrete Backward Impossible Failure Accessibility Semantics for the Access Control Program

on the abstract domain instead. Although classic abstract domains come with abstract transfer functions (operators) for both forward and backward analyses, these functions are over-approximating and are suitable only for inferring invariants (i.e. reachability semantics) or necessary preconditions (i.e. backward possible success accessibility semantics in section 2.5), but not for inferring sufficient preconditions. The reason comes from that an over-approximation of the tightest program invariant (respectively, the strongest necessary precondition) is still an invariant (respectively, a necessary precondition), but an over-approximation of the weakest sufficient precondition is not a sufficient precondition anymore (which will be discussed later in section 2.4.3), thus under-approximations are needed instead to preserve the soundness for inferring sufficient preconditions. To solve this problem, Miné [34, 42] presents under-approximating abstract operators (including a dual widening) for the classic interval/octagon/polyhedron domain, which makes au-

tomatically inferring sufficient preconditions directly by under-approximating backward analysis possible. Other attempts to infer sufficient preconditions include [52, 22, 44], but none of them can directly work on the classic numeric abstract domains.

In this section, we briefly summarize the framework of an under-approximating abstract backward impossible failure accessibility analysis, and refer to [34, 42] and the Banal static analyzer [55] for the details of implementing the under-approximating abstract operators (including a dual widening).

Under-approximating Abstract Backward Transfer Function. For the transfer function $\mathrm{F}^{\leftarrow}_{if}[\![\mathrm{P}]\!] \in (\mathbb{L} \mapsto \wp(\mathbb{M})) \mapsto (\mathbb{L} \mapsto \wp(\mathbb{M}))$ on the concrete invariant domain, we need to construct the corresponding abstract backward transfer function $\check{\mathrm{F}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!] \in (\mathbb{L} \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}}) \mapsto (\mathbb{L} \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}})$ (the symbol $\check{}$ denotes under-approximations), which satisfies the following soundness condition:

$$\forall \mathsf{I}^{\sharp} \in \mathbb{L} \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}}.\ \dot{\gamma}_{\mathbb{M}} \circ \check{\mathrm{F}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathsf{I}^{\sharp}) \dot{\subseteq} \mathrm{F}^{\leftarrow}_{if}[\![\mathrm{P}]\!] \circ \dot{\gamma}_{\mathbb{M}}(\mathsf{I}^{\sharp}). \tag{2.3}$$

Since $\mathrm{F}^{\leftarrow}_{if}[\![\mathrm{P}]\!]\mathsf{I}$ is defined by combining atomic backward transfer function $\mathrm{F}_{\ell\leftarrow\ell'}[\![\mathrm{P}]\!]$ together (i.e.$\mathrm{F}^{\leftarrow}_{if}[\![\mathrm{P}]\!]\mathsf{I} \triangleq \lambda\ell \in \mathbb{L}.\cap_{\ell'\in\mathbb{L}} \mathrm{F}_{\ell\leftarrow\ell'}[\![\mathrm{P}]\!](\mathsf{I}(\ell'))$), it is necessary to build the under-approximating versions $\check{\mathrm{F}}^{\sharp}_{\ell\leftarrow\ell'}[\![\mathrm{P}]\!] \in \mathcal{D}^{\sharp}_{\mathbb{M}} \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}}$ for atomic backward transfer functions $\mathrm{F}_{\ell\leftarrow\ell'}[\![\mathrm{P}]\!] \in \wp(\mathbb{M}) \mapsto \wp(\mathbb{M})$, such that the condition (2.4) hold.

$$\forall \mathrm{M}^{\sharp} \in \mathcal{D}^{\sharp}_{\mathbb{M}}.\ \gamma_{\mathbb{M}} \circ \check{\mathrm{F}}^{\sharp}_{\ell\leftarrow\ell'}[\![\mathrm{P}]\!](\mathrm{M}^{\sharp}) \ \subseteq\ \mathrm{F}_{\ell\leftarrow\ell'}[\![\mathrm{P}]\!] \circ \gamma_{\mathbb{M}}(\mathrm{M}^{\sharp}). \tag{2.4}$$

In order to satisfy the soundness condition (2.4), we design $\check{\mathrm{F}}^{\sharp}_{\ell\leftarrow\ell'}[\![\mathrm{P}]\!]$ such that: (1) if $\ell = \ell'$, then $\check{\mathrm{F}}^{\sharp}_{\ell\leftarrow\ell'}[\![\mathrm{P}]\!](\mathrm{M}^{\sharp}) = \mathrm{M}^{\sharp}$; (2) if $\ell \neq \ell'$ and there is not an atomic action from ℓ to ℓ', then $\check{\mathrm{F}}^{\sharp}_{\ell\leftarrow\ell'}[\![\mathrm{P}]\!](\mathrm{M}^{\sharp}) = \top^{\sharp}_{\mathbb{M}}$; and (3) otherwise, there is an atomic action from ℓ to ℓ', then $\check{\mathrm{F}}^{\sharp}_{\ell\leftarrow\ell'}[\![\mathrm{P}]\!](\mathrm{M}^{\sharp})$ is an abstract environment element in $\mathcal{D}^{\sharp}_{\mathbb{M}}$ that guarantees

$\mathrm{M}^\sharp$ to hold after executing the atomic action. It is obvious that the case (3) is the difficult one, and fortunately for the atomic actions of assignments and boolean tests in the interval/polyhedron/octagon domain, Miné has proposed the corresponding under-approximating atomic backward transfer function $\overleftarrow{\tau}^\sharp\{\!|\, x := e \,|\!\}\mathrm{M}^\sharp$ and $\overleftarrow{\tau}^\sharp\{\!|\, b \,|\!\}\mathrm{M}^\sharp$, which satisfies the soundness condition. Details see the section 3.2-3.4 of [42]. Now we can build the backward transfer function $\check{\mathrm{F}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!]$ by the following definition:

$$\begin{array}{rcl} \check{\mathrm{F}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!] & \in & (\mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}) \mapsto (\mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}) \quad \text{under-approximating backward IF function} \\ \check{\mathrm{F}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!]\mathsf{I}^\sharp & \triangleq & \lambda \mathcal{l} \in \mathbb{L}.\, \sqcap^\sharp_{\mathbb{M}\ \mathcal{l}' \in \mathbb{L}} \check{\mathrm{F}}^\sharp_{\mathcal{l} \leftarrow \mathcal{l}'}[\![\mathrm{P}]\!](\mathsf{I}^\sharp(\mathcal{l}')) \end{array}$$

The backward transfer function $\check{\mathrm{F}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!]$ satisfies the soundness condition (2.3), and its greatest fixpoint would soundly under-approximate the concrete backward impossible failure accessibility semantics.

$$\forall \mathsf{I}^\sharp_{\mathsf{post}} \in \mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}.\ \dot{\gamma}_{\mathbb{M}}(\mathrm{gfp}^{\dot{\subseteq}}_{\mathsf{I}^\sharp_{\mathsf{post}}} \check{\mathrm{F}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!]) \dot{\subseteq} \mathrm{gfp}^{\dot{\subseteq}}_{\dot{\gamma}_{\mathbb{M}}(\mathsf{I}^\sharp_{\mathsf{post}})} \mathrm{F}_{\overleftarrow{if}}[\![\mathrm{P}]\!] = \mathcal{S}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\dot{\gamma}_{\mathbb{M}}(\mathsf{I}^\sharp_{\mathsf{post}})).$$

Dual Widening. The iteration of the above defined $\check{\mathrm{F}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!]$ may not converge in finite time, since there may exist infinite decreasing chains in the abstract environment domain (e.g. intervals, polyhedra, octagons). To address this problem, we need a dual widening operator $\underline{\triangledown}_{\mathbb{I}} \in (\mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}) \times (\mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}) \mapsto (\mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}})$ on the abstract invariant domain, which obeys the following soundness and termination conditions:

(1) $\forall x^\sharp, y^\sharp \in (\mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}).\ \dot{\gamma}_{\mathbb{M}}(x^\sharp \mathbin{\underline{\triangledown}_{\mathbb{I}}} y^\sharp) \dot{\subseteq} \dot{\gamma}_{\mathbb{M}}(x^\sharp) \dot{\cap} \dot{\gamma}_{\mathbb{M}}(y^\sharp)$;

(2) for any sequence $(x^\sharp_i)_{i\in\mathbb{N}}$, the sequence $(y^\sharp_i)_{i\in\mathbb{N}}$ defined as $y^\sharp_0 = x^\sharp_0$ and $\forall i \in \mathbb{N}.\ y^\sharp_{i+1} = y^\sharp_i \mathbin{\underline{\triangledown}_{\mathbb{I}}} x^\sharp_{i+1}$ converges in finite time.

Notice that the above soundness condition is different from the one for classic widening $\triangledown_{\mathbb{I}}$ in the forward reachability analysis.

In the section 3.5 of [42], Miné has proposed a so-called "lower widening" operator $\underline{\triangledown} \in \mathcal{D}^\sharp_{\mathbb{M}} \times \mathcal{D}^\sharp_{\mathbb{M}} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}$ for the interval/polyhedron/octagon domain. Correspondingly, we define $\underline{\triangledown}_{\mathbb{I}}$ as the the pointwise version of $\underline{\triangledown}$ (i.e. $\mathsf{I}^\sharp \,\underline{\triangledown}_{\mathbb{I}}\, \mathsf{I}^{\sharp\prime} \triangleq \lambda \ell \in \mathbb{L}.\ \mathsf{I}^\sharp(\ell) \,\underline{\triangledown}\, \mathsf{I}^{\sharp\prime}(\ell)$), and it can satisfy both the soundness and the termination condition above.

Under-approximating Abstract Backward Accessibility Semantics. Given a postcondition specified as $\mathsf{I}^\sharp_{\mathsf{post}} \in \mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}$, the corresponding concrete backward impossible failure accessibility semantics $\mathcal{S}^{\overleftarrow{if}}[\![\mathrm{P}]\!](\dot{\gamma}_{\mathbb{M}}(\mathsf{I}^\sharp_{\mathsf{post}}))$ is the greatest fixpoint of function $\mathrm{F}^{\overleftarrow{if}}[\![\mathrm{P}]\!]$ which is less than or equal to $\dot{\gamma}_{\mathbb{M}}(\mathsf{I}^\sharp_{\mathsf{post}})$. That is to say, $\mathcal{S}^{\overleftarrow{if}}[\![\mathrm{P}]\!](\dot{\gamma}_{\mathbb{M}}(\mathsf{I}^\sharp_{\mathsf{post}})) = \mathrm{gfp}^{\dot{\subseteq}}_{\dot{\gamma}_{\mathbb{M}}(\mathsf{I}^\sharp_{\mathsf{post}})} \mathrm{F}^{\overleftarrow{if}}[\![\mathrm{P}]\!]$, and it can be soundly under-approximated by the limit of a ultimately stationary sequence $(\mathsf{I}^\sharp_i)_{i\in\mathbb{N}}$, where $\mathsf{I}^\sharp_0 = \mathsf{I}^\sharp_{\mathsf{post}}$ and $\forall i \in \mathbb{N}.\ \mathsf{I}^\sharp_{i+1} = \mathsf{I}^\sharp_i \,\underline{\triangledown}_{\mathbb{I}}\, \check{\mathrm{F}}^{\sharp\,\overleftarrow{if}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_i)$.

$$\forall \mathsf{I}^\sharp_{\mathsf{post}} \in \mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}.\ \dot{\gamma}_{\mathbb{M}}(\lim_{\mathsf{I}^\sharp_{\mathsf{post}}} \lambda \mathsf{I}^\sharp.\ \mathsf{I}^\sharp \,\underline{\triangledown}_{\mathbb{I}}\, \check{\mathrm{F}}^{\sharp\,\overleftarrow{if}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp)) \,\dot{\subseteq}\, \mathrm{gfp}^{\dot{\subseteq}}_{\dot{\gamma}_{\mathbb{M}}(\mathsf{I}^\sharp_{\mathsf{post}})} \mathrm{F}^{\overleftarrow{if}}[\![\mathrm{P}]\!]. \tag{2.5}$$

In the rest of this dissertation, the under-approximating abstract backward impossible failure accessibility semantics $\check{\mathcal{S}}^{\sharp\,\overleftarrow{if}}[\![\mathrm{P}]\!]$ refers to the following definition, which computes a sound under-approximation of the concrete backward impossible failure accessibility semantics, and can automatically infer the sufficient precondition of any given postcondition in finite time.

$$\begin{array}{rcll} \check{\mathcal{S}}^{\sharp\,\overleftarrow{if}}[\![\mathrm{P}]\!] & \in & (\mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}) \mapsto (\mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}) & \text{under-appro. backward IF semantics} \\ \check{\mathcal{S}}^{\sharp\,\overleftarrow{if}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{post}}) & \triangleq & \lim_{\mathsf{I}^\sharp_{\mathsf{post}}} \lambda \mathsf{I}^\sharp.\ \mathsf{I}^\sharp \,\underline{\triangledown}_{\mathbb{I}}\, \check{\mathrm{F}}^{\sharp\,\overleftarrow{if}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp) & \end{array}$$

Example 8 (Access Control, Continued) *Consider the access control program in Fig.1.4 again, we are interested in inferring the sufficient preconditions of the trace property "the access to o fails". Suppose the abstract environment domain $\mathcal{D}^\sharp_{\mathbb{M}}$ is chosen as the interval domain,*

then "the access to o fails" can be expressed by an abstract postcondition $\mathsf{I}^\sharp_{\mathsf{post}} \in \mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}$ *such that* $\mathsf{I}^\sharp_{\mathsf{post}}(\ell_8) = \mathit{acs} \in [\text{-}\infty; 0]$ *and* $\mathsf{I}^\sharp_{\mathsf{post}}(\ell) = \top^\sharp_{\mathbb{M}}$ *for* $\ell \neq \ell_8$.

Like in the example 7, the postcondition $\mathsf{I}^\sharp_{\mathsf{post}}$ *can be refined by the intersection with the abstract forward reachability semantics* $\mathcal{S}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{pre}})$ *from the table 2.2, and we get* $\mathsf{I}^{\sharp\prime}_{\mathsf{post}} = \mathsf{I}^\sharp_{\mathsf{post}} \dot{\sqcap}^\sharp_{\mathbb{M}} \mathcal{S}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{pre}})$*, which is listed in the Table 2.4.*

ℓ	$\mathsf{I}^{\sharp\prime}_{\mathsf{post}}(\ell)$
ℓ_1	$\top^\sharp_{\mathbb{M}}$
ℓ_2	$\mathit{apv} \in [1;1] \wedge \mathit{i1} \in [\text{-}\infty;\infty] \wedge \mathit{i2} \in [\text{-}\infty;\infty] \wedge \mathit{typ} \in [\text{-}\infty;\infty] \wedge \mathit{acs} \in [\text{-}\infty;\infty]$
ℓ_3	$\mathit{apv} \in [1;1] \wedge \mathit{i1} \in [\text{-}1;2] \wedge \mathit{i2} \in [\text{-}\infty;\infty] \wedge \mathit{typ} \in [\text{-}\infty;\infty] \wedge \mathit{acs} \in [\text{-}\infty;\infty]$
ℓ_4	$\mathit{apv} \in [\text{-}1;1] \wedge \mathit{i1} \in [\text{-}1;2] \wedge \mathit{i2} \in [\text{-}\infty;\infty] \wedge \mathit{typ} \in [\text{-}\infty;\infty] \wedge \mathit{acs} \in [\text{-}\infty;\infty]$
ℓ_5	$\mathit{apv} \in [\text{-}1;1] \wedge \mathit{i1} \in [\text{-}1;2] \wedge \mathit{i2} \in [\text{-}1;2] \wedge \mathit{typ} \in [\text{-}\infty;\infty] \wedge \mathit{acs} \in [\text{-}\infty;\infty]$
ℓ_6	$\mathit{apv} \in [\text{-}1;1] \wedge \mathit{i1} \in [\text{-}1;2] \wedge \mathit{i2} \in [\text{-}1;2] \wedge \mathit{typ} \in [\text{-}\infty;\infty] \wedge \mathit{acs} \in [\text{-}\infty;\infty]$
ℓ_7	$\mathit{apv} \in [\text{-}1;1] \wedge \mathit{i1} \in [\text{-}1;2] \wedge \mathit{i2} \in [\text{-}1;2] \wedge \mathit{typ} \in [1;2] \wedge \mathit{acs} \in [\text{-}\infty;\infty]$
ℓ_8	$\mathit{apv} \in [\text{-}1;1] \wedge \mathit{i1} \in [\text{-}1;2] \wedge \mathit{i2} \in [\text{-}1;2] \wedge \mathit{typ} \in [1;2] \wedge \mathit{acs} \in [\mathbf{\text{-}2};\mathbf{0}]$

Table 2.4: Refined Abstract Postcondition for "the Access to o Fails"

From the above refined abstract postcondition $\mathsf{I}^{\sharp\prime}_{\mathsf{post}}$*, there are two possible results of the backward impossible failure accessibility analysis* $\check{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathsf{I}^{\sharp\prime}_{\mathsf{post}})$*, and they are respectively displayed in the Table 2.5 and Table 2.6 (in which the interesting part is emphasized in a bold font). The difference between these two possible results comes from the assignment "*$\mathit{apv} := (\mathit{apv} \geq 1 \wedge \mathit{i2} \leq 0)\ ?\ \text{-}1 : \mathit{apv}$*" at the point* ℓ_5*. To guarantee that "*$\mathit{apv} \leq 0$*" at point* ℓ_6*, we have two possible choices: either "*$\mathit{apv} \geq 1 \wedge \mathit{i2} \leq 0$*", or "*$\mathit{apv} \leq 0$*" at point* ℓ_5*. Since* $\check{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathsf{I}^{\sharp\prime}_{\mathsf{post}})$ *is an under-approximation, we cannot join the two cases together like in the over-approximating forward reachability analysis. Instead, we would keep one case and discard the other case (e.g. the Banal analyzer adopts the former choice, and produces results as in Table 2.5).*

ℓ	$\check{\mathcal{S}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathsf{I}^{\sharp\prime}_{\mathsf{post}})\ell$
ℓ_1	$\bot^{\sharp}_{\mathbb{M}}$
ℓ_2	$\bot^{\sharp}_{\mathbb{M}}$
ℓ_3	$\bot^{\sharp}_{\mathbb{M}}$
ℓ_4	$\bot^{\sharp}_{\mathbb{M}}$
ℓ_5	$apv \in [\mathbf{1};\mathbf{1}] \wedge i1 \in [\text{-}1;2] \wedge i2 \in [\text{-}\mathbf{1};\mathbf{0}] \wedge typ \in [\text{-}\infty;\infty] \wedge acs \in [\text{-}\infty;\infty]$
ℓ_6	$apv \in [\text{-}\mathbf{1};\mathbf{0}] \wedge i1 \in [\text{-}1;2] \wedge i2 \in [\text{-}1;2] \wedge typ \in [\text{-}\infty;\infty] \wedge acs \in [\text{-}\infty;\infty]$
ℓ_7	$apv \in [\text{-}\mathbf{1};\mathbf{0}] \wedge i1 \in [\text{-}1;2] \wedge i2 \in [\text{-}1;2] \wedge typ \in [1;2] \wedge acs \in [\text{-}\infty;\infty]$
ℓ_8	$apv \in [\text{-}1;1] \wedge i1 \in [\text{-}1;2] \wedge i2 \in [\text{-}1;2] \wedge typ \in [1;2] \wedge acs \in [\text{-}\mathbf{2};\mathbf{0}]$

Table 2.5: The Under-approximating Abstract Backward Impossible Failure Accessibility Semantics (Option 1) for "the Access to o Fails"

ℓ	$\check{\mathcal{S}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathsf{I}^{\sharp\prime}_{\mathsf{post}})\ell$
ℓ_1	$\bot^{\sharp}_{\mathbb{M}}$
ℓ_2	$\bot^{\sharp}_{\mathbb{M}}$
ℓ_3	$apv \in [1;1] \wedge i1 \in [\text{-}\mathbf{1};\mathbf{0}] \wedge i2 \in [\text{-}\infty;\infty] \wedge typ \in [\text{-}\infty;\infty] \wedge acs \in [\text{-}\infty;\infty]$
ℓ_4	$apv \in [\text{-}\mathbf{1};\mathbf{0}] \wedge i1 \in [\text{-}1;2] \wedge i2 \in [\text{-}\infty;\infty] \wedge typ \in [\text{-}\infty;\infty] \wedge acs \in [\text{-}\infty;\infty]$
ℓ_5	$apv \in [\text{-}\mathbf{1};\mathbf{0}] \wedge i1 \in [\text{-}1;2] \wedge i2 \in [\text{-}1;2] \wedge typ \in [\text{-}\infty;\infty] \wedge acs \in [\text{-}\infty;\infty]$
ℓ_6	$apv \in [\text{-}\mathbf{1};\mathbf{0}] \wedge i1 \in [\text{-}1;2] \wedge i2 \in [\text{-}1;2] \wedge typ \in [\text{-}\infty;\infty] \wedge acs \in [\text{-}\infty;\infty]$
ℓ_7	$apv \in [\text{-}\mathbf{1};\mathbf{0}] \wedge i1 \in [\text{-}1;2] \wedge i2 \in [\text{-}1;2] \wedge typ \in [1;2] \wedge acs \in [\text{-}\infty;\infty]$
ℓ_8	$apv \in [\text{-}1;1] \wedge i1 \in [\text{-}1;2] \wedge i2 \in [\text{-}1;2] \wedge typ \in [1;2] \wedge acs \in [\text{-}\mathbf{2};\mathbf{0}]$

Table 2.6: The Under-approximating Abstract Backward Impossible Failure Accessibility Semantics (Option 2) for "the Access to o Fails"

Alternatively, we could use the disjunctive completion [4] and maintain the abstract environment elements (i.e. sufficient preconditions) from both two tables. In this example, the disjunctive completion could provide us with the exact backward impossible failure accessibility semantics and its cost is not too heavy, because we need to keep a disjunction of two abstract environment elements only at the point ℓ_5, while the abstract environment elements at other points are either the same from two tables or the bottom in one table (which can be omitted). In order to distinguish from the over-approximating analysis introduced later in section 2.4.3,

here we adopt the result (from the Banal analyzer) in Table 2.5 as an under-approximation.

Therefore, we have successfully inferred some sufficient preconditions of "the Access to o Fails": "acs $\in [-2; 0]$*" at* ℓ_8*, "apv* $\in [-1; 0]$*" at* ℓ_7 *and* ℓ_6*, and "apv* $\in [1; 1] \wedge i2 \in [-1; 0]$*" at* ℓ_5*, which implies that the zero or negative value of i2 (i.e. the input from 2nd admin) guarantees the access failure.* □

2.4.3 Over-approximating Abstract Backward Impossible Failure Accessibility Analysis

Besides the under-approximating backward analysis described in the last section, we would like to design an over-approximating abstract backward impossible failure accessibility analysis as well, which computes an over-approximation of the set of states from which all the executions must satisfy the given postcondition $\mathsf{I}^\sharp_{\mathsf{post}}$.

Such an over-approximation is neither a sufficient precondition for $\mathsf{I}^\sharp_{\mathsf{post}}$ to hold, nor a necessary precondition, due to the possible non-determinism of the program. Thus, it may seem to be not of practical use. However, instead of directly using such an over-approximating abstract backward impossible failure accessibility semantics in the responsibility analysis, we intend to utilize its set-complement as partitioning directives (which will be further discussed in Chapter 8), and it represents a set of states from which there must exist at least one concrete execution trace that fails the postcondition $\mathsf{I}^\sharp_{\mathsf{post}}$. This may seem to be counter-intuitive at first sight, since most abstract domains (e.g. intervals, octagons, polyhedra) do not support complements. For instance, the complement of a polyhedron is a disjunction of affine inequalities, which cannot be expressed by a single polyhedron. However, it would not be a problem for our responsibility analysis,

since we do not require to represent the complement set by a single abstract environment element. Instead, we could keep multiple partitioning directives at every program point. Take the complement of a polyhedron as an example, each affine inequality (or the heuristically selected ones when the number of affine inequalities exceeds a threshold) can be used as a partitioning directive in the responsibility analysis.

In the following, we formalize the framework of over-approximating backward impossible failure accessibility analysis, which essentially corresponds to an over-approximating version of section 3 of [42] and section 2.4.2 of this dissertation. More precisely, it consists of the over-approximating backward transfer functions (e.g. for the boolean tests and assignments in our simple programming language) and a narrowing operator that over-approximates meets and enforces termination.

Over-approximating Abstract Backward Transfer Function. Here we need an over-approximating abstract backward transfer function $\hat{\mathrm{F}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!] \in (\mathbb{L} \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}}) \mapsto (\mathbb{L} \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}})$ (the symbol $\hat{}$ denotes over-approximations) that satisfies the following soundness condition (2.6).

$$\forall \mathsf{I}^{\sharp} \in \mathbb{L} \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}}.\ \mathrm{F}_{\overleftarrow{if}}[\![\mathrm{P}]\!] \circ \dot{\gamma}_{\mathbb{M}}(\mathsf{I}^{\sharp}) \mathrel{\dot{\subseteq}} \dot{\gamma}_{\mathbb{M}} \circ \hat{\mathrm{F}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathsf{I}^{\sharp}). \tag{2.6}$$

Like $\check{\mathrm{F}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!]$ is defined by the combination of $\check{\mathrm{F}}^{\sharp}_{\ell\leftarrow\ell'}[\![\mathrm{P}]\!]$, the over-approximating version $\hat{\mathrm{F}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!]$ can be defined by combining $\hat{\mathrm{F}}^{\sharp}_{\ell\leftarrow\ell'}[\![\mathrm{P}]\!] \in \mathcal{D}^{\sharp}_{\mathbb{M}} \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}}$:

$\hat{\mathrm{F}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!] \in (\mathbb{L} \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}}) \mapsto (\mathbb{L} \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}})$ over-approximating backward IF function

$\hat{\mathrm{F}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!]\mathsf{I}^{\sharp} \triangleq \lambda\ell \in \mathbb{L}.\ \sqcap^{\sharp}_{\mathbb{M}\ \ell'\in\mathbb{L}} \hat{\mathrm{F}}^{\sharp}_{\ell\leftarrow\ell'}[\![\mathrm{P}]\!](\mathsf{I}^{\sharp}(\ell'))$

where the meet $\sqcap^{\sharp}_{\mathbb{M}}$ is exact and $\hat{\mathrm{F}}^{\sharp}_{\ell\leftarrow\ell'}[\![\mathrm{P}]\!]$ needs to satisfy the condition (2.7).

$$\forall \mathsf{M}^{\sharp} \in \mathcal{D}^{\sharp}_{\mathbb{M}}.\ \mathrm{F}_{\ell\leftarrow\ell'}[\![\mathrm{P}]\!] \circ \gamma_{\mathbb{M}}(\mathsf{M}^{\sharp}) \ \subseteq\ \gamma_{\mathbb{M}} \circ \hat{\mathrm{F}}^{\sharp}_{\ell\leftarrow\ell'}[\![\mathrm{P}]\!](\mathsf{M}^{\sharp}). \tag{2.7}$$

Similar to the definition of $\check{\mathrm{F}}^{\sharp}_{\ell\leftarrow\ell'}[\![\mathrm{P}]\!]$, here $\hat{\mathrm{F}}^{\sharp}_{\ell\leftarrow\ell'}[\![\mathrm{P}]\!]$ is defined such that: (1) if $\ell = \ell'$, then $\hat{\mathrm{F}}^{\sharp}_{\ell\leftarrow\ell'}[\![\mathrm{P}]\!](\mathrm{M}^{\sharp}) = \mathrm{M}^{\sharp}$; (2) if $\ell \neq \ell'$ and there is not an atomic action from ℓ to ℓ', then $\hat{\mathrm{F}}^{\sharp}_{\ell\leftarrow\ell'}[\![\mathrm{P}]\!](\mathrm{M}^{\sharp}) = \top^{\sharp}_{\mathbb{M}}$; and (3) otherwise, there is an atomic action from ℓ to ℓ', then $\hat{\mathrm{F}}^{\sharp}_{\ell\leftarrow\ell'}[\![\mathrm{P}]\!](\mathrm{M}^{\sharp})$ over-approximates the sufficient precondition that guarantees $\mathrm{M}^{\sharp}$ to hold after executing the atomic action.

Among the above three cases, (3) is the difficult one. In the following, we take the simple programming language in Fig. 1.2 as an example, mimic the section 3 of [42] and discusses how $\hat{\mathrm{F}}^{\sharp}_{\ell\leftarrow\ell'}[\![\mathrm{P}]\!]$ is implemented for atomic actions of form ${}^{\ell_1}a^{\ell_2}$ (e.g. boolean tests ${}^{\ell_1}b^{\ell_2}$, assignments ${}^{\ell_1}x := e^{\ell_2}$), where $\hat{\mathrm{F}}^{\sharp}_{\ell_1\leftarrow\ell_2}[\![\mathrm{P}]\!](\mathrm{M}^{\sharp}) \triangleq \overleftarrow{\tau}^{\sharp}\{\!|\, a \,|\!\}\mathrm{M}^{\sharp}$ such that $\forall \mathrm{M}^{\sharp} \in \mathcal{D}^{\sharp}_{\mathbb{M}}.\ \overleftarrow{\tau}\{\!|\, a \,|\!\} \circ \gamma_{\mathbb{M}}(\mathrm{M}^{\sharp}) \subseteq \gamma_{\mathbb{M}} \circ \overleftarrow{\tau}^{\sharp}\{\!|\, a \,|\!\}(\mathrm{M}^{\sharp})$.

1) *Boolean tests (guards)*.

Affine guards. First, we consider the polyhedron domain, and the guard is of form $\vec{a}\cdot\vec{x} \geq b$ such that it can be exactly represented by polyhedra. In this case, the concrete backward transfer function can be rephrased into:

$$\overleftarrow{\tau}\{\!|\, \vec{a}\cdot\vec{x} \geq b \,|\!\}\mathrm{M} = \mathrm{M} \cup \{\rho \in \mathbb{M} \mid [\![\vec{a}\cdot\vec{x} \geq b]\!]\rho = \{\mathrm{f}\}\} = \mathrm{M} \cup \{\rho \in \mathbb{M} \mid \vec{a}\cdot\vec{\rho} < b\}$$

where $\vec{\rho}$ denotes the vector of variable values in the environment ρ.

To over-approximate $\overleftarrow{\tau}\{\!|\, \vec{a}\cdot\vec{x} \geq b \,|\!\}$, we define the corresponding abstract transfer function $\overleftarrow{\tau}^{\sharp}\{\!|\vec{a}\cdot\vec{x} \geq b|\!\} \in \mathcal{D}^{\sharp}_{\mathbb{M}} \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}}$ as:

$$\overleftarrow{\tau}^{\sharp}\{\!|\vec{a}\cdot\vec{x} \geq b|\!\}\mathrm{M}^{\sharp} \triangleq \mathrm{M}^{\sharp} \sqcup^{\sharp}_{\mathbb{M}} \vec{a}\cdot\vec{x} < b. \tag{2.8}$$

Since $\sqcup^{\sharp}_{\mathbb{M}}$ soundly approximates the concrete join operator $\cup$, it is easy to see the soundness condition (2.7) holds. Moreover, if we use the disjunctive completion [4], then both $\mathrm{M}^{\sharp}$ and $\vec{a}\cdot\vec{x} < b$ can be kept without the join, i.e. $\overleftarrow{\tau}^{\sharp}\{\!|\, \vec{a}\cdot\vec{x} \geq b \,|\!\}\mathrm{M}^{\sharp} \triangleq \{\mathrm{M}^{\sharp},\ \vec{a}\cdot\vec{x} < b\}$, which can greatly improve the precision of analysis. When the number

of disjunctive elements exceeds a threshold, we can replace them by their join. It is worthy to mention that current polyhedra abstract domain [10] supports strict constraints like $\vec{a} \cdot \vec{x} < b$. For the original polyhedra abstract domain that cannot express strict constraints, it is sound to replace $\vec{a} \cdot \vec{x} < b$ by $\vec{a} \cdot \vec{x} \leq b$ in (2.8).

For the interval domain, the same technique can be applied to $\overleftarrow{\tau}^\sharp\{\!|\pm\mathcal{x} \geq b|\!\}$, since a box (i.e. a Cartesian products of intervals) is a special case of polyhedron. Similarly, we can handle $\overleftarrow{\tau}^\sharp\{\!|\pm\mathcal{x} \pm y \geq b|\!\}$ for the octagon domain in the same way.

Extended affine guards. For strict guards and the guards with a non-deterministic constant, the corresponding abstract transfer function is defined as:

$$\begin{aligned}
\overleftarrow{\tau}^\sharp\{\!|\vec{a} \cdot \vec{\mathcal{x}} > b|\!\}\mathrm{M}^\sharp &\triangleq \mathrm{M}^\sharp \sqcup^\sharp_{\mathbb{M}} \vec{a} \cdot \vec{x} \leq b \\
\overleftarrow{\tau}^\sharp\{\!|\vec{a} \cdot \vec{\mathcal{x}} > [b;c]|\!\}\mathrm{M}^\sharp &\triangleq \mathrm{M}^\sharp \sqcup^\sharp_{\mathbb{M}} \vec{a} \cdot \vec{x} < c \\
\overleftarrow{\tau}^\sharp\{\!|\vec{a} \cdot \vec{\mathcal{x}} = [b;c]|\!\}\mathrm{M}^\sharp &\triangleq \mathrm{M}^\sharp \sqcup^\sharp_{\mathbb{M}} \vec{a} \cdot \vec{x} < b \sqcup^\sharp_{\mathbb{M}} \vec{a} \cdot \vec{x} > c.
\end{aligned} \tag{2.9}$$

Boolean operations. For the boolean conjunctions and disjunctions of affine guards, the section 3.2 of [42] has shown that the concrete transfer function has the following property:

$$\begin{aligned}
\overleftarrow{\tau}\{\!|t_1 \vee t_2|\!\} &= \overleftarrow{\tau}\{\!|t_1|\!\} \cap \overleftarrow{\tau}\{\!|t_2|\!\} \\
\overleftarrow{\tau}\{\!|t_1 \wedge t_2|\!\} &= \overleftarrow{\tau}\{\!|t_1|\!\} \circ \overleftarrow{\tau}\{\!|t_2|\!\}.
\end{aligned} \tag{2.10}$$

Since the abstract meet $\sqcap^\sharp_{\mathbb{M}}$ is exact in the interval/octagon/polyhedron domain, we can define the corresponding abstract transfer functions which are also exact:

$$\begin{aligned}
\overleftarrow{\tau}^\sharp\{\!|t_1 \vee t_2|\!\} &= \overleftarrow{\tau}^\sharp\{\!|t_1|\!\} \sqcap^\sharp_{\mathbb{M}} \overleftarrow{\tau}^\sharp\{\!|t_2|\!\} \\
\overleftarrow{\tau}^\sharp\{\!|t_1 \wedge t_2|\!\} &= \overleftarrow{\tau}^\sharp\{\!|t_1|\!\} \circ \overleftarrow{\tau}^\sharp\{\!|t_2|\!\}.
\end{aligned} \tag{2.11}$$

In addition, the boolean negation of affine guards $\overleftarrow{\tau}\{\!|\neg(\vec{a} \cdot \vec{\mathcal{x}} \geq b)|\!\}$ is equivalent to $\overleftarrow{\tau}\{\!|\vec{a} \cdot \vec{\mathcal{x}} < b|\!\}$, and the negation of conjunctions or disjunctions can be eliminated by De Morgan' law.

2) ***Projection***.

In order to reduce the backward transfer function of assignments to the backward transfer function of guards, [42] introduces a projection action $x := [-\infty; +\infty]$, which is a special form of assignment that forgets the value of a variable. Here we do the same, and reuse the under-approximating abstract backward transfer function for projections in [42], since it is proved to be exact (i.e. both an over-approximation and an under-approximation of the concrete transfer function).

$$\overleftarrow{\tau}^{\sharp}\{\!|x := [-\infty; +\infty]|\!\}\mathrm{M}^{\sharp} \triangleq \begin{cases} \mathrm{M}^{\sharp} & \text{if } \gamma_{\mathbb{M}}(\tau^{\sharp}\{\!|x := [-\infty; +\infty]|\!\}\mathrm{M}^{\sharp}) = \gamma_{\mathbb{M}}(\mathrm{M}^{\sharp}) \\ \bot_{\mathbb{M}}^{\sharp} & \text{otherwise.} \end{cases} \tag{2.12}$$

The projection is used to model variable addition "add x" and removal "del x", which are not included in the language syntax but implicitly created to model assignments. Again, since the under-approximating abstract backward transfer functions for these two actions in [42] are exact, we can simply reuse them:

$$\begin{aligned} \overleftarrow{\tau}^{\sharp}\{\!|\text{del } x|\!\} &= \tau^{\sharp}\{\!|\text{add } x|\!\} \\ \overleftarrow{\tau}^{\sharp}\{\!|\text{add } x|\!\} &= \tau^{\sharp}\{\!|\text{del } x|\!\} \circ \overleftarrow{\tau}^{\sharp}\{\!|x := [-\infty; +\infty]|\!\}. \end{aligned} \tag{2.13}$$

3) ***Assignments***.

Reduction to guards. As shown in section 3.4 of [42], assignments $x := e$ can be reduced to: add a temporary variable x', then pass a guard $x' = e$, remove the variable x, and rename x' as x. Furthermore, the backward transfer function is reduced to:

$$\overleftarrow{\tau}\{\!|x := e|\!\} = \tau\{\!|\text{del } x'|\!\} \circ \overleftarrow{\tau}\{\!|x' := [-\infty; +\infty]|\!\} \circ \overleftarrow{\tau}\{\!|x' = e|\!\} \circ \tau\{\!|\text{add } x|\!\} \circ [x'/x]$$

where $[x'/x]$ represents renaming x as x'. Correspondingly, the over-approximating backward transfer function can be defined as:

$$\overleftarrow{\tau}^{\sharp}\{\!|\, x := e \,|\!\} \;=\; \tau^{\sharp}\{\!|\mathrm{del}\ x'|\!\} \circ \overleftarrow{\tau}^{\sharp}\{\!|\, x' := [-\infty;+\infty] \,|\!\} \circ \overleftarrow{\tau}^{\sharp}\{\!|\, x' = e \,|\!\} \circ \tau^{\sharp}\{\!|\mathrm{add}\ x|\!\} \circ [x'/x] \tag{2.14}$$

in which $\overleftarrow{\tau}^{\sharp}\{\!|\, x' = e \,|\!\}$ for the guard $x' = e$ is over-approximating, while $\tau^{\sharp}\{\!|\mathrm{del}\ x'|\!\}$, $\overleftarrow{\tau}^{\sharp}\{\!|\, x' := [-\infty;+\infty] \,|\!\}$, $\tau^{\sharp}\{\!|\mathrm{add}\ x|\!\}$ and $[x'/x]$ are exact.

Special cases of assignments. There are a few special cases such that the above general definition $\overleftarrow{\tau}^{\sharp}\{\!|\, x := e \,|\!\}$ can be simplified. For the case where the variable x is not used in the expression e, there is no need to introduce the temporal variable x', and the corresponding $\overleftarrow{\tau}^{\sharp}\{\!|\, x := e \,|\!\}$ is simplified into:

$$\overleftarrow{\tau}^{\sharp}\{\!|\, x := e \,|\!\} \;=\; \overleftarrow{\tau}^{\sharp}\{\!|\, x := [-\infty;+\infty] \,|\!\} \circ \overleftarrow{\tau}^{\sharp}\{\!|\, x = e \,|\!\}. \tag{2.15}$$

Moreover, for purely non-deterministic assignments $x := [a;b]$, variable shifts $x := x + [a;b]$ and variable copies $x := y$, the theorem 9 of [42] yields sound and exact backward transfer function, thus we can reuse them.

Another case is when the assigned expression e is invertible, i.e. there exists an expression e^{-1} that allows recovering the initial value of x. For example, in the assignment $x := x + 1$, the expression $x + 1$ can be inverted by $x - 1$. In such a case, the backward transfer function for $x := e$ can be replaced by the forward transfer function for $x := e^{-1}$, i.e. $\overleftarrow{\tau}^{\sharp}\{\!|\, x := e \,|\!\} = \tau^{\sharp}\{\!|\, x := e^{-1} \,|\!\}$, which provides a sound over-approximation.

4) ***Expression approximation***.

In the above, we have discussed how to handle affine expressions in guards and assignments. As for non-affine numeric expressions, [42] proposes to over-approximate arbitrary expressions by affine ones, and this is accomplished by the linearization technique [30] that performs interval arithmetic on non-linear expression parts. Similarly,

here we could convert non-affine expressions into affine expressions with some non-determinism embedded in a constant interval (or constant coefficients), such that the original non-affine expressions are under-approximated. Then, by replacing the original non-affine expressions with affine ones, we can reuse the solution designed for affine expressions and correspondingly get over-approximating backward transfer functions for arbitrary guards and assignments.

Narrowing. Up to now, we have discussed the design of over-approximating backward transfer function $\hat{\mathrm{F}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!]$. By the soundness condition 2.3, the greatest fixpoint $\mathrm{gfp}^{\dot{\sqsubseteq}^{\sharp}_{\mathbb{M}}}_{\mathsf{I}^{\sharp}_{\mathsf{post}}} \hat{\mathrm{F}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!]$ would be an over-approximation of the concrete backward impossible failure accessibility semantics $\mathrm{gfp}^{\dot{\subseteq}}_{\dot{\gamma}_{\mathbb{M}}(\mathsf{I}^{\sharp}_{\mathsf{post}})} \mathrm{F}_{\overleftarrow{if}}[\![\mathrm{P}]\!]$. However, it is generally difficult to compute $\mathrm{gfp}^{\dot{\sqsubseteq}^{\sharp}_{\mathbb{M}}}_{\mathsf{I}^{\sharp}_{\mathsf{post}}} \hat{\mathrm{F}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!]$, since the decreasing iteration may be infinite. In many cases, a (dual) widening is used to accelerate the convergence, but it does not apply here, since the (dual) widening makes downwards extrapolation which may jump below the greatest fixpoint. Therefore, we propose to over-approximate a decreasing iteration by narrowing, because the narrowing can only do interpolations which prevent jumping below any fixpoint.

The narrowing operator $\triangle_{\mathbb{I}} \in (\mathbb{L} \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}}) \times (\mathbb{L} \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}}) \mapsto (\mathbb{L} \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}})$ on the abstract invariant domain satisfies the following soundness and termination conditions:

(1) $\forall x^{\sharp}, y^{\sharp} \in (\mathbb{L} \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}}).\ y^{\sharp} \dot{\sqsubseteq}^{\sharp}_{\mathbb{M}} x^{\sharp} \Rightarrow y^{\sharp} \dot{\sqsubseteq}^{\sharp}_{\mathbb{M}} (x^{\sharp} \triangle_{\mathbb{I}} y^{\sharp}) \dot{\sqsubseteq}^{\sharp}_{\mathbb{M}} x^{\sharp}$;

(2) for any sequence $(x^{\sharp}_i)_{i\in\mathbb{N}}$, the sequence $(y^{\sharp}_i)_{i\in\mathbb{N}}$ defined as $y^{\sharp}_0 = x^{\sharp}_0$ and $\forall i \in \mathbb{N}.\ y^{\sharp}_{i+1} = y^{\sharp}_i \triangle_{\mathbb{I}} x^{\sharp}_{i+1}$ converges in finite time.

The implementation of $\triangle_{\mathbb{I}}$ naturally follows the narrowing operator $\triangle_{\mathbb{M}} \in \mathcal{D}^{\sharp}_{\mathbb{M}} \times \mathcal{D}^{\sharp}_{\mathbb{M}} \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}}$ provided by the abstract environment domain $\mathcal{D}^{\sharp}_{\mathbb{M}}$, such that $\mathsf{I}^{\sharp} \triangle_{\mathbb{I}} \mathsf{I}^{\sharp\prime} \triangleq \lambda \ell \in \mathbb{L}.\ \mathsf{I}^{\sharp}(\ell) \triangle_{\mathbb{M}} \mathsf{I}^{\sharp\prime}(\ell)$.

Over-approximating Abstract Backward impossible failure Accessibility Semantics. Given a postcondition specified as $\mathsf{I}^\sharp_{\mathsf{post}} \in \mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}$, the concrete backward impossible failure accessibility semantics $\mathcal{S}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\dot{\gamma}_{\mathbb{M}}(\mathsf{I}^\sharp_{\mathsf{post}})) = \mathrm{gfp}^{\dot{\subseteq}}_{\dot{\gamma}_{\mathbb{M}}(\mathsf{I}^\sharp_{\mathsf{post}})} \mathrm{F}_{\overleftarrow{if}}[\![\mathrm{P}]\!]$ can be over-approximated by the limit of a ultimately stationary sequence $(\mathsf{I}^\sharp_i)_{i\in\mathbb{N}}$, where $\mathsf{I}^\sharp_0 = \mathsf{I}^\sharp_{\mathsf{post}}$ and $\forall i \in \mathbb{N}.\ \mathsf{I}^\sharp_{i+1} = \mathsf{I}^\sharp_i \mathbin{\triangle_{\mathbb{I}}} \hat{\mathrm{F}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_i)$.

$$\forall \mathsf{I}^\sharp_{\mathsf{post}} \in \mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}.\ \mathrm{gfp}^{\dot{\subseteq}}_{\dot{\gamma}_{\mathbb{M}}(\mathsf{I}^\sharp_{\mathsf{post}})} \mathrm{F}_{\overleftarrow{if}}[\![\mathrm{P}]\!] \dot{\subseteq} \dot{\gamma}_{\mathbb{M}}(\mathrm{lim}_{\mathsf{I}^\sharp_{\mathsf{post}}}\ \lambda \mathsf{I}^\sharp.\ \mathsf{I}^\sharp \mathbin{\triangle_{\mathbb{I}}} \hat{\mathrm{F}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp)). \quad (2.16)$$

In the rest of this dissertation, the over-approximating abstract backward impossible failure accessibility semantics $\hat{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!]$ refers to the following definition, which gives an over-approximation of $\mathcal{S}_{\overleftarrow{if}}[\![\mathrm{P}]\!]$ and can be computed in finite time.

$$\begin{array}{rcll} \hat{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!] & \in & (\mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}) \mapsto (\mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}) & \text{over-approximating IF semantics} \\ \hat{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{post}}) & \triangleq & \mathrm{lim}_{\mathsf{I}^\sharp_{\mathsf{post}}}\ \lambda \mathsf{I}^\sharp.\ \mathsf{I}^\sharp \mathbin{\triangle_{\mathbb{I}}} \hat{\mathrm{F}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp) & \end{array}$$

In practice, the abstract environment domain $\mathcal{D}^\sharp_{\mathbb{M}}$ may not have an effective narrowing operator $\triangle_{\mathbb{M}}$, which makes the corresponding $\triangle_{\mathbb{I}}$ of no practical use. If this is the case, like in the forward reachability analysis, we can just omit the narrowing operator, and iterate the function $\hat{\mathrm{F}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!]$ until the analysis result is satisfactory (typcially, the number of iterations needed is quite low).

Example 9 (Access Control, Continued) *Using the refined abstract postcondition* $\mathsf{I}^{\sharp\prime}_{\mathsf{post}}$ *from Example 8 that represents the trace property "the access to o fails", an over-approximating backward impossible failure accessibility analysis* $\hat{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathsf{I}^{\sharp\prime}_{\mathsf{post}})$ *creates the result displayed in Table 2.7. Here we adopt the disjunctive completion to gain precision, i.e. at point* ℓ_5*, the disjunction of two abstract environment elements are maintained, which gives the most precise backward impossible failure accessibility semantics. If the disjunctive completion is not used at point* ℓ_5*,*

then we can simply join these two abstract elements together, and get the result same as the abstract forward reachability semantics $\mathcal{S}^{\sharp}_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^{\sharp}_{\mathsf{pre}})$ *from the point* ℓ_5 *to the point* ℓ_1*, which is still sound but imprecise for the further responsibility analysis.* □

ℓ	$\hat{\mathcal{S}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathsf{I}^{\sharp\prime}_{\mathsf{post}})\ell$
ℓ_1	$\bot^{\sharp}_{\mathbb{M}}$
ℓ_2	$\bot^{\sharp}_{\mathbb{M}}$
ℓ_3	$apv \in [1;1] \wedge i1 \in [\text{-}\mathbf{1};\mathbf{0}] \wedge i2 \in [\text{-}\infty;\infty] \wedge typ \in [\text{-}\infty;\infty] \wedge acs \in [\text{-}\infty;\infty]$
ℓ_4	$apv \in [\text{-}\mathbf{1};\mathbf{0}] \wedge i1 \in [\text{-}1;2] \wedge i2 \in [\text{-}\infty;\infty] \wedge typ \in [\text{-}\infty;\infty] \wedge acs \in [\text{-}\infty;\infty]$
ℓ_5	$\{apv \in [\text{-}\mathbf{1};\mathbf{0}] \wedge i1 \in [\text{-}1;2] \wedge i2 \in [\text{-}1;2] \wedge typ \in [\text{-}\infty;\infty] \wedge acs \in [\text{-}\infty;\infty],$ $apv \in [\mathbf{1};\mathbf{1}] \wedge i1 \in [\text{-}1;2] \wedge i2 \in [\text{-}\mathbf{1};\mathbf{0}] \wedge typ \in [\text{-}\infty;\infty] \wedge acs \in [\text{-}\infty;\infty]\}$
ℓ_6	$apv \in [\text{-}\mathbf{1};\mathbf{0}] \wedge i1 \in [\text{-}1;2] \wedge i2 \in [\text{-}1;2] \wedge typ \in [\text{-}\infty;\infty] \wedge acs \in [\text{-}\infty;\infty]$
ℓ_7	$apv \in [\text{-}\mathbf{1};\mathbf{0}] \wedge i1 \in [\text{-}1;2] \wedge i2 \in [\text{-}1;2] \wedge typ \in [1;2] \wedge acs \in [\text{-}\infty;\infty]$
ℓ_8	$apv \in [\text{-}1;1] \wedge i1 \in [\text{-}1;2] \wedge i2 \in [\text{-}1;2] \wedge typ \in [1;2] \wedge acs \in [\text{-}\mathbf{2};\mathbf{0}]$

Table 2.7: The Over-approximating Abstract Backward Impossible Failure Accessibility Semantics for "the Access to o Fails" with Disjunctive Completion

2.5 Other Backward/Forward Semantics

For the sake of completeness, this section briefly introduces two other types of backward accessibility or forward reachability semantics, which are not used in the responsibility analysis.

2.5.1 Backward Possible Success Accessibility Semantics

The backward possible success accessibility semantics is defined as the conjugate of the backward impossible failure accessibility semantics. More precisely, given a post-condition $\mathsf{I}_{\mathsf{post}} \in \mathbb{L} \mapsto \wp(\mathbb{M})$, the backward impossible failure accessibility semantics

$\mathcal{S}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{post}})$ specifies a precondition for reaching only the states satisfying $\mathsf{I}_{\mathsf{post}}$, while the backward possible success accessibility semantics $\mathcal{S}_{\overleftarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{post}})$ specifies a precondition for the existence of at least one execution reaching a state satisfying $\mathsf{I}_{\mathsf{post}}$. That is to say, $\mathcal{S}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{post}})$ infers sufficient preconditions of $\mathsf{I}_{\mathsf{post}}$, and $\mathcal{S}_{\overleftarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{post}})$ infers necessary preconditions of $\mathsf{I}_{\mathsf{post}}$. It is obvious that the strongest necessary precondition of $\mathsf{I}_{\mathsf{post}}$ is the complement (or negation) of the weakest sufficient precondition of its complement $\dot{\neg}\mathsf{I}_{\mathsf{post}}$. Thus, the definition of $\mathcal{S}_{\overleftarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{post}})$ is formally given as the following.

$$
\begin{array}{rcl}
\mathcal{S}_{\overleftarrow{ps}}[\![\mathrm{P}]\!] & \in & (\mathbb{L} \mapsto \wp(\mathbb{M})) \mapsto (\mathbb{L} \mapsto \wp(\mathbb{M})) \quad \text{backward PS accessibility semantics} \\
\mathcal{S}_{\overleftarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{post}})\ell & \triangleq & \dot{\neg}\, \mathcal{S}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\dot{\neg}\, \mathsf{I}_{\mathsf{post}})\ell \\
& = & \neg\{\rho \in \mathbb{M} \mid \forall \sigma \in \mathbb{S}^*, \ell' \in \mathbb{L}, \rho' \in \mathbb{M}.\ (\langle \ell,\ \rho\rangle \sigma \langle \ell',\ \rho'\rangle \in [\![\mathrm{P}]\!]^{\mathsf{It}} \Rightarrow \\
& & \qquad \rho' \notin \mathsf{I}_{\mathsf{post}}(\ell'))\} \\
& = & \neg\{\rho \in \mathbb{M} \mid \forall \sigma \in \mathbb{S}^*, \ell' \in \mathbb{L}, \rho' \in \mathbb{M}.\ (\langle \ell,\ \rho\rangle \sigma \langle \ell',\ \rho'\rangle \notin [\![\mathrm{P}]\!]^{\mathsf{It}} \vee \\
& & \qquad \rho' \notin \mathsf{I}_{\mathsf{post}}(\ell'))\} \\
& = & \{\rho \in \mathbb{M} \mid \exists \sigma \in \mathbb{S}^*, \ell' \in \mathbb{L}, \rho' \in \mathbb{M}.\ (\langle \ell,\ \rho\rangle \sigma \langle \ell',\ \rho'\rangle \in [\![\mathrm{P}]\!]^{\mathsf{It}} \wedge \\
& & \qquad \rho' \in \mathsf{I}_{\mathsf{post}}(\ell'))\}
\end{array}
$$

Similar to the fixpoint definition of backward impossible failure accessibility semantics $\mathcal{S}_{\overleftarrow{if}}[\![\mathrm{P}]\!]$, the backward possible success accessibility semantics $\mathcal{S}_{\overleftarrow{ps}}[\![\mathrm{P}]\!]$ can be defined as the least fixpoint of a concrete backward transfer function $\mathrm{F}_{\overleftarrow{ps}}[\![\mathrm{P}]\!]$.

$$
\begin{array}{rcl}
\mathcal{S}_{\overleftarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{post}}) & = & \mathrm{lfp}^{\dot{\subseteq}}_{\mathsf{I}_{\mathsf{post}}}\, \mathrm{F}_{\overleftarrow{ps}}[\![\mathrm{P}]\!] \\
\mathrm{F}_{\overleftarrow{ps}}[\![\mathrm{P}]\!] & \in & (\mathbb{L} \mapsto \wp(\mathbb{M})) \mapsto (\mathbb{L} \mapsto \wp(\mathbb{M})) \qquad \text{backward PS transfer function} \\
\mathrm{F}_{\overleftarrow{ps}}[\![\mathrm{P}]\!]\mathsf{I} & \triangleq & \mathsf{I} \mathbin{\dot{\cup}} \lambda \ell \in \mathbb{L}.\{\rho \in \mathbb{M} \mid \exists \ell' \in \mathbb{L}, \rho' \in \mathsf{I}(\ell').\ \langle \ell,\ \rho\rangle \rightarrow \langle \ell',\ \rho'\rangle\}
\end{array}
$$

In the abstract, an over-approximating backward possible success accessibility analysis is used to infer necessary preconditions, since an over-approximation of the strongest necessary precondition is still a necessary precondition. Usually it is combined with the forward (possible success) reachability analysis to compute program invariants (e.g. the

Interproc Analyzer [50]), and the corresponding analysis result would be more precise than sole forward analyses.

However, it is rare to see an under-approximating backward possible success accessibility analysis in the literature, even though the result of such an analysis would be useful. For example, let the postcondition $\mathsf{I}_{\mathsf{post}}$ specify error states, then the over-approximating backward possible success accessibility analysis infers necessary preconditions of reaching an error state. Meanwhile, the corresponding under-approximating analysis computes a set of states from which there must exist at least one concrete execution going wrong, and further inspections on such states can be used to determine the origin of errors.

The keys of designing such an under-approximating abstract backward possible success accessibility analysis include: (1) an abstract backward transfer function that under-approximates the corresponding concrete backward transfer function $\mathrm{F}_{\overleftarrow{ps}}[\![\mathrm{P}]\!]$; (2) a dual widening operator that under-approximates joins and guarantees termination. It is a thorny problem to build such a dual widening operator for classic numerical abstract domains. Therefore, in this dissertation, we replace the under-approximating backward possible success accessibility analysis by the complement of an over-approximating backward impossible failure accessibility analysis, whose result fits in our framework of responsibility analysis.

2.5.2 Forward Impossible Failure Reachability Semantics

It is not hard to find that $\mathcal{S}_{\overleftarrow{ps}}[\![\mathrm{P}]\!]$ is the lower adjoint of a Galois connection, and the corresponding upper adjoint is called the *forward impossible failure reachability semantics* $\mathcal{S}_{\overrightarrow{if}}[\![\mathrm{P}]\!]$, which computes a set of states that can be reached only from states satisfying

the given precondition $\mathsf{I}_{\mathsf{pre}}$. More formally, we have:

$$\langle \mathbb{L} \mapsto \wp(\mathbb{M}),\ \dot{\subseteq} \rangle \underset{\mathcal{S}_{\overrightarrow{ps}}[\![\mathrm{P}]\!]}{\overset{\mathcal{S}_{\overrightarrow{if}}[\![\mathrm{P}]\!]}{\leftrightarrows}} \langle \mathbb{L} \mapsto \wp(\mathbb{M}),\ \dot{\subseteq} \rangle$$

where $\mathcal{S}_{\overrightarrow{if}}[\![\mathrm{P}]\!]$ is defined as:

$$\begin{array}{rcll} \mathcal{S}_{\overrightarrow{if}}[\![\mathrm{P}]\!] & \in & (\mathbb{L} \mapsto \wp(\mathbb{M})) \mapsto (\mathbb{L} \mapsto \wp(\mathbb{M})) & \text{forward IF reachability semantics} \\ \mathcal{S}_{\overrightarrow{if}}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{pre}})\ell' & \triangleq & \dot{\neg}\, \mathcal{S}_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\dot{\neg}\, \mathsf{I}_{\mathsf{pre}})\ell' & \\ & = & \neg\{\rho' \in \mathbb{M} \mid \exists \sigma \in \mathbb{S}^*, \ell \in \mathbb{L}, \rho \in \mathbb{M} \backslash \mathsf{I}_{\mathsf{pre}}(\ell).\ \langle \ell,\ \rho \rangle \sigma \langle \ell',\ \rho' \rangle \in [\![\mathrm{P}]\!]^{\mathsf{lt}}\} & \\ & = & \{\rho' \in \mathbb{M} \mid \forall \sigma \in \mathbb{S}^*, \ell \in \mathbb{L}, \rho \in \mathbb{M} \backslash \mathsf{I}_{\mathsf{pre}}(\ell).\ \langle \ell,\ \rho \rangle \sigma \langle \ell',\ \rho' \rangle \notin [\![\mathrm{P}]\!]^{\mathsf{lt}}\} & \end{array}$$

Proof. For any $\mathsf{I}_{\mathsf{pre}}, \mathsf{I}_{\mathsf{post}} \in \mathbb{L} \mapsto \wp(\mathbb{M})$:

$$\begin{array}{lr} \mathcal{S}_{\overleftarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{post}}) \dot{\subseteq} \mathsf{I}_{\mathsf{pre}} & \\ \Leftrightarrow \dot{\neg}\, \mathcal{S}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\dot{\neg}\, \mathsf{I}_{\mathsf{post}}) \dot{\subseteq} \mathsf{I}_{\mathsf{pre}} & \text{〈def. } \mathcal{S}_{\overleftarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{post}})\text{〉} \\ \Leftrightarrow \dot{\neg}\, \mathsf{I}_{\mathsf{pre}} \dot{\subseteq} \mathcal{S}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\dot{\neg}\, \mathsf{I}_{\mathsf{post}}) & \text{〈def. } \dot{\neg} \text{ and } \dot{\subseteq}\text{〉} \\ \Leftrightarrow \mathcal{S}_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\dot{\neg}\, \mathsf{I}_{\mathsf{pre}}) \dot{\subseteq} \dot{\neg}\, \mathsf{I}_{\mathsf{post}} & \text{〈def. } \mathcal{S}_{\overrightarrow{ps}}[\![\mathrm{P}]\!]\text{〉} \\ \Leftrightarrow \mathsf{I}_{\mathsf{post}} \dot{\subseteq} \dot{\neg}\, \mathcal{S}_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\dot{\neg}\, \mathsf{I}_{\mathsf{pre}}) & \text{〈def. } \dot{\neg} \text{ and } \dot{\subseteq}\text{〉} \\ \Leftrightarrow \mathsf{I}_{\mathsf{post}} \dot{\subseteq} \mathcal{S}_{\overrightarrow{if}}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{pre}}) & \text{〈def. } \mathcal{S}_{\overrightarrow{if}}[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{pre}}) \triangleq \dot{\neg}\, \mathcal{S}_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\dot{\neg}\, \mathsf{I}_{\mathsf{pre}})\text{〉} \end{array}$$

□

In the rest of this dissertation, the notation of backward accessibility semantics (or analysis) refers to the backward impossible failure accessibility semantics (or analysis), while the notation of forward reachability semantics (or analysis) refers to the forward possible success reachability semantics (or analysis) by default, unless it is explicitly specified "impossible failure" or "possible success".

Chapter 3

Trace Partitioning

The forward reachability analysis discussed in chapter 2 intends to compute an over-approximation of reachable states of the program, while the information about the execution history and concrete flow paths would be lost in such a process, which makes the correspondingly generated over-approximating reachability semantics in some cases imprecise to determine if a behavior really occurs or not.

In [14, 43], Mauborgne and Rival propose a trace partitioning domain, which allows the partitioning of traces based on the history of memory and control states. Essentially, for any given transition system, they build an extended transition system by augmenting the program points (i.e. control states, labels) with partitioning tokens, which can distinguish traces by the control flow or variable values. This technique has been successfully implemented in the abstract interpretation-based Astrée analyzer [13, 35], significantly improving the precision of analysis and reducing the execution time.

This chapter briefly summarizes the key idea of trace partitioning, proposes to represent elements in the trace partitioning abstract domain as trace partitioning automata,

and extends the existing types of partitioning directive to include program invariants, which facilitates determining responsibility in the abstract (see part III). For more details about the theoretical framework and practical implementation of the trace partitioning domain, we refer to [43].

3.1 The Trace Partitioning Abstract Domain

This section starts with a simple motivating example from [43], and illustrates how the trace partitioning improves the precision of forward reachability analysis.

$$
\begin{array}{ll}
 & \text{int } x, sgn; \\
\ell_0: & \text{if } (x < 0)\{ \\
\ell_1: & \quad sgn := \text{-1}; \\
\ell_2: & \}\text{else } \{ \\
\ell_3: & \quad sgn := 1; \\
\ell_4: & \} \\
\ell_5: & y := x/sgn; \\
\ell_6: & \ldots
\end{array}
$$

Figure 3.1: Motivating Example for Trace Partitioning

In the above program of Fig. 3.1, it is obvious that the value of *sgn* is either 1 or -1 at point ℓ_5, and in particular it cannot be 0 in the concrete. Therefore, dividing by *sgn* at point ℓ_5 is safe, and there is no possible "division by zero" error in the program. However, if we use the interval domain as the abstract environment domain, then by the over-approximating forward reachability analysis introduced in 2.3.2, we would get the reachability semantics (or say, program invariants) $\mathcal{S}^{\sharp}_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^{\sharp}_{\mathsf{pre}})$ listed in the table 3.1, where $\mathsf{I}^{\sharp}_{\mathsf{pre}} \in \mathbb{L} \mapsto \mathcal{D}^{\sharp}_{\mathbb{M}}$ is defined such that $\mathsf{I}^{\sharp}_{\mathsf{pre}}(\ell_0) = \top^{\sharp}_{\mathbb{M}}$ and $\mathsf{I}^{\sharp}_{\mathsf{pre}}(\ell) = \bot^{\sharp}_{\mathbb{M}}$ for

$\ell \neq \ell_0$. Particularly, the value of *sgn* at point ℓ_5 belongs to the interval $[-1; 1]$, which is not precise enough to exclude the possibility of "division by zero" in the program.

ℓ	$\mathcal{S}^{\sharp}_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathrm{I}^{\sharp}_{\mathsf{pre}})\ell$
ℓ_0	$\top^{\sharp}_{\mathbb{M}} = x \in [-\infty; \infty] \wedge sgn \in [-\infty; \infty] \wedge y \in [-\infty; \infty]$
ℓ_1	$x \in [-\infty; -1] \wedge sgn \in [-\infty; \infty] \wedge y \in [-\infty; \infty]$
ℓ_2	$x \in [-\infty; -1] \wedge sgn \in [-1; -1] \wedge y \in [-\infty; \infty]$
ℓ_3	$x \in [0; \infty] \wedge sgn \in [-\infty; \infty] \wedge y \in [-\infty; \infty]$
ℓ_4	$x \in [0; \infty] \wedge sgn \in [1; 1] \wedge y \in [-\infty; \infty]$
ℓ_5	$x \in [-\infty; \infty] \wedge sgn \in [-1; 1] \wedge y \in [-\infty; \infty]$
ℓ_6	$x \in [-\infty; \infty] \wedge sgn \in [-1; 1] \wedge y \in [-\infty; \infty]$

Table 3.1: Abstract Forward Reachability Semantics of the Motivating Example

An intuitive idea to solve the imprecision problem is to relate the value of *sgn* to the way it is computed. In this very example here, if the *true* branch of the conditional was taken, then the value of *sgn* at point ℓ_5 is -1; otherwise, it is 1. That is to say, we partition the set of all possible concrete traces into two parts: in one partition, the *true* branch is taken; in the other partition, the *false* is taken. For each partition, the standard over-approximating forward reachability analysis can be performed, and the analysis results together would be more precise.

To generalize the idea of partitioning, Mauborgne and Rival [14, 43] propose a trace partitioning abstract domain, which is flexible and general to analyze and verify semantic properties in the same way as other classic abstract domains. In the following, we will briefly describe how to construct the trace partitioning abstract domain.

Extended Transition Systems. Suppose T is a set of *partitioning tokens*, which are used to capture useful information about the history of execution and to guide trace partitioning. In practice, each partitioning token $t \in T$ is defined as a stack of *parti-*

tioning directives that have been encountered during the execution, and all the possible partitioning directives are listed in Fig. 3.2, each of which creates a partition as its name implies. For example, in the case of a conditional at point ℓ, by the partitioning directives part$\langle$If, ℓ, t$\rangle$ and part$\langle$If, ℓ, f$\rangle$, two partitions are created right after testing the boolean condition, which respectively correspond to "true branch of the conditional at point ℓ" and "false branch of the conditional at point ℓ" .

d	$::=$	part$\langle$If, ℓ, $b\rangle$	traces in the b branch of the conditional at point ℓ
	$\mid$	part$\langle$While, ℓ, $n\rangle$	traces with exactly n iterations in the loop at point ℓ
	$\mid$	part$\langle$While, ℓ, $> n\rangle$	traces with more than n iterations in the loop at point ℓ
	$\mid$	part$\langle$Val, ℓ, $\chi = n\rangle$	traces such that $\chi = n$ at point ℓ
	$\mid$	part$\langle$Fun, ℓ, $f\rangle$	traces calling function f at point ℓ
	$\mid$	part$\langle$None$\rangle$	void directive
t	$::=$	ϵ	empty stack, initial partition
	$\mid$	$d :: t'$	addition of a partitioning directive on top of t'

Figure 3.2: Partitioning Directives $d \in D$ and Tokens $t \in T$

Given a set of partitioning tokens T, the *extended transition systems* are defined as transition systems over the set of program points (or, control states, labels) extended with the partitioning tokens T. More formally, let $\mathbb{L}_T \triangleq \mathbb{L} \times T$ be the set of *extended program points*, $\mathbb{S}_T \triangleq \mathbb{L}_T \times \mathbb{M}$ be the set of *extended states*, $\mathbb{S}^i_T \subseteq \mathbb{S}_T$ be the set of *extended initial states*, and $\rightarrow_T \in \wp(\mathbb{S}_T \times \mathbb{S}_T)$ be the *transition relation* among extended states. Then, we define an *extended transition system* as a tuple $\langle T, \mathbb{S}^i_T, \rightarrow_T\rangle$. In addition, a *forget function* π_τ can be defined to remove the partitioning tokens from extended program points, extended states and transition relations, such that an extended transition system $\langle T, \mathbb{S}^i_T, \rightarrow_T\rangle$ can be transformed back into a standard transition system $\langle \mathbb{S}^i, \rightarrow\rangle$.

Trace Partitioning Abstract Domain. An extended transition system $\mathrm{P}_T = \langle T,\ \mathbb{S}^i_T,\ \rightarrow_T \rangle$ is a *covering* of the original transition system $\mathrm{P} = \langle \mathbb{S}^i,\ \rightarrow \rangle$, if and only if every initial state $s \in \mathbb{S}^i$ has at least one corresponding initial state $s' \in \mathbb{S}^i_T$ such that $\pi_\tau(s') = s$, and every transition step in P is simulated (mimicked) by at least one transition step in P_T. Therefore, if P_T is a covering of P, then every trace in P is simulated by one or more traces in P_T. For the formal definitions of covering and partition see section 3.2 of [43].

The *trace partitioning abstract domain* $\mathbb{D}^\sharp$ is the set of tuples $\langle \mathrm{P}_T,\ \Phi^\sharp \rangle$, where T is a set of partitioning tokens, $\mathrm{P}_T = \langle T,\ \mathbb{S}^i_T,\ \rightarrow_T \rangle$ is a covering of the original transition system $\mathrm{P} = \langle \mathbb{S}^i,\ \rightarrow \rangle$, and $\Phi^\sharp \in \mathbb{L}_T \mapsto \mathcal{D}^\sharp_{\mathbb{M}}$ is a function mapping each extended program point $\langle \ell,\ t \rangle$ of P_T into an abstract environment element in $\mathcal{D}^\sharp_{\mathbb{M}}$ that approximates the set of environments observed at point $\langle \ell,\ t \rangle$.

Take the program in Fig. 3.1 as an example, if we use partitioning directives designed for the conditional, then the forward reachability analysis with trace partitioning would construct the corresponding $\Phi^\sharp$ function, which is listed in the table 3.2.

$\langle \ell,\ t \rangle$	$\Phi^\sharp(\langle \ell,\ t \rangle)$
$\langle \ell_0,\ \epsilon \rangle$	$x \in [-\infty; \infty] \wedge sgn \in [-\infty; \infty] \wedge y \in [-\infty; \infty]$
$\langle \ell_1,\ \mathrm{part}\langle \mathrm{If},\ \ell_0,\ \mathrm{t} \rangle \rangle$	$x \in [-\infty; -1] \wedge sgn \in [-\infty; \infty] \wedge y \in [-\infty; \infty]$
$\langle \ell_2,\ \mathrm{part}\langle \mathrm{If},\ \ell_0,\ \mathrm{t} \rangle \rangle$	$x \in [-\infty; -1] \wedge sgn \in [-1; -1] \wedge y \in [-\infty; \infty]$
$\langle \ell_3,\ \mathrm{part}\langle \mathrm{If},\ \ell_0,\ \mathrm{f} \rangle \rangle$	$x \in [0; \infty] \wedge sgn \in [-\infty; \infty] \wedge y \in [-\infty; \infty]$
$\langle \ell_4,\ \mathrm{part}\langle \mathrm{If},\ \ell_0,\ \mathrm{f} \rangle \rangle$	$x \in [0; \infty] \wedge sgn \in [1; 1] \wedge y \in [-\infty; \infty]$
$\langle \ell_5,\ \mathrm{part}\langle \mathrm{If},\ \ell_0,\ \mathrm{t} \rangle \rangle$	$x \in [-\infty; -1] \wedge sgn \in [-1; -1] \wedge y \in [-\infty; \infty]$
$\langle \ell_5,\ \mathrm{part}\langle \mathrm{If},\ \ell_0,\ \mathrm{f} \rangle \rangle$	$x \in [0; \infty] \wedge sgn \in [1; 1] \wedge y \in [-\infty; \infty]$
$\langle \ell_6,\ \mathrm{part}\langle \mathrm{If},\ \ell_0,\ \mathrm{t} \rangle \rangle$	$x \in [-\infty; -1] \wedge sgn \in [-1; -1] \wedge y \in [1; \infty]$
$\langle \ell_6,\ \mathrm{part}\langle \mathrm{If},\ \ell_0,\ \mathrm{f} \rangle \rangle$	$x \in [0; \infty] \wedge sgn \in [1; 1] \wedge y \in [0; \infty]$

Table 3.2: Partitioned Forward Reachability Semantics of the Motivating Example

From the above table, we can see that there are two extended program points for ℓ_5:

$\langle \ell_5, \text{part}\langle \text{If}, \ell_0, \text{t}\rangle\rangle$ and $\langle \ell_5, \text{part}\langle \text{If}, \ell_0, \text{f}\rangle\rangle$, and the corresponding abstract environments indicates the value of *sgn* is either -1 or 1, which is exactly the desired result.

However, if we have successive creations of partitions in the extended transition system, the cost would be prohibitive in practice. For instance, the partitioning of a conditional multiplies by 2 the number of partitions in the current flow, thus a series of n conditionals would lead to 2^n partitions, which brings an exponential cost. To solve this issue, we can merge partitions together when they are no longer necessary, which is implemented by popping (or removing) partitioning directives from the token. For example, at point ℓ_6 of the program in Fig. 3.1, the partitions based on "which branch of the conditional was taken" are not expected to lead to improvement in the precision of further analysis, so we can merge those two partitions, and replace the last two rows of table 3.2 by $\Phi^\sharp(\langle \ell_6, \epsilon\rangle) = x \in [\text{-}\infty; \infty] \wedge \mathit{sgn} \in [\text{-}1; 1] \wedge y \in [0; \infty]$, which is still more precise than the standard forward reachability analysis.

3.2 The Trace Partitioning Automata

In order to facilitate determining abstract responsibility on graph structures (in part III), this section proposes to represent the result of forward reachability analysis with trace partitioning as automata, which are called *trace partitioning automata*.

More formally, each element $\langle \text{P}_T = \langle T, \mathbb{S}^i_T, \rightarrow_T\rangle, \Phi^\sharp\rangle$ in the trace partitioning abstract domain $\mathbb{D}^\sharp$ can be represented as an automaton $\mathcal{A} = \langle \mathcal{Q}^i, \delta\rangle$, where:

- The set of initial nodes (extended initial abstract states) $\mathcal{Q}^i = \{\langle \ell^i, t, \text{M}^\sharp\rangle \in \mathbb{L}_T \times \mathcal{D}^\sharp_{\mathbb{M}} \mid \exists \rho \in \mathbb{M}.\ \langle \ell^i, t, \rho\rangle \in \mathbb{S}^i_T \wedge \text{M}^\sharp = \Phi^\sharp(\langle \ell^i, t\rangle)\}$ such that every initial state $\langle \ell^i, t, \rho\rangle$ in P_T is represented by an initial node, which is associated with

an abstract environment element $\mathrm{M}^\sharp = \Phi^\sharp(\langle \ell^i,\ t\rangle)$. By the property of $\Phi^\sharp$ in the trace partitioning abstract domain, it is guaranteed that $\rho \in \gamma_{\mathbb{M}}(\mathrm{M}^\sharp)$.

- The set of edges (extended abstract transition relations) $\delta = \{\langle \ell,\ t,\ \mathrm{M}^\sharp\rangle \to \langle \ell',\ t',\ \mathrm{M}^{\sharp\prime}\rangle \in (\mathbb{L}_T \times \mathcal{D}^\sharp_{\mathbb{M}}) \times (\mathbb{L}_T \times \mathcal{D}^\sharp_{\mathbb{M}}) \mid \exists \rho, \rho' \in \mathbb{M}.\ \langle \ell,\ t,\ \rho\rangle \to_T \langle \ell',\ t',\ \rho'\rangle \ \wedge\ \mathrm{M}^\sharp = \Phi^\sharp(\langle \ell,\ t\rangle) \wedge \mathrm{M}^{\sharp\prime} = \Phi^\sharp(\langle \ell',\ t'\rangle)\}$ such that every concrete transition relation in P_T has a corresponding edge in the automaton.

Again, consider the program in Fig. 3.1, its partitioned forward reachability analysis result from table 3.2 can be represented as a trace partitioning automaton, which is depicted as in Fig. 3.3. For the sake of concision, instead of explicitly drawing partitioning tokens inside the nodes, we comment some edges with "push d" such that every node after the edge has the partitioning directive d pushed into its stack of directives (i.e. its partitioning token). For instance, in Fig. 3.3, all the nodes after the edge commented with "push part$\langle$If, ℓ_0, t$\rangle$" has part$\langle$If, ℓ_0, t$\rangle$ in their partitioning tokens.

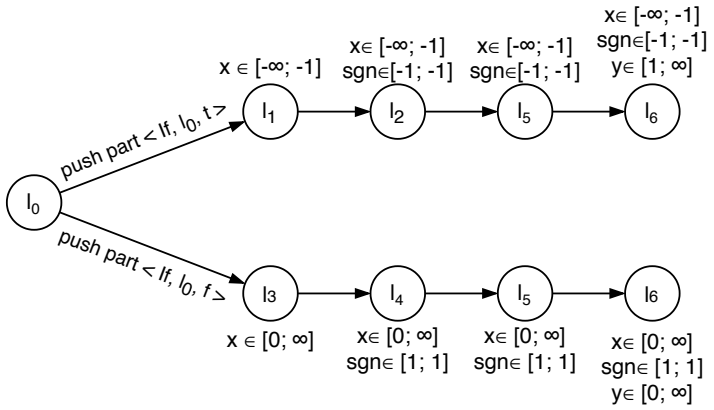

Figure 3.3: Trace Partitioning Automaton for the Motivating Example without Merge

In addition, in order to represent the merge of partitions, we comment some edges with "pop d" such that the partitioning directive d is popped from the stack of directives

of every node after the edge. For instance, Fig. 3.4 depicts the trace partitioning automaton for the program in Fig. 3.1 with partitions merged at point ℓ_6, so the partitioning token in the node ℓ_6 is ϵ (i.e. its stack of partitioning directives is empty).

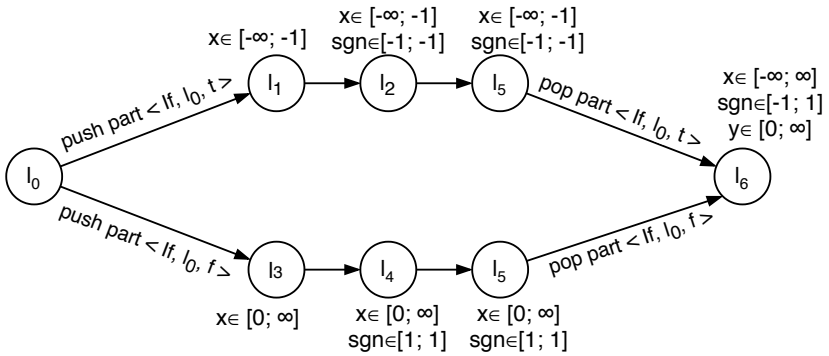

Figure 3.4: Trace Partitioning Automaton for the Motivating Example with Merge

3.3 The Extension of Partitioning Directives

As illustrated in [43], partitioning directives are inserted in the source code as special comments in a preprocessing phase. Specifically, among the six types of partitioning directives described in Fig. 3.2, five of them partition traces based on the control flow, and only part$\langle$Val, ℓ, $x = n\rangle$ introduces a partition guided by the value of a variable x at some point ℓ. Although these partitioning directives have successfully handled a broad range of cases, there are still many cases that cannot be well coped with, and we would like to introduce a new partitioning directive to partition traces by environment properties (which are represented by abstract environment elements).

For example, in order to improve the precision of forward reachability analysis for the access control program in Fig. 1.4, it is intuitive to partition traces by some environ-

ment properties that can be easily expressed by abstract environment elements in $\mathcal{D}^\sharp_{\mathbb{M}}$ (i.e. *i1* $\in [-\infty, 0]$ and *i1* $\in [1; \infty]$ at point ℓ_3; *apv* $\in [1, \infty] \wedge$ *i2* $\in [-\infty, 0]$, *apv* $\in [-\infty, 0]$ and *i2* $\in [1, \infty]$ at point ℓ_5), and such properties (e.g. *apv* $\in [1, \infty] \wedge$ *i2* $\in [-\infty, 0]$) may not be expressed by directives of form part$\langle$Val, ℓ, $x = n\rangle$ when more than one variables are used in partitioning. Of course, the access control program can be equivalently transformed into a program with conditionals (by replacing ternary operators with conditionals), then the problem of partitioning guided by environment properties is transformed to partitioning based on the branch of conditionals. However, this is not always the case. For example, consider a simple program "$\ell_1 : z := x - y;\ \ell_2 :$", suppose we are interested in whether the value of z is positive or negative at point ℓ_2, then it is of value to create partitions guided by $x \geq y$ and $x < y$ at point ℓ_1. Such partitions can be expressed by abstract environment elements in the polyhedra/octagons domain, but not by the existing partitioning directives.

Therefore, here we propose a new partitioning directive of the form: part$\langle$Inv, ℓ, $\mathrm{M}^\sharp\rangle$ (where $\mathrm{M}^\sharp$ is an abstract environment element in $\mathcal{D}^\sharp_{\mathbb{M}}$), which generates a new partition of traces such that $\mathrm{M}^\sharp$ is satisfied at point ℓ. In practice, the trace partitioning introduced by a directive part$\langle$Inv, ℓ, $\mathrm{M}^\sharp\rangle$ can be simply implemented by creating a new node, such that its partitioning token (i.e. the stack of partitioning directives) has this directive on the top, and the corresponding abstract environment element is the meet of $\mathrm{M}^\sharp$ and the standard forward reachability semantics $\mathcal{S}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{pre}})\ell$ at point ℓ.

Example 10 (Access Control, Continued) *In example 6, we have discussed the standard abstract forward reachability semantics of the access control program, in which the abstract environment domain $\mathcal{D}^\sharp_{\mathbb{M}}$ is the interval domain. Now we can gain more precision by introducing*

five partitioning directives: $\mathrm{d}_3 : \mathit{part}\langle \mathit{Inv},\ \ell_3,\ \mathit{i1} \in [\text{-}\infty, 0]\rangle$, $\mathrm{d}'_3 : \mathit{part}\langle \mathit{Inv},\ \ell_3,\ \mathit{i1} \in [1, \infty]\rangle$, $\mathrm{d}_5 : \mathit{part}\langle \mathit{Inv},\ \ell_5,\ \mathit{apv} \in [1, \infty] \wedge \mathit{i2} \in [\text{-}\infty, 0]\rangle$, $\mathrm{d}'_5 : \mathit{part}\langle \mathit{Inv},\ \ell_5,\ \mathit{apv} \in [\infty, 0]\rangle$ *and* $\mathrm{d}''_5 : \mathit{part}\langle \mathit{Inv},\ \ell_5,\ \mathit{i2} \in [1, \infty]\rangle$*, and the corresponding partitioned forward reachability semantics is listed in table 3.3. For the sake of conciseness, trivial elements like "*$\mathit{acs} \in [\text{-}\infty; \infty]$*" are omitted, and the forward reachability analysis stops at invalid extended program points that are associated with* $\bot^\sharp_{\mathbb{M}}$.

$\langle \ell,\ t\rangle$	$\Phi^\sharp(\langle \ell,\ t\rangle)$
$\langle \ell_1,\ \epsilon\rangle$	$\top^\sharp_{\mathbb{M}}$
$\langle \ell_2,\ \epsilon\rangle$	$\mathit{apv} \in [1; 1]$
$\langle \ell_3,\ d_3\rangle$	$\mathit{apv} \in [1; 1] \wedge \mathit{i1} \in [\text{-}1; 0]$
$\langle \ell_3,\ d'_3\rangle$	$\mathit{apv} \in [1; 1] \wedge \mathit{i1} \in [1; 2]$
$\langle \ell_4,\ d_3\rangle$	$\mathit{apv} \in [\text{-}1; \text{-}1] \wedge \mathit{i1} \in [\text{-}1; 0]$
$\langle \ell_4,\ d'_3\rangle$	$\mathit{apv} \in [1; 1] \wedge \mathit{i1} \in [1; 2]$
$\langle \ell_5,\ d_5 :: d_3\rangle$	$\bot^\sharp_{\mathbb{M}}$
$\langle \ell_5,\ d'_5 :: d_3\rangle$	$\mathit{apv} \in [\text{-}1; \text{-}1] \wedge \mathit{i1} \in [\text{-}1; 0] \wedge \mathit{i2} \in [\text{-}1; 2]$
$\langle \ell_5,\ d''_5 :: d_3\rangle$	$\mathit{apv} \in [\text{-}1; \text{-}1] \wedge \mathit{i1} \in [\text{-}1; 0] \wedge \mathit{i2} \in [1; 2]$
$\langle \ell_5,\ d_5 :: d'_3\rangle$	$\mathit{apv} \in [1; 1] \wedge \mathit{i1} \in [1; 2] \wedge \mathit{i2} \in [\text{-}1; 0]$
$\langle \ell_5,\ d'_5 :: d'_3\rangle$	$\bot^\sharp_{\mathbb{M}}$
$\langle \ell_5,\ d''_5 :: d'_3\rangle$	$\mathit{apv} \in [1; 1] \wedge \mathit{i1} \in [1; 2] \wedge \mathit{i2} \in [1; 2]$
$\langle \ell_6,\ d'_5 :: d_3\rangle$	$\mathit{apv} \in [\text{-}1; \text{-}1] \wedge \mathit{i1} \in [\text{-}1; 0] \wedge \mathit{i2} \in [\text{-}1; 2]$
$\langle \ell_6,\ d''_5 :: d_3\rangle$	$\mathit{apv} \in [\text{-}1; \text{-}1] \wedge \mathit{i1} \in [\text{-}1; 0] \wedge \mathit{i2} \in [1; 2]$
$\langle \ell_6,\ d_5 :: d'_3\rangle$	$\mathit{apv} \in [\text{-}1; \text{-}1] \wedge \mathit{i1} \in [1; 2] \wedge \mathit{i2} \in [\text{-}1; 0]$
$\langle \ell_6,\ d''_5 :: d'_3\rangle$	$\mathit{apv} \in [1; 1] \wedge \mathit{i1} \in [1; 2] \wedge \mathit{i2} \in [1; 2]$
$\langle \ell_7,\ d'_5 :: d_3\rangle$	$\mathit{apv} \in [\text{-}1; \text{-}1] \wedge \mathit{i1} \in [\text{-}1; 0] \wedge \mathit{i2} \in [\text{-}1; 2] \wedge \mathit{typ} \in [1; 2]$
$\langle \ell_7,\ d''_5 :: d_3\rangle$	$\mathit{apv} \in [\text{-}1; \text{-}1] \wedge \mathit{i1} \in [\text{-}1; 0] \wedge \mathit{i2} \in [1; 2] \wedge \mathit{typ} \in [1; 2]$
$\langle \ell_7,\ d_5 :: d'_3\rangle$	$\mathit{apv} \in [\text{-}1; \text{-}1] \wedge \mathit{i1} \in [1; 2] \wedge \mathit{i2} \in [\text{-}1; 0] \wedge \mathit{typ} \in [1; 2]$
$\langle \ell_7,\ d''_5 :: d'_3\rangle$	$\mathit{apv} \in [1; 1] \wedge \mathit{i1} \in [1; 2] \wedge \mathit{i2} \in [1; 2] \wedge \mathit{typ} \in [1; 2]$
$\langle \ell_8,\ d'_5 :: d_3\rangle$	$\mathit{apv} \in [\text{-}1; \text{-}1] \wedge \mathit{i1} \in [\text{-}1; 0] \wedge \mathit{i2} \in [\text{-}1; 2] \wedge \mathit{typ} \in [1; 2] \wedge \mathit{acs} \in [\text{-}2; \text{-}1]$
$\langle \ell_8,\ d''_5 :: d_3\rangle$	$\mathit{apv} \in [\text{-}1; \text{-}1] \wedge \mathit{i1} \in [\text{-}1; 0] \wedge \mathit{i2} \in [1; 2] \wedge \mathit{typ} \in [1; 2] \wedge \mathit{acs} \in [\text{-}2; \text{-}1]$
$\langle \ell_8,\ d_5 :: d'_3\rangle$	$\mathit{apv} \in [\text{-}1; \text{-}1] \wedge \mathit{i1} \in [1; 2] \wedge \mathit{i2} \in [\text{-}1; 0] \wedge \mathit{typ} \in [1; 2] \wedge \mathit{acs} \in [\text{-}2; \text{-}1]$
$\langle \ell_8,\ d''_5 :: d'_3\rangle$	$\mathit{apv} \in [1; 1] \wedge \mathit{i1} \in [1; 2] \wedge \mathit{i2} \in [1; 2] \wedge \mathit{typ} \in [1; 2] \wedge \mathit{acs} \in [1; 2]$

Table 3.3: Partitioned Forward Reachability Semantics for the Access Control Program

Compared with the standard forward reachability semantics $\mathcal{S}^{\sharp}_{\overrightarrow{p\hat{s}}}[\![\mathrm{P}]\!](\mathsf{I}^{\sharp}_{\mathsf{pre}})\ell$ *in example 6, the partitioned forward reachability semantics is much more precise, revealing the relation between* acs *and other variables, which is of significance in determining responsibility later.*

Furthermore, the partitioned forward reachability semantics can be represented by a trace partitioning automaton in Fig. 3.5. It is worthy to mention that, as what we have done in Fig. 3.4, the partitions can be merged after the access check to acs *finishes at point* ℓ_8*, such that all the partitioning directives pushed at point* ℓ_3 *or* ℓ_5 *can be popped from the partitioning tokens at point* ℓ_8*.*

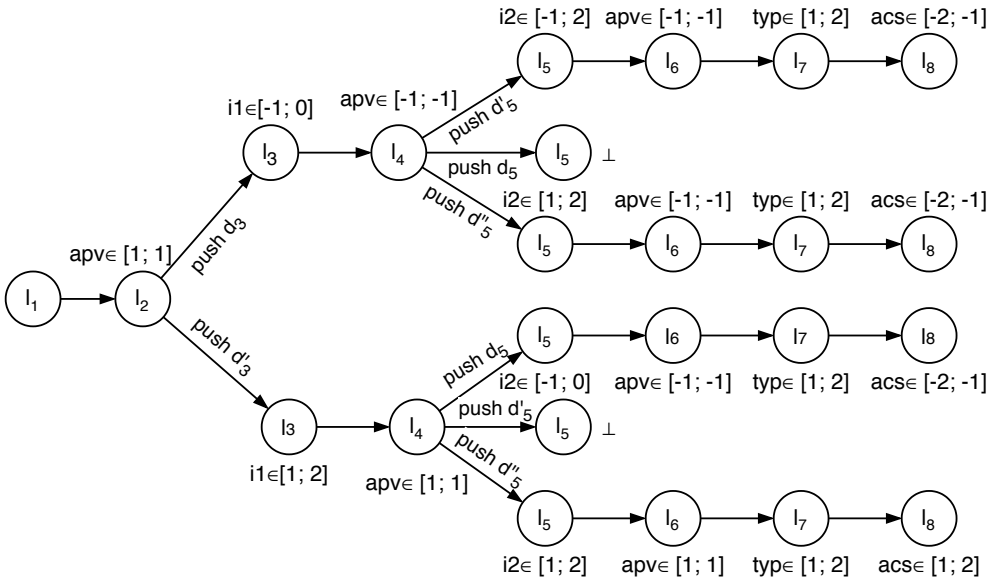

Figure 3.5: Trace Partitioning Automaton for the Access Control Program

□

Part II

Concrete Responsibility Analysis

PART II. CONCRETE RESPONSIBILITY ANALYSIS

The problem of responsibility analysis is pervasive in various scientific fields. For any behavior of interest, no matter it is a forest fire in the realistic life or an error in program executions, the corresponding responsibility analysis aims at identifying entities that have the primary control over that behavior, which are called *responsible entities*.

This dissertation focuses on detecting responsible entities, while the possible way of exploiting the detected responsible entities varies on a case-by-case basis, and is beyond the scope of this dissertation. For instance, in the scenario of a forest fire, if an action of dropping a lit match in the forest is found responsible for the fire, then we could make use of such information by bringing the arsonist who conducted this action to a trial; yet, if a lightening is found responsible for the forest fire, then no further operation is necessary in this case. Similarly, when we complete the responsibility analysis of certain behaviors in the program, the procedure afterwards can only be decided manually depending on specific cases, and typically it is time for the user to configure the permissions granted to the responsible entity at her/his discretion. More specifically, if the behavior of interest is always desired (e.g. program non-termination, passing a safety check) or the responsible entity is authorized to take control over the behavior of interest, then the permissions granted to the responsible entity can be kept or even expanded; on the contrary, if the behavior of interest is always undesired (e.g. a division-by-zero error, a buffer overflow error) or it is against the policy for the responsible entity to control the behavior of interest, the permissions granted to the responsible entity shall be restricted.

In this part, the objective is to give a formal definition of responsibility in the concrete, which is originally proposed in [24, 33] and generic to cope with miscellaneous scenarios. To start with, chapter 4 introduces a simple but thought-provoking exam-

ple of forest fire, which characterizes the difference of responsibility with dependency, causality and other techniques in detecting causes. Inspired by this forest fire example, we suggest an informal definition of responsibility, which is quite intuitive and applicable to analyzing various program behaviors. Moreover, chapter 5 designs a framework of concrete responsibility analysis, formalizes the definition of responsibility as an abstraction of the program trace semantics, and takes the access failure behavior in the access control program from part I as an example to illustrate the process of concrete responsibility analysis. Chapter 6 gives several examples of the application of responsibility analysis, which include negative balance / buffer overflow, division by zero / login attack, and information leakage.

Chapter 4

The Characteristics of Responsibility

In order to give an informal introduction to responsibility, as well as its main distinctions with dependency, causality and other techniques in detecting causes, this chapter starts with a classic example of forest fire used in the definition of actual cause [47, 48], and further characterizes three indispensable elements in defining responsibility.

4.1 Discussion of the Forest Fire Example

Example 11 (Forest Fire) *Consider the example of forest fire taken from [47, 48]. Suppose that two arsonists drop lit matches in different parts of a dry forest, and both cause trees to start burning. Here it is assumed that one arsonist named A drops the lit match before the other arsonist B, and there are two scenarios. In the first scenario, called the disjunctive scenario, either match by itself suffices to burn down the whole forest. That is to say, even if only one match were lit, the forest would burn down. In the second scenario, called the conjunctive scenario, two lit matches are necessary to burn down the whole forest; if only one match were*

lit, some trees would be burnt, but the fire dies down before the whole forest is destroyed. □

It is quite natural to bring up this question: who shall be responsible for burning down the whole forest? The literature has several possible answers. A simple but popular solution is to use the *dependency analysis* that determines how entities (e.g. values of variables) depend upon other entities. Suppose we use variables to represent all the entities in the forest fire example (e.g. the decisions of two arsonist, the status of matches, the fire condition of the forest, the weather), then the real life example of forest fire can be viewed as an equivalent computer program. By the definition of dependency [19, 51, 39, 15, 23], in both scenarios the forest fire depends on each of those two arsonists, as well as many other non-decisive factors, such as the wind which influences the spreading speed of forest fire. Such a result is correct in some sense, but far from precise. The reason is that, although the wind does affect the forest fire, it is not decisive (i.e. the wind could not either enforce or prevent the fire), and it is against the intuition to mix arsonists with the wind as the responsible entity of a forest fire. Thus, the responsibility analysis shall have the ability to distinguish decisive factors from non-decisive factors.

A "naive" definition of *causality* [53, 54] based on counterfactual dependency could exclude non-decisive factors (e.g. the wind in this example) from the analysis result. This definition proposed by Lewis adopts an alternative world semantics and determines causality relations according to a criterion: an event e is a cause of the occurrence of another event e' if and only if, were e not to occur, e' would not happen. The testing of this condition hinges upon the availability of alternative worlds. For instance, in the conjunctive scenario of this forest fire example, we can infer that the forest would not be burnt down in an alternative world where the arsonist A does not drop a lit match, thus

the arsonist A is causal for the forest fire; yet, in the alternative world where there is no wind, the forest would still be burnt down, hence the wind is not a cause of the forest fire. However, the counterfactual causality may be too strict in some circumstances such that no cause could be found. Take the disjunctive scenario of forest fire as an example, in the alternative world where one arsonist A (respectively, B) does not drop a lit match, the forest would still have been burnt down due to the other arsonist B (respectively, A), hence neither of these two arsonists would be determined as the cause of forest fire. Thus, it may be inappropriate to directly adopt the idea of counterfactual dependency in the responsibility analysis.

The *actual cause* proposed by Halpern and Pearl [47, 48, 57] is based on the structural equations model (SEM) [60], and extends Lewis's notion of counterfactual dependency to allow "contingent dependency". More precisely, events are represented by variable values in the SEM, and contingencies can be viewed as possible alternative worlds where a variable value is changed. An event e is an actual cause of another event e', if there exists a contingency (where the values for other variables may be changed) such that e' counterfactually depends on e. Take the disjunctive scenario of forest fire as an example, the arsonist A is determined as an actual cause of the forest fire, since the forest fire counterfactually depends on A's action of dropping a lit match under the contingency (i.e. in an alternative world) where the other arsonist B does not drop a lit match; similarly, the arsonist B is also an actual cause of the forest fire, since the forest fire counterfactually depends on B under the contingency where A does not drop a lit match. Such a structural model method has allowed for a great progress in causality analysis, solving many problems of previous approaches. In addition, it has been extended to reason about com-

putational models and applied to bounded model checking [20, 29, 27]. However, as an abstraction of the concrete semantics, the structural equations model would unnecessarily miss some information that are indispensable in determinating responsible entities accurately, including the following three important points.

(P1) *Time (or say, the temporal ordering of events/actions) should be taken into account*. For instance, in the forest fire example, the structural equations model approach cannot tell the difference whether A or B drops a lit match first, hence determines both arsonists as the cause of forest fire. Such a result may not seem to be absurd, but imagine the case that the forest has already been burnt down by the match dropped by A before B lit her/his match in the disjunctive scenario. In such a case, it is against intuition to put B as a cause of the forest fire. To deal with this problem, Halpern and Pearl's solution is to modify the structural equations model and introduce some new variable [17] to distinguish whether the forest was actually destroyed by A or B, which is difficult to accomplish in practice for programs. In contrast, a much simpler method is to keep the temporal sequence of events/actions, such that only the first action that guarantees the behavior of interest is counted as the responsible entity. For instance, in the disjunctive scenario of forest fire, the action of dropping a lit match by A ensures burning down the whole forest even before B makes his choice, thus only A is responsible for the forest fire.

(P2) *The responsible entity must be free to make choices*. In the forest fire example, suppose that the match is taken as a separate entity, and its value (i.e. lit or not-lit) solely depends on the corresponding arsonist. In the structural equations model of actual cause, both the arsonist and the match are represented by endogenous variables

and further determined as actual causes of burning down the forest. However, it is common sense that the match itself does not have a choice to light or not, and it is inappropriate to identify matches as responsible entities for the forest fire. Hence, only the action that can make choices at its own discretion can possibly be responsible for a behavior. Specifically, in computer programs, such actions include but are not limited to user inputs, system settings, files read, parameters of procedures or modules, returned values of external functions, variable initialization, random number generations and the parallelism. To be more accurate, it is the external subject (who does the input, configures the system settings, etc.) that is free to make choices, but we say that actions like user inputs are free to make choices, as an abuse of language.

(P3) *It is necessary to explicitly specify "to whose cognizance" when analyzing the responsibility*. All the above reasoning on causality is implicitly based on the cognizance/knowledge of an omniscient observer who knows everything about the whole system, yet it is non-trivial to consider the cognizance of a non-omniscient observer. For instance, consider the forest fire example again, and here we can adopt the cognizance of the second arsonist B. In the disjunctive scenario, if B is aware that A has already dropped a lit match in the forest, then B is not responsible for the forest fire to his/her cognizance, since B knows that the forest is guaranteed to burn down no matter whether she/he drops a lit match or not; otherwise, if B does not know a lit match has been dropped in the forest, then B is responsible for the forest fire to her/his cognizance, although she/he is not responsible to the cognizance of an omniscient observer. Similarly, in the conjunctive scenario, if B is aware that A has

already dropped a lit match in the forest, then B understands that it is her/his own action that ensures burning down the whole forest, hence she/he shall take the responsibility to her/his cognizance; otherwise, if B does not know that a lit match has been dropped, then she/he does not expect the whole forest to be burnt down, hence to her/his own cognizance B is only responsible for burning some trees, but not the whole forest. It is worthy noting that, in most cases, the cognizance of an omniscient observer will be adopted, but not always.

4.2 An Informal Definition of Responsibility

In the last section, with the assistance of an intuitive example of forest fire, we have characterized three essential points in responsibility analysis: temporal ordering, free choices and the cognizance. In the rest of this dissertation, we focus on analyzing the responsibility in computer programs, and an informal definition of *responsibility* is presented as follows, which takes the above three points into account and allows for building an expressive framework of responsibility analysis.

Definition 1 (Responsibility, informally) *To the cognizance of an observer, an action a_{R} is responsible for the behavior $\mathcal{B}$ of interest in a given execution, if and only if, according to the observer's observation, a_{R} is free to make choices, and such a choice is the first one that guarantees the occurrence of $\mathcal{B}$ in that execution.*

It is necessary to point out that, for the whole system whose concrete semantics is a set of executions, there may exist more than one action that is responsible for $\mathcal{B}$. Nevertheless, in every single execution where $\mathcal{B}$ occurs, there is only one action that is

responsible for $\mathcal{B}$. To decide which action in an execution is responsible, the execution alone is not sufficient, and it is required to reason on the whole semantics to exhibit the action's "free choices" and guarantee of $\mathcal{B}$. Thus, responsibility is not a trace property (neither safety nor liveness property), but a hyper-property [11], which is a property of sets of execution traces.

In the following, we consider the access control program example in Fig. 1.4 again, and discuss the advantage of the responsibility analysis over the classic dependency / causality analysis in an informal way, while the responsibility analysis procedure of this access control program will be formalized in chapter 5.

Example 12 (Access Control, Continued) *For the access control program in Fig. 1.4, the question that we are interested in is: when the access to o fails in the program execution (referred as "Access Failure", i.e. acs* ≤ 0 *at point* ℓ_8*), which action (actions) shall be responsible?*

First, we consider the dependency analysis and corresponding slicing techniques. No matter whether we adopt the syntactic dependency or semantic dependency, it is not hard to see that the value of acs at point ℓ_8 *depends on the value of apv and typ at point* ℓ_7*, which further depend on the inputs from the two admins and system settings. That is to say, the behavior "access failure" depends on all variables in the program, thus program slicing techniques (both syntactic slicing [45] and semantic slicing [25]) would take the whole program as the slice related with access failure. Although the slicing technique intends to rule out parts of the program that are completely irrelevant with the behavior of interest, it is too imprecise to be practically useful in this example. For instance, the computed slice include the actions such as* $apv := 1$*,* $apv := (i1 \leq 0)\ ?\ \text{-}1 : apv$ *and* $acs := apv \times typ$*, which have no free choices: they are completely deterministic and act merely as the intermediary between causes*

and effects, thus shall not be treated as responsible entities. Moreover, similar to the wind in the forest fire example, the action typ $:= [1; 2]$ *representing the input from system settings is a non-decisive factor for the access failure behavior (i.e. no matter whether typ is 1 or 2, it cannot either enforce or prevent the access failure), although it does affect the value of acs at point* ℓ_8*. Therefore, the dependency analysis and slicing are not precise enough to identify responsible entities.*

Second, using the counterfactual causality proposed by Lewis, we can exclude non-decisive factors (i.e. the action typ $:= [1; 2]$ *in this example), but it fails to find any cause of the access failure behavior in the executions where the inputs from both two admins are negative or zero. For example, in the execution where i1* $= 0$ *and i2* $= 0$*, neither of these two admin inputs would be determined as the cause of access failure, because the behavior of access failure does not counterfactually depend on either of them. More precisely, if the input from one admin (either i1 or i2) is changed to a strictly positive value (i.e. 1 or 2), the access failure would still occur due to the input* 0 *from the other admin.*

Third, we consider the definition of actual cause proposed by Halpern and Pearl, and represent the access control program by a structural equations model (SEM): three non-deterministic inputs from admins and system settings (i.e. $[-1; 2]$ *and* $[1; 2]$*) are represented by exogenous variables, and each program variable is presented by an endogenous variable, whose value is deterministically decided by the values of other (exogenous or endogenous) variables. Similar to the counterfactual causality by Lewis, non-decisive factors (i.e. the assignment to typ) would not be counted as actual causes. Yet, the actual cause allows reasoning counterfactual dependency under a contingency, such that it can identify causes in the executions where the inputs from both admins are negative or zero. For example, in the execution where the*

inputs from two admins are 0, both $i1 = 0$ *and* $i2 = 0$ *are determined as actual causes of access failure, because the access failure counterfactually depends on* $i1 = 0$ *(respectively,* $i2 = 0$*) under the contingency where the value of i2 (respectively, i1) is changed to* 1 *or* 2*. Besides, similar to the dependency analysis, the intermediate events between causes and effects (e.g.* $apv = -1$ *and* $acs = -1$*) are also determined as actual causes of access failure.*

Lastly, compared with the above dependency/causality analysis, the responsibility analysis according to the Definition 1 would be much more precise, and it can accurately identify the responsible entities of access failure in various cases. Here we list the entire desired responsibility analysis results, while the detailed procedure of producing such results is formalized in the next chapter. (1) To the cognizance of an omniscient observer: for any execution, if the input from the 1st admin is negative or zero, then no matter what the other two inputs are, only the action $i1 := [-1; 2]$ *(which represents the input from the 1st admin) is responsible for the access failure behavior, because it guarantees the access failure even before the 2nd admin inputs her/his decision; if the input from the 1st admin is positive and the input from the 2nd admin is negative or zero, then only the action* $i2 := [-1; 2]$ *(which represents the input from the 2nd admin) is responsible for the access failure behavior, because the positive input from the 1st admin does not either enforce or prevent the access failure, while the negative or zero input from the 2nd admin is the first action that guarantees the access failure; otherwise, if the inputs from both admins are positive, then the access failure behavior does not occur, thus there is no responsible entity. (2) To the cognizance of a non-omniscient observer who does not know the input from the 1st admin: for any execution, if the input from the 2nd admin is negative or zero, then no matter what the input from the 1st admin is, only the action* $i2 := [-1; 2]$ *(which represents the input from the 2nd admin) is responsible for the access failure behavior, because*

from the knowledge of the non-omniscient observer, the access failure behavior is ensured only after the 2nd admin inputs a negative value or zero; otherwise, if the input from the 2nd admin is positive, then whether the access failure occurs or not is uncertain from the perspective of non-omniscient observer, thus no entity is responsible for the access failure.

After finishing the responsibility analysis, it is time for the user to configure permissions granted to each responsible entity at her/his discretion. In this example, suppose the cognizance of an omniscient observer is adopted, then we find that only the inputs from two admins are possibly responsible for the access failure behavior. If the two admins are authorized to control the access, their permissions to input negative values or zero can be kept; otherwise, if those two admins have no authorization to decline the access to o, then their permissions to input negative values or zero shall be removed. □

Chapter 5

Formal Definition of Responsibility

In order to put the informal definition of responsibility (Definition 1) into effect, here we design a framework of concrete responsibility analysis as illustrated in Fig.5.1, which essentially consists of three components: (1) *Program semantics*, i.e. the set of all possible executions, each of which can be analyzed individually. (2) *A lattice of system behaviors of interest*, which is ordered such that the stronger a behavior is, the lower is its position in the lattice. (3) *An observation function for each observer*, which maps every (probably unfinished) execution to a behavior in the lattice that is guaranteed to occur, even though such a behavior may not have occurred yet. These three components are formally defined in this chapter, and their abstractions are presented in part III.

In this framework of concrete analysis, if an observer's observation finds that the guaranteed behavior grows stronger after extending an execution by an action, then the extended part of execution (i.e. the action) must be responsible for ensuring the occurrence of the stronger behavior. Consider the example in Fig. 5.1 that sketches the analysis for a certain execution of the access control program, where the inputs from

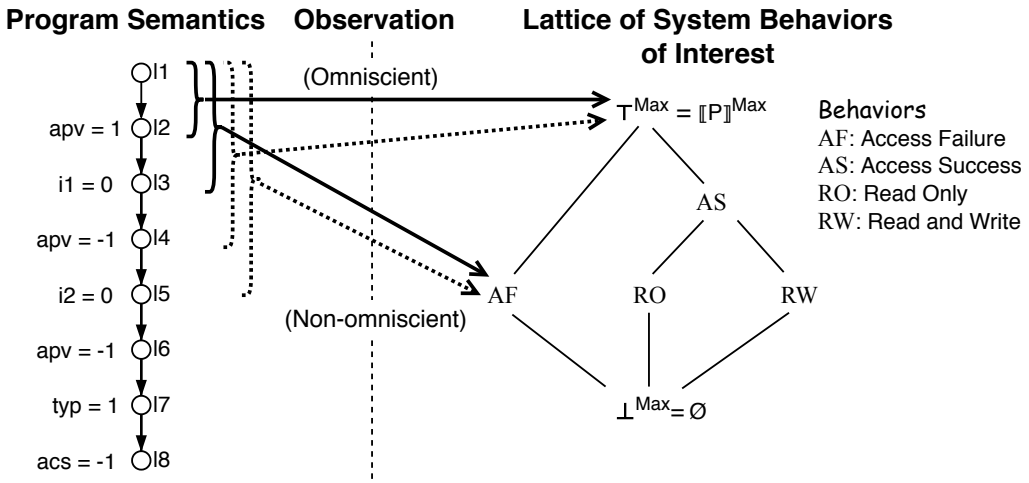

Figure 5.1: Framework of Concrete Responsibility Analysis for Access Control Example

both admins are zeros while the input from system settings is one. Suppose in the lattice of system behaviors, the top $\top^{\mathsf{Max}}$ represents the behavior "not sure if the access to o fails or not", AF represents the behavior of access failure, and AS represents the behavior of access success, whose formal definitions are given in section 5.2. The solid arrow from executions to the lattice stands for the observation of an omniscient observer who knows everything, while the dashed arrow stands for the observation of a non-omniscient observer who is unaware of the input from 1st admin.

As illustrated in Fig. 5.1, the omniscient observer finds that the execution from point ℓ_1 to point ℓ_2 can guarantee only $\top^{\mathsf{Max}}$ (i.e. before the 1st admin inputs her/his decision, whether the access to o fails or succeeds is undecided), while the stronger behavior AF is guaranteed when the execution reaches point ℓ_3 (i.e. after the 1st admin inputs zero, it is ensured that the access to o will fail, even though it has not occurred yet). Thus, to the cognizance of the omniscient observer, the action between point ℓ_2 and ℓ_3 (i.e. $i1 := [-1; 2]$ representing the input from 1st admin) is responsible for the access failure

behavior. In contrast, the non-omniscient observer finds that all the executions upto point ℓ_4 guarantee $\top^{\mathsf{Max}}$ (i.e. the non-omniscient observer does not know the 1st admin already inputs 0, thus believes that the access failure behavior is not guaranteed yet), and AF is guaranteed only after point ℓ_5 is reached (i.e. only after the 2nd admin inputs zero, the non-omniscient observer knows that the access failure is ensured to occur). Hence, to the cognizance of the non-omniscient observer, the action between point ℓ_4 and point ℓ_5 (i.e. $i2 := [\text{-}1; 2]$ representing the input from 2nd admin) is responsible for the access failure. It is easy to see that such analysis results are consistent with Example 12.

More formally, this chapter presents the program trace semantics, builds a lattice of system behaviors by trace properties, proposes an observation function that derives from the observer's cognizance and an inquiry function on system behaviors. Furthermore, this section formally defines responsibility as an abstraction of program semantics, using the observation function. To strengthen the intuition of responsibility analysis, the analysis of the access control program example will be illustrated step by step.

5.1 Program Semantics

Generally speaking, no matter what type of program we are concerned with and no matter which programming language is used to implement that program, the corresponding program semantics can be represented as a set of execution traces.

As introduced in chapter 1, every program can be modeled as a transition system of the form $\mathrm{P} = \langle \mathbb{S}^i, \rightarrow \rangle$, and its execution traces are represented as finite or infinite sequences of states. Furthermore, the intermediate trace semantics $[\![\mathrm{P}]\!]^{\mathsf{It}}$ is defined as the set of traces such that every two successive states are related by $\rightarrow$; the prefix trace

semantics $[\![\mathrm{P}]\!]^{\mathsf{Pref}}$ is defined as the set of intermediate traces that start from initial states; and the maximal trace semantics $[\![\mathrm{P}]\!]^{\mathsf{Max}}$ is the set of prefix traces that either terminate at final states or the error state ω, or do not ever terminate. A trace σ is said to be *valid* for a program P, if and only if $\sigma \in [\![\mathrm{P}]\!]^{\mathsf{Pref}}$. Obviously, the intermediate/prefix/maximal trace semantics do preserve the temporal ordering of actions, which is missed by the structural equations model (SEM) used by actual causes [47, 48, 57].

Specifically, for the access control program example in Fig. 1.4, its definition of maximal trace semantics refers to Example 2. For the sake of simplicity, it is assumed that the initial environment is fixed (e.g. the value of each variable is assumed to be 0 at the initial point ℓ_1), hence its maximal trace semantics $[\![\mathrm{P}]\!]^{\mathsf{Max}}$ consists of 32 traces that correspond to different input values from two admins and the system settings.

5.2 Lattice of System Behaviors of Interest

5.2.1 Trace Property

A *trace property* is a set of traces. For any given system, many behaviors can be represented as a maximal trace property $\mathcal{T} \in \wp([\![\mathrm{P}]\!]^{\mathsf{Max}})$.

Example 13 (Access Control, Continued) *For the access control program example in Fig. 1.4, the behavior "Access Success" AS (i.e. the access to o succeeds) is represented by a set of maximal traces such that the value of acs is strictly positive at point ℓ_8, i.e. $AS = \{\sigma \in [\![\mathrm{P}]\!]^{\mathsf{Max}} \mid \exists \rho \in \mathbb{M}.\ \sigma_{[7]} = \langle \ell_8,\ \rho \rangle \wedge \rho(acs) > 0\}$. More precisely, along every trace in AS, each input from the 2 admins or the system settings is either 1 or 2. Since the initial environment is assumed to be fixed, AS consists of 8 different traces.*

The behavior "Access Failure" AF (i.e. the access to o fails) is represented as a set of maximal traces such that the value of acs is less than or equal to zero at point ℓ_8, which is the complement of AS, i.e. $AF = [\![\mathrm{P}]\!]^{\mathsf{Max}} \backslash AS = \{\sigma \in [\![\mathrm{P}]\!]^{\mathsf{Max}} \mid \exists \rho \in \mathbb{M}.\ \sigma_{[7]} = \langle \ell_8,\ \rho \rangle \wedge \rho(\mathit{acs}) <= 0\}$. *It is not hard to see that, along every trace in AF, at least one input from the two admin is* -1 *or* 0*, while the input from system settings is* 1 *or* 2*. Hence, AF consists of 24 different traces.*

Furthermore, the behavior AS can be split into two parts: $RO = \{\sigma \in [\![\mathrm{P}]\!]^{\mathsf{Max}} \mid \exists \rho \in \mathbb{M}.\ \sigma_{[7]} = \langle \ell_8,\ \rho \rangle \wedge \rho(\mathit{acs}) = 1\}$ *represents a stronger behavior "Read Only access is granted", which consists of 4 traces; and* $RW = \{\sigma \in [\![\mathrm{P}]\!]^{\mathsf{Max}} \mid \exists \rho \in \mathbb{M}.\ \sigma_{[7]} = \langle \ell_8,\ \rho \rangle \wedge \rho(\mathit{acs}) = 2\}$ *represents another behavior "Read and Write access is granted", which also consists of 4 traces.*

□

5.2.2 Lattice of System Behaviors of Interest

Here we build a complete lattice of maximal trace properties, each of which represents a behavior of interest. Typically, such a lattice is of the form $\langle \mathcal{L}^{\mathsf{Max}}, \subseteq, \top^{\mathsf{Max}}, \bot^{\mathsf{Max}}, \cup, \cap \rangle$, where

- $\mathcal{L}^{\mathsf{Max}} \in \wp(\wp([\![\mathrm{P}]\!]^{\mathsf{Max}}))$ is a set of behaviors of interest, each of which is represented by a maximal trace property;
- $\top^{\mathsf{Max}} = [\![\mathrm{P}]\!]^{\mathsf{Max}}$, i.e. the top of the lattice is the weakest maximal trace property which holds in every valid maximal trace;
- $\bot^{\mathsf{Max}} = \emptyset$, i.e. the bottom of the lattice is the strongest property such that no valid trace has this property, hence it is used to represent the property of invalidity;
- $\subseteq$ is the standard set inclusion operation;

– $\cup$ and $\cap$ are join and meet operations, which might not be the standard $\cup$ and $\cap$, since $\mathcal{L}^{\mathsf{Max}}$ is a subset of $\wp([\![\mathrm{P}]\!]^{\mathsf{Max}})$ but not necessarily a sublattice.

For any given system, there is possibly more than one way to build the complete lattice of maximal trace properties, depending on which behaviors are of interest. A special case of lattice is the power set of maximal trace semantics, i.e. $\mathcal{L}^{\mathsf{Max}} = \wp([\![\mathrm{P}]\!]^{\mathsf{Max}})$, which can be used to examine the responsibility for every possible behavior in the system. However, in most cases, a single behavior is of interest, and it is sufficient to adopt a lattice with only four elements: $\mathcal{B}$ representing the behavior of interest, $[\![\mathrm{P}]\!]^{\mathsf{Max}} \backslash \mathcal{B}$ representing the complement of the behavior of interest, as well as the top $[\![\mathrm{P}]\!]^{\mathsf{Max}}$ and bottom $\emptyset$. Particularly, if $\mathcal{B}$ is equal to $[\![\mathrm{P}]\!]^{\mathsf{Max}}$, i.e. every valid maximal trace in the system has this behavior of interest, then a trivial lattice with only the top and bottom is built, from which no responsibility can be found, making the corresponding analysis futile.

Example 14 (Access Control, Continued) *For the access control program, there are two possible ways to build the lattice of maximal trace properties. To start with, we consider the lattice displayed in Fig. 5.1, which consists of 6 elements. Regarding whether the access to o fails or not, the top* $\top^{\mathsf{Max}} = [\![\mathrm{P}]\!]^{\mathsf{Max}}$ *is split into two properties "Access Failure" AF and "Access Success" AS, which are formally defined in Example 13 such that* $AF \cup AS = [\![\mathrm{P}]\!]^{\mathsf{Max}}$ *and* $AF \cap AS = \emptyset$*. Furthermore, regarding whether the write access is granted or not, AS is split into "Read Only access is granted" RO and "Read and Write access is granted" RW, such that* $RO \cup RW = AS$ *and* $RO \cap RW = \emptyset$*. With the assistance of such a lattice of system behaviors, we can determine not only the responsible entity for access failure/success, but also the entity in charge of the write access.*

Meanwhile, if we are interested in only one behavior (e.g. "Access Failure" AF), then RO and RW can be simply removed from the lattice and we can get a lattice with 4 elements. □

5.2.3 Prediction Abstraction

Although the maximal trace property is well-suited to represent system behaviors, it does not reveal the point along the maximal trace from which a property is guaranteed to hold later in the execution. Thus, we propose to abstract every maximal trace property $\mathcal{X} \in \mathcal{L}^{\mathsf{Max}}$ isomorphically into a set $\mathcal{Y}$ of prefixes of maximal traces in $\mathcal{X}$, excluding those whose maximal prolongation may not satisfy the property $\mathcal{X}$. This abstraction is called *prediction abstraction*, and $\mathcal{Y}$ is called the *prediction trace property* corresponding to $\mathcal{X}$. It is easy to see that $\mathcal{Y}$ is a superset of $\mathcal{X}$, and is not necessarily prefix-closed.

$$
\begin{array}{rcll}
\alpha_{\mathsf{Pred}}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}) & \in & \wp(\mathbb{S}^{*\infty}) \mapsto \wp(\mathbb{S}^{*\infty}) & \text{prediction abstraction} \\
\alpha_{\mathsf{Pred}}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}})\mathcal{X} & \triangleq & \{\sigma \in \mathsf{Pref}(\mathcal{X}) \mid \forall \sigma' \in \llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}.\ \sigma \preceq \sigma' \Rightarrow \sigma' \in \mathcal{X}\} & \\
\gamma_{\mathsf{Pred}}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}) & \in & \wp(\mathbb{S}^{*\infty}) \mapsto \wp(\mathbb{S}^{*\infty}) & \text{prediction concretization} \\
\gamma_{\mathsf{Pred}}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}})\mathcal{Y} & \triangleq & \{\sigma \in \mathcal{Y} \mid \sigma \in \llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}\} = \mathcal{Y} \cap \llbracket \mathrm{P} \rrbracket^{\mathsf{Max}} &
\end{array}
$$

By the above definition, for any program P, every valid maximal trace σ' that is greater than or equal to a prefix trace σ in $\alpha_{\mathsf{Pred}}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}})\mathcal{X}$ is guaranteed to have the maximal trace property $\mathcal{X}$ (i.e. $\sigma' \in \mathcal{X}$). Hence, the prefix traces in $\alpha_{\mathsf{Pred}}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}})\mathcal{X}$ gives a hint on the point along the maximal trace from which the property $\mathcal{X}$ is guaranteed to hold. More formally, we have the following lemma:

Lemma 1 *For any maximal trace property $\mathcal{X} \in \wp(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}})$, if a prefix trace σ belongs to $\alpha_{\mathsf{Pred}}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}})\mathcal{X}$, then σ guarantees the satisfaction of property $\mathcal{X}$ (i.e. every valid maximal trace that is greater than or equal to σ is guaranteed to have property $\mathcal{X}$).*

Moreover, we have a Galois isomorphism between maximal trace properties and prediction trace properties:

$$\langle \wp(\llbracket P \rrbracket^{\mathsf{Max}}),\ \subseteq \rangle \xleftarrow[\alpha_{\mathsf{Pred}}(\llbracket P \rrbracket^{\mathsf{Max}})]{\gamma_{\mathsf{Pred}}(\llbracket P \rrbracket^{\mathsf{Max}})} \langle \bar{\alpha}_{\mathsf{Pred}}\{\llbracket P \rrbracket^{\mathsf{Max}}\}(\wp(\llbracket P \rrbracket^{\mathsf{Max}})),\ \subseteq \rangle \tag{5.1}$$

where the abstract domain is obtained by a function $\bar{\alpha}_{\mathsf{Pred}}\{\llbracket P \rrbracket^{\mathsf{Max}}\} \in \wp(\wp(\mathbb{S}^{*\infty})) \mapsto \wp(\wp(\mathbb{S}^{*\infty}))$ such that $\bar{\alpha}_{\mathsf{Pred}}\{\llbracket P \rrbracket^{\mathsf{Max}}\}(\mathfrak{X}) \triangleq \{\alpha_{\mathsf{Pred}}(\llbracket P \rrbracket^{\mathsf{Max}})\mathcal{X} \mid \mathcal{X} \in \mathfrak{X}\}$.

Proof. First, we prove that $\alpha_{\mathsf{Pred}}(\llbracket P \rrbracket^{\mathsf{Max}})$ and $\gamma_{\mathsf{Pred}}(\llbracket P \rrbracket^{\mathsf{Max}})$ are increasing.

– $\mathcal{X} \subseteq \mathcal{X}'$

$\Rightarrow \forall \sigma' \in \llbracket P \rrbracket^{\mathsf{Max}}.\ (\sigma' \in \mathcal{X}) \Rightarrow (\sigma' \in \mathcal{X}')$ ⟅def. $\subseteq$⟆

$\Rightarrow \forall \sigma \in \mathbb{S}^{*\infty}, \sigma' \in \llbracket P \rrbracket^{\mathsf{Max}}.\ (\neg(\sigma \preceq \sigma') \vee (\sigma' \in \mathcal{X})) \Rightarrow (\neg(\sigma \preceq \sigma') \vee (\sigma' \in \mathcal{X}'))$

⟅def. $\vee$⟆

$\Rightarrow \{\sigma \in \mathbb{S}^{*\infty} \mid \forall \sigma' \in \llbracket P \rrbracket^{\mathsf{Max}}.\ \neg(\sigma \preceq \sigma') \vee (\sigma' \in \mathcal{X})\} \subseteq$

$\{\sigma \in \mathbb{S}^{*\infty} \mid \forall \sigma' \in \llbracket P \rrbracket^{\mathsf{Max}}.\ \neg(\sigma \preceq \sigma') \vee (\sigma' \in \mathcal{X}')\}$ ⟅def. $\subseteq$⟆

$\Rightarrow \{\sigma \in \mathbb{S}^{*\infty} \mid \forall \sigma' \in \llbracket P \rrbracket^{\mathsf{Max}}.\ \sigma \preceq \sigma' \Rightarrow \sigma' \in \mathcal{X}\} \subseteq$

$\{\sigma \in \mathbb{S}^{*\infty} \mid \forall \sigma' \in \llbracket P \rrbracket^{\mathsf{Max}}.\ \sigma \preceq \sigma' \Rightarrow \sigma' \in \mathcal{X}'\}$ ⟅def. $\Rightarrow$⟆

$\Rightarrow (\mathsf{Pref}(\mathcal{X}) \cap \{\sigma \mid \forall \sigma' \in \llbracket P \rrbracket^{\mathsf{Max}}.\ \sigma \preceq \sigma' \Rightarrow \sigma' \in \mathcal{X}\}) \subseteq$

$(\mathsf{Pref}(\mathcal{X}') \cap \{\sigma \mid \forall \sigma' \in \llbracket P \rrbracket^{\mathsf{Max}}.\ \sigma \preceq \sigma' \Rightarrow \sigma' \in \mathcal{X}'\})$ ⟅def. $\cap$ and Pref is increasing⟆

$\Rightarrow \{\sigma \in \mathsf{Pref}(\mathcal{X}) \mid \forall \sigma' \in \llbracket P \rrbracket^{\mathsf{Max}}.\ \sigma \preceq \sigma' \Rightarrow \sigma' \in \mathcal{X}\} \subseteq$

$\{\sigma \in \mathsf{Pref}(\mathcal{X}') \mid \forall \sigma' \in \llbracket P \rrbracket^{\mathsf{Max}}.\ \sigma \preceq \sigma' \Rightarrow \sigma' \in \mathcal{X}'\}$ ⟅def. $\cap$⟆

$\Rightarrow \alpha_{\mathsf{Pred}}(\llbracket P \rrbracket^{\mathsf{Max}})\mathcal{X} \subseteq \alpha_{\mathsf{Pred}}(\llbracket P \rrbracket^{\mathsf{Max}})\mathcal{X}'$ ⟅def. $\alpha_{\mathsf{Pred}}(\llbracket P \rrbracket^{\mathsf{Max}})$⟆

– $\mathcal{Y} \subseteq \mathcal{Y}'$

$\Rightarrow (\mathcal{Y} \cap [\![\mathrm{P}]\!]^{\mathsf{Max}}) \subseteq (\mathcal{Y}' \cap [\![\mathrm{P}]\!]^{\mathsf{Max}})$ ⟅def. $\cap$⟆

$\Rightarrow \gamma_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\mathcal{Y} \subseteq \gamma_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\mathcal{Y}'$ ⟅def. $\gamma_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})$⟆

Then, we prove that $\gamma_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}}) \circ \alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})$ and $\alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}}) \circ \gamma_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})$ are identity functions.

– $\gamma_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}}) \circ \alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\mathcal{X}$

= $\gamma_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})(\{\sigma \in \mathsf{Pref}(\mathcal{X}) \mid \forall \sigma' \in [\![\mathrm{P}]\!]^{\mathsf{Max}}.\ \sigma \preceq \sigma' \Rightarrow \sigma' \in \mathcal{X}\})$ ⟅def. α_{Pred}⟆

= $\gamma_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})(\mathcal{X} \cup \{\sigma \in \mathsf{Pref}(\mathcal{X}) \backslash [\![\mathrm{P}]\!]^{\mathsf{Max}} \mid \forall \sigma' \in [\![\mathrm{P}]\!]^{\mathsf{Max}}.\ \sigma \preceq \sigma' \Rightarrow \sigma' \in \mathcal{X}\})$

⟅$\mathcal{X} = \mathsf{Pref}(\mathcal{X}) \cap [\![\mathrm{P}]\!]^{\mathsf{Max}}$ since $\mathcal{X} \in \wp([\![\mathrm{P}]\!]^{\mathsf{Max}})$⟆

= $[\![\mathrm{P}]\!]^{\mathsf{Max}} \cap (\mathcal{X} \cup \{\sigma \in \mathsf{Pref}(\mathcal{X}) \backslash [\![\mathrm{P}]\!]^{\mathsf{Max}} \mid \forall \sigma' \in [\![\mathrm{P}]\!]^{\mathsf{Max}}.\ \sigma \preceq \sigma' \Rightarrow \sigma' \in \mathcal{X}\})$

⟅def. γ_{Pred}⟆

= $[\![\mathrm{P}]\!]^{\mathsf{Max}} \cap \mathcal{X}$ ⟅$[\![\mathrm{P}]\!]^{\mathsf{Max}} \cap (\mathsf{Pref}(\mathcal{X}) \backslash [\![\mathrm{P}]\!]^{\mathsf{Max}}) = \emptyset$⟆

= $\mathcal{X}$ ⟅$\mathcal{X} \in \wp([\![\mathrm{P}]\!]^{\mathsf{Max}})$⟆

– $\alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}}) \circ \gamma_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\mathcal{Y}$

= $\alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}}) \circ \gamma_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}}) \circ \alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\mathcal{X}'$

⟅$\mathcal{Y} \in \bar{\alpha}_{\mathsf{Pred}}\{[\![\mathrm{P}]\!]^{\mathsf{Max}}\}(\wp([\![\mathrm{P}]\!]^{\mathsf{Max}}))$, thus $\exists \mathcal{X}'.\ \mathcal{Y} = \alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\mathcal{X}'$⟆

= $\alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\mathcal{X}'$ ⟅$\gamma_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}}) \circ \alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\mathcal{X}' = \mathcal{X}'$⟆

= $\mathcal{Y}$ ⟅by the assumption $\mathcal{Y} = \alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\mathcal{X}'$⟆

– By the four properties proved above, $\alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})$ and $\gamma_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})$ form a Galois isomorphism. □

Corollary 1 *Given the semantics* $[\![\mathrm{P}]\!]^{\mathsf{Max}}$ *and lattice* $\mathcal{L}^{\mathsf{Max}}$ *of system behaviors, for any maximal trace property* $\mathcal{T} \in \mathcal{L}^{\mathsf{Max}}$*, if a trace* σ *belongs to the prediction trace property that corresponds to* $\mathcal{T}$*, then every valid trace greater than* σ *belongs to that prediction trace property too. I.e.* $\forall \mathcal{T} \in \mathcal{L}^{\mathsf{Max}}.\ \forall \sigma, \sigma' \in [\![\mathrm{P}]\!]^{\mathsf{Pref}}.\ (\sigma \in \alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\mathcal{T} \wedge \sigma \preceq \sigma') \Rightarrow \sigma' \in \alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\mathcal{T}$.

Proof. Proof by contradiction. Here we assume $\exists \mathcal{T} \in \mathcal{L}^{\mathsf{Max}}.\ \exists \sigma, \sigma' \in [\![\mathrm{P}]\!]^{\mathsf{Pref}}.\ \sigma \in \alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\mathcal{T} \wedge \sigma \preceq \sigma' \wedge \sigma' \notin \alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\mathcal{T}$. By the definition of prediction abstraction, $\alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\mathcal{T} = \{\sigma \in \mathsf{Pref}(\mathcal{T}) \mid \forall \sigma' \in [\![\mathrm{P}]\!]^{\mathsf{Max}}.\ \sigma \preceq \sigma' \Rightarrow \sigma' \in \mathcal{T}\}$. There are two possibilities for $\sigma' \notin \alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\mathcal{T}$:

1) $\sigma' \notin \mathsf{Pref}(\mathcal{T})$, hence every maximal trace greater than σ' does not belong to $\mathcal{T}$;

2) $\exists \sigma'' \in [\![\mathrm{P}]\!]^{\mathsf{Max}}.\ \sigma' \preceq \sigma'' \wedge \sigma'' \notin \mathcal{T}$.

Both cases imply that there is a maximal trace $\sigma'' \in [\![\mathrm{P}]\!]^{\mathsf{Max}}$ such that $\sigma \preceq \sigma' \preceq \sigma'' \wedge \sigma'' \notin \mathcal{T}$, which contradicts with the assumption of $\sigma \in \alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\mathcal{T}$. □

Corollary 2 *Given the semantics* $[\![\mathrm{P}]\!]^{\mathsf{Max}}$ *and the lattice* $\mathcal{L}^{\mathsf{Max}}$ *of system behaviors, for any maximal trace property* $\mathcal{T} \in \mathcal{L}^{\mathsf{Max}}$ *and any valid prefix trace* π *that is not maximal, if every valid prefix trace* πs *which concatenates* π *with a new event* s *belongs to the prediction trace property* $\alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\mathcal{T}$*, then* π *belongs to* $\alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\mathcal{T}$ *too.*

More formally, $\forall \mathcal{T} \in \mathcal{L}^{\mathsf{Max}}.\ \forall \pi \in [\![\mathrm{P}]\!]^{\mathsf{Pref}} \backslash [\![\mathrm{P}]\!]^{\mathsf{Max}}.\ (\forall s \in \mathbb{S}.\ \pi s \in [\![\mathrm{P}]\!]^{\mathsf{Pref}} \Rightarrow \pi s \in \alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\mathcal{T}) \Rightarrow \pi \in \alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\mathcal{T}$.

Proof. Prove by contradiction, and here we assume that $\exists \mathcal{T} \in \mathcal{L}^{\mathsf{Max}}. \exists \pi \in [\![\mathrm{P}]\!]^{\mathsf{Pref}} \backslash [\![\mathrm{P}]\!]^{\mathsf{Max}}. (\forall s \in \mathbb{S}. \pi s \in [\![\mathrm{P}]\!]^{\mathsf{Pref}} \Rightarrow \pi s \in \alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\mathcal{T}) \wedge \pi \notin \alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\mathcal{T}$. According to the definition that $\alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\mathcal{T} = \{\sigma \in \mathsf{Pref}(\mathcal{T}) \mid \forall \sigma' \in [\![\mathrm{P}]\!]^{\mathsf{Max}}. \sigma \preceq \sigma' \Rightarrow \sigma' \in \mathcal{T}\}$, there are two possibilities to have $\pi \notin \alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\mathcal{T}$:

1) $\pi \notin \mathsf{Pref}(\mathcal{T})$. This implies that $\forall s \in \mathbb{S}. \pi s \in [\![\mathrm{P}]\!]^{\mathsf{Pref}} \Rightarrow \pi s \notin \mathsf{Pref}(\mathcal{T})$, which further implies that $\forall s \in \mathbb{S}. \pi s \in [\![\mathrm{P}]\!]^{\mathsf{Pref}} \Rightarrow \pi s \notin \alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\mathcal{T}$. Since $\pi \in [\![\mathrm{P}]\!]^{\mathsf{Pref}} \backslash [\![\mathrm{P}]\!]^{\mathsf{Max}}$, there must exist at least one s such that $\pi s \in [\![\mathrm{P}]\!]^{\mathsf{Pref}} \wedge \pi s \notin \alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\mathcal{T}$.

2) There is a maximal trace $\sigma' \in [\![\mathrm{P}]\!]^{\mathsf{Max}}$ such that $\pi \prec \sigma' \wedge \sigma' \notin \mathcal{T}$. Take $s = \sigma'_{[|\pi|]}$, then $\pi s \in [\![\mathrm{P}]\!]^{\mathsf{Pref}} \wedge \pi s \preceq \sigma' \wedge \sigma' \notin \mathcal{T}$ holds, which implies $\pi s \in [\![\mathrm{P}]\!]^{\mathsf{Pref}} \wedge \pi s \notin \alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\mathcal{T}$.

Both two cases find that $\exists s \in \mathbb{S}. \pi s \in [\![\mathrm{P}]\!]^{\mathsf{Pref}} \wedge \pi s \notin \alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\mathcal{T}$, which contradicts with the assumption $\forall s \in \mathbb{S}. \pi s \in [\![\mathrm{P}]\!]^{\mathsf{Pref}} \Rightarrow \pi s \in \alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\mathcal{T}$. □

Example 15 (Access Control, Continued) *By the function $\alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})$, each behavior in the lattice $\mathcal{L}^{\mathsf{Max}}$ of Example 14 can be abstracted into a prediction trace property:*

- $\alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\top^{\mathsf{Max}} = [\![\mathrm{P}]\!]^{\mathsf{Pref}}$*, i.e. every valid prefix trace in* $[\![\mathrm{P}]\!]^{\mathsf{Pref}}$ *guarantees* $\top^{\mathsf{Max}}$.
- $\alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})AF = \{\sigma \in [\![\mathrm{P}]\!]^{\mathsf{Pref}} \mid \exists \rho_1 \in \mathbb{M}, v \in \{\text{-}1, 0\}, v' \in \{1, 2\}. \langle \ell_1, \rho_1 \rangle \langle \ell_2, \rho_2 = \rho_1[apv \mapsto 1] \rangle \langle \ell_3, \rho_3 = \rho_2[i1 \mapsto v] \rangle \preceq \sigma \vee \langle \ell_1, \rho_1 \rangle \langle \ell_2, \rho_2 = \rho_1[apv \mapsto 1] \rangle \langle \ell_3, \rho_3 = \rho_2[i1 \mapsto v'] \rangle \langle \ell_4, \rho_4 = \rho_3 \rangle \langle \ell_5, \rho_5 = \rho_4[i2 \mapsto v] \rangle \preceq \sigma\}$. *For any valid prefix trace σ, if at least one input from the two admins is* -1 *or* 0*, then the behavior "Access Failure" AF is guaranteed to occur in all the maximal traces that are greater than or equal to σ.*
- $\alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})AS = \{\sigma \in [\![\mathrm{P}]\!]^{\mathsf{Pref}} \mid \exists \rho_1 \in \mathbb{M}, v \in \{1, 2\}. \langle \ell_1, \rho_1 \rangle \langle \ell_2, \rho_2 = \rho_1[apv \mapsto 1] \rangle \langle \ell_3, \rho_3 = \rho_2[i1 \mapsto v] \rangle \langle \ell_4, \rho_4 = \rho_3 \rangle \langle \ell_5, \rho_5 = \rho_4[i2 \mapsto v] \rangle \preceq \sigma\}$. *For any valid prefix trace σ, if the inputs from both admins are 1 or 2, "Access Success" AS is guaranteed.*

– $\alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})RO = \{\sigma \in [\![\mathrm{P}]\!]^{\mathsf{Pref}} \mid \exists \rho_1 \in \mathbb{M}, v \in \{1,2\}.\ \langle \ell_1,\ \rho_1\rangle\langle \ell_2,\ \rho_2 = \rho_1[\mathit{apv} \mapsto 1]\rangle\langle \ell_3,\ \rho_3 = \rho_2[\mathit{i1} \mapsto v]\rangle\langle \ell_4,\ \rho_4 = \rho_3\rangle\langle \ell_5,\ \rho_5 = \rho_4[\mathit{i2} \mapsto v]\rangle\langle \ell_6,\ \rho_6 = \rho_5\rangle\langle \ell_7,\ \rho_7 = \rho_6[\mathit{typ} \mapsto 1]\rangle \preceq \sigma\}$. *For any valid trace, if the inputs from both admins are 1 or 2 and the input from system settings is 1, then it guarantees "Read Only access is granted" RO.*

– $\alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})RW = \{\sigma \in [\![\mathrm{P}]\!]^{\mathsf{Pref}} \mid \exists \rho_1 \in \mathbb{M}, v \in \{1,2\}.\ \langle \ell_1,\ \rho_1\rangle\langle \ell_2,\ \rho_2 = \rho_1[\mathit{apv} \mapsto 1]\rangle\langle \ell_3,\ \rho_3 = \rho_2[\mathit{i1} \mapsto v]\rangle\langle \ell_4,\ \rho_4 = \rho_3\rangle\langle \ell_5,\ \rho_5 = \rho_4[\mathit{i2} \mapsto v]\rangle\langle \ell_6,\ \rho_6 = \rho_5\rangle\langle \ell_7,\ \rho_7 = \rho_6[\mathit{typ} \mapsto 2]\rangle \preceq \sigma\}$. *For any valid trace, if the inputs from both admins are 1 or 2 and the input from system settings is 2, then it guarantees "Read and Write access is granted" RW.*

– $\alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\bot^{\mathsf{Max}} = \emptyset$*, i.e. no valid trace can guarantee the bottom* $\bot^{\mathsf{Max}}$. □

5.3 Observation of System Behaviors

Let $[\![\mathrm{P}]\!]^{\mathsf{Max}}$ be the maximal trace semantics and $\mathcal{L}^{\mathsf{Max}}$ be the lattice of system behaviors designed as in Section 5.2. Given any prefix trace $\sigma \in \mathbb{S}^{*\infty}$, an observer can learn some information from it, more precisely, a maximal trace property $\mathcal{T} \in \mathcal{L}^{\mathsf{Max}}$ that is guaranteed by σ from the observer's perspective. In this section, an *observation* function $\mathbb{O}$ is proposed to represent such a "property learning process" of the observer, which is formally defined in the following three steps.

5.3.1 Inquiry Function

First, an *inquiry function* $\mathbb{I}$ is defined to map every trace $\sigma \in \mathbb{S}^{*\infty}$ to the strongest maximal trace property in $\mathcal{L}^{\mathsf{Max}}$ that σ can guarantee.

$$\mathbb{I} \in \wp(\mathbb{S}^{*\infty}) \mapsto \wp(\wp(\mathbb{S}^{*\infty})) \mapsto \mathbb{S}^{*\infty} \mapsto \wp(\mathbb{S}^{*\infty}) \qquad \text{inquiry (5.2)}$$

$$\mathbb{I}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma) \triangleq$$
$$\quad let\ \alpha_{\mathsf{Pred}}(\mathcal{S})\mathcal{T} = \{\sigma \in \mathsf{Pref}(\mathcal{T}) \mid \forall \sigma' \in \mathcal{S}.\ \sigma \preceq \sigma' \Rightarrow \sigma' \in \mathcal{T}\}\ in$$
$$\quad\quad \curvearrowright\{\mathcal{T} \in \mathcal{L}^{\mathsf{Max}} \mid \sigma \in \alpha_{\mathsf{Pred}}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}})\mathcal{T}\}$$

Specially, for every invalid trace $\sigma \notin \llbracket \mathrm{P} \rrbracket^{\mathsf{Pref}}$, there does not exist any $\mathcal{T} \in \mathcal{L}^{\mathsf{Max}}$ such that $\sigma \in \alpha_{\mathsf{Pred}}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}})\mathcal{T}$, thus $\mathbb{I}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma) = \emptyset = \bot^{\mathsf{Max}}$. In contrast, for any valid trace $\sigma \in \llbracket \mathrm{P} \rrbracket^{\mathsf{Pref}}$, it is ensured that $\sigma \in \alpha_{\mathsf{Pred}}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}})\top^{\mathsf{Max}}$, hence $\mathbb{I}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma) \neq \bot^{\mathsf{Max}}$. Therefore, $\mathbb{I}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma) = \bot^{\mathsf{Max}}$ if and only if σ is invalid.

Example 16 (Access Control, Continued) *Using the maximal trace semantics* $\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}$ *from Example 2 and the lattice of system behaviors* $\mathcal{L}^{\mathsf{Max}}$ *from Example 14, here we define the inquiry function* $\mathbb{I}$ *for the access control program such that for any initial environment* $\rho_1 \in \mathbb{M}$*:*

- $\mathbb{I}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \langle \ell_1,\ \rho_1 \rangle \langle \ell_2,\ \rho_2 = \rho_1[\mathit{apv} \mapsto 1] \rangle) = \top^{\mathsf{Max}}$*, i.e. every prefix trace that terminates at point* ℓ_2 *(before the admins input their decisions) can guarantee only* $\top^{\mathsf{Max}}$*.*

- $\mathbb{I}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \langle \ell_1,\ \rho_1 \rangle \langle \ell_2,\ \rho_2 = \rho_1[\mathit{apv} \mapsto 1] \rangle \langle \ell_3,\ \rho_3 = \rho_2[\mathit{i1} \mapsto 0] \rangle) =$ *AF, i.e. after the 1st admin inputs 0, the behavior "Access Failure" AF is guaranteed.*

- $\mathbb{I}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \langle \ell_1,\ \rho_1 \rangle \langle \ell_2,\ \rho_2 = \rho_1[\mathit{apv} \mapsto 1] \rangle \langle \ell_3,\ \rho_3 = \rho_2[\mathit{i1} \mapsto 1] \rangle) = \mathbb{I}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \langle \ell_1,\ \rho_1 \rangle \langle \ell_2,\ \rho_2 = \rho_1[\mathit{apv} \mapsto 1] \rangle \langle \ell_3,\ \rho_3 = \rho_2[\mathit{i1} \mapsto 1] \rangle \langle \ell_4,\ \rho_4 = \rho_3 \rangle) = \top^{\mathsf{Max}}$*, i.e. if the first admin inputs 1, only the top* $\top^{\mathsf{Max}}$ *can be guaranteed before the second admin inputs her/his decision.*

- $\mathbb{I}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \langle \ell_1,\ \rho_1 \rangle \langle \ell_2,\ \rho_2 = \rho_1[\mathit{apv} \mapsto 1] \rangle \langle \ell_3,\ \rho_3 = \rho_2[\mathit{i1} \mapsto 1] \rangle \langle \ell_4,\ \rho_4 = \rho_3 \rangle \langle \ell_5,\ \rho_5 = \rho_4[\mathit{i2} \mapsto 0] \rangle) =$ *AF, i.e. after the second admin inputs 0, the behavior "Access Failure" AF is guaranteed.*

– $\mathbb{I}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \langle \ell_1,\ \rho_1\rangle\langle \ell_2,\ \rho_2 = \rho_1[\mathit{apv} \mapsto 1]\rangle\langle \ell_3,\ \rho_3 = \rho_2[\mathit{i1} \mapsto 1]\rangle\langle \ell_4,\ \rho_4 = \rho_3\rangle\langle \ell_5,\ \rho_5 = \rho_4[\mathit{i2} \mapsto 1]\rangle) =$ *AS, i.e. if both two admin inputs 1, "Access Success" AS is guaranteed.*

– $\mathbb{I}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \langle \ell_1,\ \rho_1\rangle\langle \ell_2,\ \rho_2 = \rho_1[\mathit{apv} \mapsto 1]\rangle\langle \ell_3,\ \rho_3 = \rho_2[\mathit{i1} \mapsto 1]\rangle\langle \ell_4,\ \rho_4 = \rho_3\rangle\langle \ell_5,\ \rho_5 = \rho_4[\mathit{i2} \mapsto 1]\rangle\langle \ell_6,\ \rho_6 = \rho_5\rangle\langle \ell_7,\ \rho_7 = \rho_6[\mathit{typ} \mapsto 1]\rangle) =$ *RO, i.e. if both two admin input 1, then after the input from system settings is set as 1, a stronger property "Read Only access is granted" RO is guaranteed.*

– $\mathbb{I}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \langle \ell_1,\ \rho_1\rangle\langle \ell_2,\ \rho_2 = \rho_1[\mathit{apv} \mapsto 1]\rangle\langle \ell_3,\ \rho_3 = \rho_2[\mathit{i1} \mapsto 1]\rangle\langle \ell_4,\ \rho_4 = \rho_3\rangle\langle \ell_5,\ \rho_5 = \rho_4[\mathit{i2} \mapsto 1]\rangle\langle \ell_6,\ \rho_6 = \rho_5\rangle\langle \ell_7,\ \rho_7 = \rho_6[\mathit{typ} \mapsto 2]\rangle) =$ *RW, i.e. if both two admin input 1, then after the input from system settings is set as 2, a stronger property "Read and Write access is granted" RW is guaranteed.* □

Corollary 3 *Given the semantics* $[\![\mathrm{P}]\!]^{\mathsf{Max}}$ *and lattice* $\mathcal{L}^{\mathsf{Max}}$ *of system behaviors, if the inquiry function* $\mathbb{I}$ *maps a trace* σ *to a maximal trace property* $\mathcal{T} \in \mathcal{L}^{\mathsf{Max}}$*, then* σ *guarantees the satisfaction of* $\mathcal{T}$ *(i.e. every valid maximal trace that is greater than or equal to* σ *is guaranteed to have property* $\mathcal{T}$*).*

Proof. The proof immediately follows Lemma 1 and the definition (5.2) of inquiry. □

Lemma 2 *Given the semantics* $[\![\mathrm{P}]\!]^{\mathsf{Max}}$ *and lattice* $\mathcal{L}^{\mathsf{Max}}$ *of system behaviors, the inquiry function* $\mathbb{I}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}})$ *is decreasing on the inquired trace* σ*: the greater (longer)* σ *is, the stronger property it can guarantee. I.e.* $\forall \sigma, \sigma' \in \mathbb{S}^{*\infty}.\ \sigma \preceq \sigma' \Rightarrow \mathbb{I}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma) \supseteq \mathbb{I}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma')$.

Proof. First, if σ is invalid (i.e. $\sigma \notin [\![\mathrm{P}]\!]^{\mathsf{Pref}}$), then every trace σ' that is greater than σ must also be invalid (i.e. $\sigma' \notin [\![\mathrm{P}]\!]^{\mathsf{Pref}}$), hence it is obvious that $\mathbb{I}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma) = \mathbb{I}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma') = \bot^{\mathsf{Max}}$.

Second, if σ' is invalid ($\sigma' \notin [\![P]\!]^{\mathsf{Pref}}$), then we have $\mathbb{I}([\![P]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma') = \bot^{\mathsf{Max}}$, hence $\mathbb{I}([\![P]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma) \supseteq \bot^{\mathsf{Max}} = \mathbb{I}([\![P]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma')$.

Last, if both σ and σ' are valid($\sigma, \sigma' \in [\![P]\!]^{\mathsf{Pref}}$), then we have

$\sigma \preceq \sigma'$

$\Rightarrow \forall \mathcal{T} \in \mathcal{L}^{\mathsf{Max}}.\ \sigma \in \alpha_{\mathsf{Pred}}([\![P]\!]^{\mathsf{Max}})\mathcal{T} \Rightarrow \sigma' \in \alpha_{\mathsf{Pred}}([\![P]\!]^{\mathsf{Max}})\mathcal{T}$ ⦇corollary 1⦈

$\Rightarrow \{\mathcal{T} \in \mathcal{L}^{\mathsf{Max}} \mid \sigma \in \alpha_{\mathsf{Pred}}([\![P]\!]^{\mathsf{Max}})\mathcal{T}\} \subseteq \{\mathcal{T} \in \mathcal{L}^{\mathsf{Max}} \mid \sigma' \in \alpha_{\mathsf{Pred}}([\![P]\!]^{\mathsf{Max}})\mathcal{T}\}$

⦇def. $\Rightarrow$⦈

$\Rightarrow \curlywedge\{\mathcal{T} \in \mathcal{L}^{\mathsf{Max}} \mid \sigma \in \alpha_{\mathsf{Pred}}([\![P]\!]^{\mathsf{Max}})\mathcal{T}\} \supseteq \curlywedge\{\mathcal{T} \in \mathcal{L}^{\mathsf{Max}} \mid \sigma' \in \alpha_{\mathsf{Pred}}([\![P]\!]^{\mathsf{Max}})\mathcal{T}\}$

⦇def. $\curlywedge$⦈

$\Rightarrow \mathbb{I}([\![P]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma) \supseteq \mathbb{I}([\![P]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma')$ ⦇def. $\mathbb{I}$⦈

To sum up the three cases above, we prove that $\mathbb{I}([\![P]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}})$ is decreasing. □

Corollary 4 *Given the semantics* $[\![P]\!]^{\mathsf{Max}}$ *and lattice* $\mathcal{L}^{\mathsf{Max}}$ *of behaviors,* $\forall \sigma \in [\![P]\!]^{\mathsf{Pref}} \setminus [\![P]\!]^{\mathsf{Max}}$. $\mathbb{I}([\![P]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma) = \bigcurlyvee_{s \in \mathbb{S}} \mathbb{I}([\![P]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma s) = \bigcurlyvee_{\sigma s \in [\![P]\!]^{\mathsf{Pref}}} \mathbb{I}([\![P]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma s)$.

Proof. First, $\curlyvee\{\mathbb{I}([\![P]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma s) \mid s \in \mathbb{S}\} = (\curlyvee\{\mathbb{I}([\![P]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma s) \mid \sigma s \in [\![P]\!]^{\mathsf{Pref}}\}) \curlyvee (\curlyvee\{\mathbb{I}([\![P]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma s) \mid \sigma s \notin [\![P]\!]^{\mathsf{Pref}}\}) = (\curlyvee\{\mathbb{I}([\![P]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma s) \mid \sigma s \in [\![P]\!]^{\mathsf{Pref}}\}) \curlyvee \bot^{\mathsf{Max}} = \curlyvee\{\mathbb{I}([\![P]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma s) \mid \sigma s \in [\![P]\!]^{\mathsf{Pref}}\}$.

Second, we prove $\curlyvee\{\mathbb{I}([\![P]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma s) \mid \sigma s \in [\![P]\!]^{\mathsf{Pref}}\} = \mathbb{I}([\![P]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma)$ in two steps: 1) by lemma 2, it is proved that $\forall \sigma, \sigma s \in \mathbb{S}^{*\infty}.\ \mathbb{I}([\![P]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma) \supseteq \mathbb{I}([\![P]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma s)$, thus $\mathbb{I}([\![P]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma) \supseteq \curlyvee\{\mathbb{I}([\![P]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma s) \mid \sigma s \in [\![P]\!]^{\mathsf{Pref}}\}$. 2) assume $\mathbb{I}([\![P]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma) \supsetneq \curlyvee\{\mathbb{I}([\![P]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma s) \mid \sigma s \in [\![P]\!]^{\mathsf{Pref}}\} = \mathcal{T}$. By

the definition of $\mathbb{I}$ in (5.2), we know that $\sigma \notin \alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\mathcal{T}$ and $\forall \sigma s \in [\![\mathrm{P}]\!]^{\mathsf{Pref}}$. $\sigma s \in \alpha_{\mathsf{Pred}}([\![\mathrm{P}]\!]^{\mathsf{Max}})\mathcal{T}$, which is impossible by corollary 2. Thus, by contradiction, $\mathbb{I}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma) = \dot{\cup}\{\mathbb{I}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma s) \mid \sigma s \in [\![\mathrm{P}]\!]^{\mathsf{Pref}}\}$. □

5.3.2 Cognizance Function

As discussed in (P3) of section 4.1, it is necessary to take the observer's cognizance into account. Specifically, in program security, the cognizance can represent attackers' capabilities, e.g. what they can learn from program executions (see section 6.2 for more details). Given a trace σ (not necessarily valid), if the observer cannot distinguish σ from some other traces, then she/he does not have an omniscient cognizance of σ, and the *cognizance* function $\mathbb{C}(\sigma)$ is defined to include all traces indistinguishable from σ.

$$\mathbb{C} \in \mathbb{S}^{*\infty} \mapsto \wp(\mathbb{S}^{*\infty}) \qquad \text{cognizance (5.3)}$$
$$\mathbb{C}(\sigma) \triangleq \{\sigma' \in \mathbb{S}^{*\infty} \mid \text{the observer cannot distinguish } \sigma' \text{ from } \sigma\}$$

Such a cognizance function is extensive, i.e. $\forall \sigma \in \mathbb{S}^{*\infty}.\ \sigma \in \mathbb{C}(\sigma)$. In particular, there is an *omniscient observer* and its corresponding cognizance function is denoted as $\mathbb{C}_o$ such that $\forall \sigma \in \mathbb{S}^{*\infty}.\ \mathbb{C}_o(\sigma) = \{\sigma\}$, which means that every trace is unambiguous to the omniscient observer.

To facilitate the proof of some desired properties for the observation function defined later, two assumptions are made here without loss of generality:

(A1) The cognizance of a trace $\sigma\sigma'$ is the concatenation of cognizances of σ and σ'. I.e. $\forall \sigma, \sigma' \in \mathbb{S}^{*\infty}.\ \mathbb{C}(\sigma\sigma') = \{\pi\pi' \mid \pi \in \mathbb{C}(\sigma) \wedge \pi' \in \mathbb{C}(\sigma')\}$. Specially, we require that $\mathbb{C}(\varepsilon) = \{\varepsilon\}$, such that for any non-empty finite trace σ, $\mathbb{C}(\sigma) = \mathbb{C}(\sigma\varepsilon) = \{\pi\pi' \mid \pi \in \mathbb{C}(\sigma) \wedge \pi' \in \mathbb{C}(\varepsilon)\}$ would not include infinite traces.

(A2) Given an invalid trace, the cognizance function would not return a valid trace. I.e. $\forall \sigma \in \mathbb{S}^{*\infty}.\ \sigma \notin [\![\mathrm{P}]\!]^{\mathsf{Pref}} \Rightarrow \mathbb{C}(\sigma) \cap [\![\mathrm{P}]\!]^{\mathsf{Pref}} = \emptyset$.

In practice, we can define an equivalence relation on traces that satisfy the above two assumptions, thus it is assumed that the observer cannot distinguish two traces if and only if they are equivalent. That is to say, for any trace σ, $\mathbb{C}(\sigma)$ is a class of traces that are equivalent to σ, and $\{\langle \sigma,\ \sigma' \rangle \mid \sigma' \in \mathbb{C}(\sigma)\}$ is an equivalence relation.

Corollary 5 *For any cognizance function $\mathbb{C}$, we have* $\bigcup\!\!\!\bullet_{s \in \mathbb{S}} \mathbb{C}(s) \supseteq \mathbb{S}$.

Proof. This corollary follows immediately from the fact that the cognizance function $\mathbb{C}$ is extensive. □

Example 17 (Access Control, Continued) *For the access control program, consider the cognizance function for two different observers.*

(i) For an omniscient observer: $\forall \sigma \in \mathbb{S}^{*\infty}.\ \mathbb{C}_o(\sigma) = \{\sigma\}$.

(ii) For an observer who is unaware of the input from 1st admin: $\mathbb{C}(\langle \ell_1,\ \rho_1 \rangle \langle \ell_2,\ \rho_2 = \rho_1[\mathit{apv} \mapsto 1] \rangle \langle \ell_3,\ \rho_3 = \rho_2[\mathit{i1} \mapsto 0] \rangle) = \{\langle \ell_1,\ \rho_1 \rangle \langle \ell_2,\ \rho_2 = \rho_1[\mathit{apv} \mapsto 1] \rangle \langle \ell_3,\ \rho_3 = \rho_2[\mathit{i1} \mapsto$ -1$] \rangle, \langle \ell_1,\ \rho_1 \rangle \langle \ell_2,\ \rho_2 = \rho_1[\mathit{apv} \mapsto 1] \rangle \langle \ell_3,\ \rho_3 = \rho_2[\mathit{i1} \mapsto 0] \rangle, \langle \ell_1,\ \rho_1 \rangle \langle \ell_2,\ \rho_2 = \rho_1[\mathit{apv} \mapsto 1] \rangle \langle \ell_3,\ \rho_3 = \rho_2[\mathit{i1} \mapsto 1] \rangle, \langle \ell_1,\ \rho_1 \rangle \langle \ell_2,\ \rho_2 = \rho_1[\mathit{apv} \mapsto 1] \rangle \langle \ell_3,\ \rho_3 = \rho_2[\mathit{i1} \mapsto 2] \rangle\}$*, i.e. this observer cannot distinguish whether the input from 1st admin is* -1 *or* 0 *or* 1 *or* 2.

Similarly, for a prefix trace in which the inputs from both two admins are zeros, $\mathbb{C}(\langle \ell_1,\ \rho_1 \rangle \langle \ell_2,\ \rho_2 = \rho_1[\mathit{apv} \mapsto 1] \rangle \langle \ell_3,\ \rho_3 = \rho_2[\mathit{i1} \mapsto 0] \rangle \langle \ell_4,\ \rho_4 = \rho_3 \rangle \langle \ell_5,\ \rho_5 = \rho_4[\mathit{i2} \mapsto 0] \rangle) = \{\langle \ell_1,\ \rho_1 \rangle \langle \ell_2,\ \rho_2 = \rho_1[\mathit{apv} \mapsto 1] \rangle \langle \ell_3,\ \rho_3 = \rho_2[\mathit{i1} \mapsto$ -1$] \rangle \langle \ell_4,\ \rho_4 = \rho_3 \rangle \langle \ell_5,\ \rho_5 = \rho_4[\mathit{i2} \mapsto 0] \rangle, \langle \ell_1,\ \rho_1 \rangle \langle \ell_2,\ \rho_2 = \rho_1[\mathit{apv} \mapsto 1] \rangle \langle \ell_3,\ \rho_3 = \rho_2[\mathit{i1} \mapsto 0] \rangle \langle \ell_4,\ \rho_4 = \rho_3 \rangle \langle \ell_5,\ \rho_5 = \rho_4[\mathit{i2} \mapsto 0] \rangle, \langle \ell_1,\ \rho_1 \rangle \langle \ell_2,\ \rho_2 = \rho_1[\mathit{apv} \mapsto 1] \rangle \langle \ell_3,\ \rho_3 = \rho_2[\mathit{i1} \mapsto 1] \rangle \langle \ell_4,\ \rho_4 = \rho_3 \rangle \langle \ell_5,$

$\rho_5 = \rho_4[i2 \mapsto 0]\rangle, \langle \ell_1,\ \rho_1\rangle\langle \ell_2,\ \rho_2 = \rho_1[apv \mapsto 1]\rangle\langle \ell_3,\ \rho_3 = \rho_2[i1 \mapsto 2]\rangle\langle \ell_4,\ \rho_4 = \rho_3\rangle\langle \ell_5,\ \rho_5 = \rho_4[i2 \mapsto 0]\rangle\}$ *consists of 4 traces, such that the value of i1 is not distinguishable while the value of i2 is. In the same way, the cognizance on other traces can be defined.* □

5.3.3 Observation Function

For an observer with cognizance function $\mathbb{C}$, given a single trace σ, the observer cannot distinguish σ with other traces in $\mathbb{C}(\sigma)$. In order to formalize the information that the observer can learn from σ, we apply the inquiry function $\mathbb{I}$ on each trace in $\mathbb{C}(\sigma)$, and get a set of maximal trace properties. By joining them together, we get the strongest property in $\mathcal{L}^{\mathsf{Max}}$ that σ can guarantee from the observer's perspective. Such a process is defined as the *observation* function $\mathbb{O}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma)$.

$$\mathbb{O} \in \wp(\mathbb{S}^{*\infty}) \mapsto \wp(\wp(\mathbb{S}^{*\infty})) \mapsto (\mathbb{S}^{*\infty} \mapsto \wp(\mathbb{S}^{*\infty})) \mapsto \mathbb{S}^{*\infty} \mapsto \wp(\mathbb{S}^{*\infty})$$

$$\begin{array}{l}\mathbb{O}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma) \triangleq \\ \quad let\ \alpha_{\mathsf{Pred}}(\mathcal{S})\mathcal{T} = \{\sigma \in \mathsf{Pref}(\mathcal{T}) \mid \forall \sigma' \in \mathcal{S}.\ \sigma \preceq \sigma' \Rightarrow \sigma' \in \mathcal{T}\}\ in \\ \quad\quad let\ \mathbb{I}(\mathcal{S}, \mathcal{L}, \sigma) = \curlywedge\{\mathcal{T} \in \mathcal{L} \mid \sigma \in \alpha_{\mathsf{Pred}}(\mathcal{S})\mathcal{T}\}\ in \\ \quad\quad\quad \curlyvee\{\mathbb{I}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma') \mid \sigma' \in \mathbb{C}(\sigma)\}.\end{array} \quad \text{observation (5.4)}$$

From the above definition, it is easy to see that, for every invalid trace $\sigma \notin \llbracket \mathrm{P} \rrbracket^{\mathsf{Pref}}$, we have $\mathbb{O}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma) = \bot^{\mathsf{Max}}$, since every trace σ' in $\mathbb{C}(\sigma)$ is invalid by (A2) and $\mathbb{I}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma') = \bot^{\mathsf{Max}}$. In addition, for an omniscient observer with cognizance function $\mathbb{C}_o$, its observation $\mathbb{O}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}_o, \sigma) = \mathbb{I}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma)$.

Corollary 6 *Given the semantics $\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}$ and lattice $\mathcal{L}^{\mathsf{Max}}$ of system behaviors, for any observer with cognizance $\mathbb{C}$, if the corresponding observation function maps a trace σ to a maximal trace property $\mathcal{T} \in \mathcal{L}^{\mathsf{Max}}$, then σ guarantees the satisfaction of property $\mathcal{T}$ (i.e. every valid maximal trace that is greater than or equal to σ is guaranteed to have property $\mathcal{T}$).*

Proof. Suppose $\mathbb{I}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma) = \mathcal{T}'$. By the corollary 3, σ guarantees the property $\mathcal{T}'$, i.e. every valid maximal trace that is greater than or equal to σ belongs to $\mathcal{T}'$.

In addition, since the cognizance is extensive (i.e. $\sigma \in \mathbb{C}(\sigma)$), then from the definition of observation function in (5.4), we know that $\mathcal{T} = \mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma) = \biguplus\{\mathbb{I}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma') \mid \sigma' \in \mathbb{C}(\sigma)\} \supseteq \mathbb{I}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma) = \mathcal{T}'$. Therefore, every valid maximal trace that is greater than or equal to σ belongs to $\mathcal{T}$. That is to say, σ guarantees the satisfaction of property $\mathcal{T}$. □

Corollary 7 *Given the semantics $[\![\mathrm{P}]\!]^{\mathsf{Max}}$, the lattice $\mathcal{L}^{\mathsf{Max}}$ of system behaviors and the cognizance function $\mathbb{C}$, we have:* $\forall \sigma \in [\![\mathrm{P}]\!]^{\mathsf{Pref}} \backslash [\![\mathrm{P}]\!]^{\mathsf{Max}}.\ \mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma)$
$= \biguplus_{s \in \mathbb{S}} \mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma s) = \biguplus_{\sigma s \in [\![\mathrm{P}]\!]^{\mathsf{Pref}}} \mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma s)$.

Proof. We start the proof from the right side.

$$
\begin{aligned}
& \biguplus_{\sigma s \in [\![\mathrm{P}]\!]^{\mathsf{Pref}}} \mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma s) \\
= \ & (\biguplus_{\sigma s \in [\![\mathrm{P}]\!]^{\mathsf{Pref}}} \mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma s)) \uplus \bot^{\mathsf{Max}} && \wr \text{def.} \bot^{\mathsf{Max}} \wr \\
= \ & \biguplus_{\sigma s \in [\![\mathrm{P}]\!]^{\mathsf{Pref}}} \mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma s) \uplus \biguplus_{\sigma s \notin [\![\mathrm{P}]\!]^{\mathsf{Pref}}} \mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma s) && \wr \text{def. } \mathbb{O} \wr \\
= \ & \biguplus_{s \in \mathbb{S}} \mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma s) && \wr \text{merge two cases} \wr \\
= \ & \biguplus\{\mathbb{I}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \pi) \mid \pi \in \mathbb{C}(\sigma s) \wedge s \in \mathbb{S}\} && \wr \text{def. } \mathbb{O} \wr \\
= \ & \biguplus\{\mathbb{I}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma' \sigma'') \mid \sigma' \sigma'' \in \mathbb{C}(\sigma s) \wedge s \in \mathbb{S}\} && \wr \text{replace } \pi \text{ with } \sigma' \sigma'' \wr \\
= \ & \biguplus\{\mathbb{I}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma' \sigma'') \mid \sigma' \in \mathbb{C}(\sigma) \wedge \sigma'' \in \mathbb{C}(s) \wedge s \in \mathbb{S}\} && \wr \text{assumption (A1)} \wr \\
= \ & (\biguplus\{\mathbb{I}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma' \sigma'') \mid \sigma' \in \mathbb{C}(\sigma) \wedge \sigma'' \in \mathbb{C}(s) \wedge s \in \mathbb{S} \wedge |\sigma''| = 1\}) \\
& \uplus (\biguplus\{\mathbb{I}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma' \sigma'') \mid \sigma' \in \mathbb{C}(\sigma) \wedge \sigma'' \in \mathbb{C}(s) \wedge s \in \mathbb{S} \wedge |\sigma''| = 0\}) \\
& \uplus (\biguplus\{\mathbb{I}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma' \sigma'') \mid \sigma' \in \mathbb{C}(\sigma) \wedge \sigma'' \in \mathbb{C}(s) \wedge s \in \mathbb{S} \wedge |\sigma''| > 1\})
\end{aligned}
$$

In the above, the formula is split into 3 cases by the length of σ''. The first case:

$$\biguplus\{\mathbb{I}(\llbracket P \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma'\sigma'') \mid \sigma' \in \mathbb{C}(\sigma) \wedge \sigma'' \in \mathbb{C}(s) \wedge s \in \mathbb{S} \wedge |\sigma''| = 1\}$$

$$= \biguplus\{\mathbb{I}(\llbracket P \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma' s) \mid \sigma' \in \mathbb{C}(\sigma) \wedge s \in \mathbb{S}\} \qquad \text{(corollary 5)}$$

$$= \biguplus\{\mathbb{I}(\llbracket P \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma') \mid \sigma' \in \mathbb{C}(\sigma)\} \qquad \text{(corollary 4)}$$

$$= \mathbb{O}(\llbracket P \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma) \qquad \text{(def. } \mathbb{O}\text{)}$$

The second case: if there is $s \in \mathbb{S}$ such that $\varepsilon \in \mathbb{C}(s)$, then $\biguplus\{\mathbb{I}(\llbracket P \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma'\sigma'') \mid \sigma' \in \mathbb{C}(\sigma) \wedge \sigma'' \in \mathbb{C}(s) \wedge s \in \mathbb{S} \wedge |\sigma''| = 0\} = \biguplus\{\mathbb{I}(\llbracket P \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma') \mid \sigma' \in \mathbb{C}(\sigma)\} = \mathbb{O}(\llbracket P \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma)$. Otherwise, it is an empty set.

The third case:

$$\biguplus\{\mathbb{I}(\llbracket P \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma'\sigma'') \mid \sigma' \in \mathbb{C}(\sigma) \wedge \sigma'' \in \mathbb{C}(s) \wedge s \in \mathbb{S} \wedge |\sigma''| > 1\}$$

$$\subseteq \biguplus\{\mathbb{I}(\llbracket P \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma') \mid \sigma' \in \mathbb{C}(\sigma) \wedge \sigma'' \in \mathbb{C}(s) \wedge s \in \mathbb{S} \wedge |\sigma''| > 1\} \qquad \text{(lemma 2)}$$

$$\subseteq \biguplus\{\mathbb{I}(\llbracket P \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma') \mid \sigma' \in \mathbb{C}(\sigma)\} \qquad \text{(def. } \biguplus\text{)}$$

$$= \mathbb{O}(\llbracket P \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma) \qquad \text{(def. } \mathbb{O}\text{)}$$

Joining the above three cases together, we have proved that

$$\biguplus_{\sigma s \in \llbracket P \rrbracket^{\mathsf{Pref}}} \mathbb{O}(\llbracket P \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma s) = \mathbb{O}(\llbracket P \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma). \qquad \square$$

Lemma 3 *Given the semantics* $\llbracket P \rrbracket^{\mathsf{Max}}$*, lattice* $\mathcal{L}^{\mathsf{Max}}$ *of system behaviors and cognizance function* $\mathbb{C}$*, the observation function* $\mathbb{O}(\llbracket P \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C})$ *is decreasing on the observed trace* σ*: the greater (longer)* σ *is, the stronger property it can observe. I.e.* $\forall \sigma, \sigma' \in \mathbb{S}^{*\infty}.\ \sigma \preceq \sigma' \Rightarrow \mathbb{O}(\llbracket P \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma) \supseteq \mathbb{O}(\llbracket P \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma')$.

Proof. We only need to consider the case where $\sigma \prec \sigma'$. First, if σ is invalid (i.e. $\sigma \notin [\![\mathrm{P}]\!]^{\mathsf{Pref}}$), then every trace σ' that is greater than σ must also be invalid (i.e. $\sigma' \notin [\![\mathrm{P}]\!]^{\mathsf{Pref}}$), hence it is easy to find that $\mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma) = \mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma') = \bot^{\mathsf{Max}}$.

Second, if $\sigma' \notin [\![\mathrm{P}]\!]^{\mathsf{Pref}}$, then we have $\mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma') = \bot^{\mathsf{Max}}$. Hence, it is trivial to find $\mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma) \supseteq \bot^{\mathsf{Max}} = \mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma')$.

Last, if $\sigma, \sigma' \in [\![\mathrm{P}]\!]^{\mathsf{Pref}}$, then σ must be a valid non-maximal trace, i.e. $\sigma \in [\![\mathrm{P}]\!]^{\mathsf{Pref}} \backslash [\![\mathrm{P}]\!]^{\mathsf{Max}}$. From corollary 7, it is easy to see $\forall s \in \mathbb{S}.\ \mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma) \supseteq \mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma s)$. Since σ' is greater than σ(or say, σ' is a prolongation of σ with states), then by the transitivity of $\supseteq$, it is not hard to see that $\mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma) \supseteq \mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma')$. □

Example 18 (Access Control, Continued) *For an omniscient observer, the observation function is identical to the inquiry function in Example 16. If the cognizance of a non-omniscient observer defined in Example 17 is adopted, we get an observation function that works exactly the same as the dashed arrows in Fig. 5.1:*

- $\mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \langle \ell_1,\ \rho_1\rangle\langle \ell_2,\ \rho_2 = \rho_1[\mathit{apv} \mapsto 1]\rangle\langle \ell_3,\ \rho_3 = \rho_2[\mathit{i1} \mapsto 0]\rangle) =$ $\biguplus\{\mathbb{I}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \langle \ell_1,\ \rho_1\rangle\langle \ell_2,\ \rho_2 = \rho_1[\mathit{apv} \mapsto 1]\rangle\langle \ell_3,\ \rho_3 = \rho_2[\mathit{i1} \mapsto v]\rangle) \mid v \in \{\text{-}1, 0, 1, 2\}\} = \mathit{AF} \uplus \mathit{AF} \uplus \top^{\mathsf{Max}} \uplus \top^{\mathsf{Max}} = \top^{\mathsf{Max}}$*, i.e. even if the 1st admin already inputs* 0*, only* $\top^{\mathsf{Max}}$ *can be guaranteed from the perspective of the non-omniscient observer.*

- $\mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \langle \ell_1,\ \rho_1\rangle\langle \ell_2,\ \rho_2 = \rho_1[\mathit{apv} \mapsto 1]\rangle\langle \ell_3,\ \rho_3 = \rho_2[\mathit{i1} \mapsto 0]\rangle\langle \ell_4,\ \rho_4 = \rho_3\rangle\langle \ell_5,\ \rho_5 = \rho_4[\mathit{i2} \mapsto 0]\rangle) = \biguplus\{\mathbb{I}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \langle \ell_1,\ \rho_1\rangle\langle \ell_2,\ \rho_2 = \rho_1[\mathit{apv} \mapsto 1]\rangle\langle \ell_3,\ \rho_3 = \rho_2[\mathit{i1} \mapsto v]\rangle\langle \ell_4,\ \rho_4 = \rho_3\rangle\langle \ell_5,\ \rho_5 = \rho_4[\mathit{i2} \mapsto 0]\rangle) \mid v \in \{\text{-}1, 0, 1, 2\}\} = \mathit{AF} \uplus \mathit{AF} \uplus \mathit{AF} \uplus \mathit{AF} = \mathit{AF}$*, i.e. only after the 2nd admin inputs* 0 *(or* -1*), "Access Failure" AF can be guaranteed from the perspective of the non-omniscient observer.*

– $\mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \langle \ell_1,\ \rho_1\rangle\langle \ell_2,\ \rho_2 = \rho_1[apv \mapsto 1]\rangle\langle \ell_3,\ \rho_3 = \rho_2[i1 \mapsto 0]\rangle\langle \ell_4,\ \rho_4 = \rho_3\rangle\langle \ell_5,\ \rho_5 = \rho_4[i2 \mapsto 1]\rangle) = \uplus\{\mathbb{I}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \langle \ell_1,\ \rho_1\rangle\langle \ell_2,\ \rho_2 = \rho_1[apv \mapsto 1]\rangle\langle \ell_3,\ \rho_3 = \rho_2[i1 \mapsto v]\rangle\langle \ell_4,\ \rho_4 = \rho_3\rangle\langle \ell_5,\ \rho_5 = \rho_4[i2 \mapsto 1]\rangle) \mid v \in \{\text{-}1, 0, 1, 2\}\} = AF \uplus AF \uplus \top^{\mathsf{Max}} \uplus \top^{\mathsf{Max}} = \top^{\mathsf{Max}}$*, i.e. if the 2nd admin inputs* 1 *(or* 2*), only the top* $\top^{\mathsf{Max}}$ *can be guaranteed from the perspective of the non-omniscient observer, even if the 1st admin already inputs* 0 *or* -1. □

5.4 Formal Definition of Responsibility

Using the three components of responsibility analysis introduced above, responsibility is formally defined as the *responsibility abstraction* α_R in (5.5). Specifically, the first parameter is the maximal trace semantics $[\![\mathrm{P}]\!]^{\mathsf{Max}}$, the second parameter is the lattice $\mathcal{L}^{\mathsf{Max}}$ of system behaviors, the third parameter is the cognizance function of a given observer, the fourth parameter is the behavior $\mathcal{B}$ whose responsibility is of interest, and the last parameter is the analyzed traces $\mathcal{T}$.

For every trace $\sigma \in \mathcal{T}$ to be analyzed, we split it into three parts such that $\sigma = \sigma_{\mathrm{H}}\tau_{\mathrm{R}}\sigma_{\mathrm{F}}$, where $\sigma_{\mathrm{H}} = s_0 \cdots s_{r-1} \in \mathbb{S}^*$ represents the *History* part of trace σ, the transition $\tau_{\mathrm{R}} = s_{r-1} \xrightarrow{a_{\mathrm{R}}} s_r$ represents the *Responsible* part of trace σ (which is a transition between two states, and the corresponding action a_{R} can be retrieved from the source code), and $\sigma_{\mathrm{F}} = s_r \cdots \in \mathbb{S}^{*\infty}$ represents the *Future* part of trace σ.

If $\emptyset \subsetneq \mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma_{\mathrm{H}}\tau_{\mathrm{R}}) \subseteq \mathcal{B} \wedge \mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma_{\mathrm{H}}) \not\subseteq \mathcal{B}$ holds, then σ_{H} does not guarantee the behavior $\mathcal{B}$, while $\sigma_{\mathrm{H}}\tau_{\mathrm{R}}$ guarantees a behavior which is at least as strong as $\mathcal{B}$ and is not the invalid trace property represented by $\bot^{\mathsf{Max}} = \emptyset$. Therefore,

to the cognizance $\mathbb{C}$ of a given observer, the transition $\tau_{\mathrm{R}} = s_{r-1} \xrightarrow{a_{\mathrm{R}}} s_r$ (or say, the action a_{R}) is said to be *responsible* for the behavior $\mathcal{B}$ in the trace $\sigma_{\mathrm{H}}\tau_{\mathrm{R}}\sigma_{\mathrm{F}}$.

Responsibility Abstraction α_R

$$\begin{array}{l}
\alpha_R \in \wp(\mathbb{S}^{*\infty}) \mapsto \wp(\wp(\mathbb{S}^{*\infty})) \mapsto (\mathbb{S}^{*\infty} \mapsto \wp(\mathbb{S}^{*\infty})) \mapsto \wp(\mathbb{S}^{*\infty}) \mapsto \wp(\mathbb{S}^{*\infty}) \\
\qquad \mapsto \wp(\mathbb{S}^{*} \times (\mathbb{S} \times \mathbb{S}) \times \mathbb{S}^{*\infty}) \qquad (5.5) \\
\alpha_R([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \mathcal{B}, \mathcal{T}) \triangleq \\
\quad let\ \alpha_{\mathsf{Pred}}(\mathcal{S})\mathcal{T} = \{\sigma \in \mathsf{Pref}(\mathcal{T}) \mid \forall \sigma' \in \mathcal{S}.\ \sigma \preceq \sigma' \Rightarrow \sigma' \in \mathcal{T}\}\ in \\
\quad\quad let\ \mathbb{I}(\mathcal{S}, \mathcal{L}, \sigma) = \curlywedge\{\mathcal{T} \in \mathcal{L} \mid \sigma \in \alpha_{\mathsf{Pred}}(\mathcal{S})\mathcal{T}\}\ in \\
\quad\quad\quad let\ \mathbb{O}(\mathcal{S}, \mathcal{L}, \mathbb{C}, \sigma) = \uplus\{\mathbb{I}(\mathcal{S}, \mathcal{L}, \sigma') \mid \sigma' \in \mathbb{C}(\sigma)\}\ in \\
\quad\quad\quad\quad \{\langle \sigma_{\mathrm{H}},\ \tau_{\mathrm{R}},\ \sigma_{\mathrm{F}} \rangle \mid \sigma_{\mathrm{H}}\tau_{\mathrm{R}}\sigma_{\mathrm{F}} \in \mathcal{T} \ \wedge\ \emptyset \subsetneq \mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma_{\mathrm{H}}\tau_{\mathrm{R}}) \subseteq \mathcal{B} \ \wedge \\
\quad\quad\quad\quad\quad\quad \mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma_{\mathrm{H}}) \not\subseteq \mathcal{B}\}
\end{array}$$

Since $\alpha_R([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \mathcal{B})$ preserves joins on analyzed traces $\mathcal{T}$, we have a Galois connection: $\langle \wp(\mathbb{S}^{*\infty}),\ \subseteq \rangle \underset{\alpha_R([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \mathcal{B})}{\overset{\gamma_R([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \mathcal{B})}{\leftrightarrows}} \langle \wp(\mathbb{S}^{*} \times (\mathbb{S} \times \mathbb{S}) \times \mathbb{S}^{*\infty}),\ \subseteq \rangle$.

It is worthy noting that, compared with our original definition of responsibility abstraction α_R in [24, 33] (which adopts the condition $\emptyset \subsetneq \mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma_{\mathrm{H}}\tau_{\mathrm{R}}) \subseteq \mathcal{B} \subsetneq \mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma_{\mathrm{H}})$), the definition 5.5 proposed in this dissertation is more generic: when the lattice of system behavior $\mathcal{L}^{\mathsf{Max}}$ is of complex structure (i.e. it consists of more than four elements), the observation $\mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma_{\mathrm{H}})$ may return a behavior that is incomparable with $\mathcal{B}$; as long as $\emptyset \subsetneq \mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma_{\mathrm{H}}\tau_{\mathrm{R}}) \subseteq \mathcal{B}$ holds after extending σ_{H} with τ_{R}, we know the transition τ_{R} shall be responsible for $\mathcal{B}$.

Theorem 1 *If τ_{R} is said to be responsible for a behavior $\mathcal{B}$ in a valid trace $\sigma_{\mathrm{H}}\tau_{\mathrm{R}}\sigma_{\mathrm{F}}$, then $\sigma_{\mathrm{H}}\tau_{\mathrm{R}}$ guarantees the occurrence of behavior $\mathcal{B}$, and there must exist another valid prefix trace $\sigma_{\mathrm{H}}\tau'_{\mathrm{R}}$ such that the behavior $\mathcal{B}$ is not guaranteed.*

Proof. First, from the definition of responsibility, we know $\mathbb{O}(\mathcal{S}^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma_{\mathrm{H}}\tau_{\mathrm{R}}) \subseteq \mathcal{B}$.

By corollary 6, $\sigma_{\mathrm{H}}\tau_{\mathrm{R}}$ guarantees the satisfaction of $\mathbb{O}(\mathcal{S}^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma_{\mathrm{H}}\tau_{\mathrm{R}})$, which is at least as strong as $\mathcal{B}$. Thus, the occurrence of behavior $\mathcal{B}$ is guaranteed.

Second, we prove by contradiction. Assume that every valid trace $\sigma_{\mathrm{H}}\tau'_{\mathrm{R}}$ guarantees the occurrence of behavior $\mathcal{B}$ (i.e. $\forall \sigma_{\mathrm{H}}\tau'_{\mathrm{R}} \in \mathcal{S}^{\mathsf{Pref}}.\ \mathbb{O}(\mathcal{S}^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma_{\mathrm{H}}\tau'_{\mathrm{R}}) \subseteq \mathcal{B}$). By corollary 7, we can prove that $\mathbb{O}(\mathcal{S}^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma_{\mathrm{H}}) \subseteq \mathcal{B}$, which contradicts with the condition $\mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma_{\mathrm{H}}) \not\subseteq \mathcal{B}$ for τ_{R} to be responsible for the behavior $\mathcal{B}$. □

Now recall the three essential characteristics for defining responsibility (i.e. the temporal ordering of actions, free choices and the observer's cognizance) in section 4.1. It is obvious that the responsibility abstraction α_R has taken both the temporal ordering of actions and the observer's cognizance into account. As for the free choices, from theorem 1 it is easy to find that, if the transition τ_{R} is completely determined by its history trace σ_{H} and is not free to make choices (i.e. $\forall \sigma_{\mathrm{H}}\tau_{\mathrm{R}}, \sigma_{\mathrm{H}}\tau'_{\mathrm{R}} \in [\![\mathrm{P}]\!]^{\mathsf{Pref}}.\ \tau_{\mathrm{R}} = \tau'_{\mathrm{R}}$), then τ_{R} cannot be responsible for any behavior in the trace $\sigma_{\mathrm{H}}\tau_{\mathrm{R}}\sigma_{\mathrm{F}}$.

5.5 Concrete Responsibility Analysis

To sum up, the responsibility analysis in the concrete typically consists of four steps: **I)** collect the system's trace semantics $[\![\mathrm{P}]\!]^{\mathsf{Max}}$ (in Section 1.2 and 5.1); **II)** build the lattice of system behaviors of interest $\mathcal{L}^{\mathsf{Max}}$ (in Section 5.2.2); **III)** derive an inquiry function $\mathbb{I}$ from $\mathcal{L}^{\mathsf{Max}}$ (in Section 5.3.1), define a cognizance function $\mathbb{C}$ for each observer (in Section 5.3.2), and create the corresponding observation function $\mathbb{O}$ (in Section 5.3.3); **IV)** specify the behavior $\mathcal{B} \in \mathcal{L}^{\mathsf{Max}}$ of interest and the analyzed traces $\mathcal{T} \in \wp([\![\mathrm{P}]\!]^{\mathsf{Max}})$, and apply the responsibility abstraction $\alpha_R([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \mathcal{B}, \mathcal{T})$ to get the analysis result (in Section 5.4). Hence, the responsibility analysis is essentially an abstract interpretation

of the program trace semantics.

Moreover, in the definition 5.5 of responsibility, the sets of traces involved in the trace semantics, system behaviors and the cognizance function are concrete. For the simple access control program example, such concrete traces are explicitly displayed for the sake of clarity. However, they are uncomputable in general, and we cannot require the user to directly provide concrete traces in the implementation of responsibility analysis. To solve this problem, an abstract responsibility analysis that can soundly over-approximate the concrete responsibility analysis results is proposed in part III.

Example 19 (Access Control, Continued) *Using the observation functions in example 18, the abstraction α_R can analyze the responsibility of any behavior $\mathcal{B}$ in the specified set $\mathcal{T}$ of traces. If we would like to analyze "Access Failure" in every possible execution, then $\mathcal{B}$ is set as AF, and $\mathcal{T}$ includes all valid maximal traces, i.e. $\mathcal{T} = [\![\mathrm{P}]\!]^{\mathsf{Max}}$. Thus, by the responsibility abstraction $\alpha_R([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, AF, [\![\mathrm{P}]\!]^{\mathsf{Max}})$, we could compute the responsibility analysis result, which is essential the same as desired in Example 12 and omitted here.*

In addition, if we would like to analyze the responsibility of "Read and Write access is granted", then the behavior of interest $\mathcal{B}$ shall be replaced by RW instead, and we can get the following result. To the cognizance of an omniscient observer, in every execution that both two admins input 1 or 2, the input from system settings (i.e. typ $:= [1; 2]$) is responsible for RW. Meanwhile, to the cognizance of the non-omniscient observer who is unaware of the input from 1st admin, no one would be found responsible for RW, because whether the write access is granted or not is always uncertain due to the unknown input from 1st admin. □

Chapter 6

Applications of Responsibility Analysis

Responsibility is a broad concept, and our definition of responsibility based on the abstraction of trace semantics is applicable in various scientific fields. We have examined every example supplied in actual cause [47, 48] and found that our definition of responsibility can handle them well, in which events like "drop a lit match in the forest" or "throw a rock at the bottle" are treated as actions along the trace.

In this chapter, we focus on analyzing computer programs, and illustrate the application of responsibility analysis by three more examples: (i) the "negative balance" problem of a withdrawal transaction, which can be equivalently viewed as the "buffer overflow" problem; (ii) a program with "division by zero" error, which can be also interpreted as a scenario of "login attack"; and (iii) the "information leakage" problem. It is worthy noting that, for any behavior $\mathcal{B}$ of interest, our responsibility analysis is designed to analyze the programs where the behavior $\mathcal{B}$ does not always occur, i.e. $\mathcal{B} \subsetneq [\![\mathrm{P}]\!]^{\mathsf{Max}}$. Yet, for the programs where every trace has the behavior $\mathcal{B}$, we need to admit that the responsibility analysis cannot identify any responsible entity, unless "launching the program" is treated

as a separate action and it would be found responsible for $\mathcal{B}$.

6.1 Example of Negative Balance / Buffer Overflow

Consider a withdrawal transaction scenario, which is simplified into a program with only three lines of code as in Fig. 6.1 for the sake of clarity. At point ℓ_1, we read the bank account balance before the withdrawal transaction, which is assumed to be a positive integer or zero; in practice, this read action is typically implemented by a query in the database system. At point ℓ_2, the user inputs the withdrawal amount, which is assumed to be a strictly positive integer. At point ℓ_3, we update the bank account balance after the withdrawal transaction by subtracting *num* from *balance*. When the withdrawal transaction completes at point ℓ_4, if the account balance is negative (i.e. *balance* < 0), then it is an error and we would like to detect the responsible entity for it.

ℓ_1 : *balance* $:= [0; \text{INT\_MAX}];$ //Account balance before the transaction
ℓ_2 : *num* $:= [1; \text{INT\_MAX}];$ //Withdrawal amount
ℓ_3 : *balance* $:=$ *balance* $-$ *num*; //Account balance after the transaction
ℓ_4 : //Error if *balance* < 0

Figure 6.1: The Withdrawal Transaction Program with Negative Balance Problem

It is not hard to see that, the "negative balance" problem can be transformed into an equivalent "buffer overflow" problem, where a memory of size *balance* is allocated, the index at *num* $- 1$ is visited, and a buffer overflow error occurs when *balance* $\leq$ *num* $- 1$ holds. Although this problem has been well studied, it suffices to demonstrate the advantages of responsibility analysis over dependency/causality analysis.

In this example, we consider only the cognizance of the omniscient observer, and the responsibility analysis consists of four steps as discussed in section 5.5:

(1) Collect the trace semantics $[\![\mathrm{P}]\!]^{\mathsf{Max}}$. In the withdrawal transaction program, each maximal trace is of length 4, and $[\![\mathrm{P}]\!]^{\mathsf{Max}} = \{\langle \ell_1,\ \rho_1\rangle\langle \ell_2,\ \rho_2\rangle\langle \ell_3,\ \rho_3\rangle\langle \ell_4,\ \rho_4\rangle \mid (\rho_1 \in \mathbb{M}) \wedge (\rho_2 = \rho_1[\textit{balance} \mapsto v] \wedge v \in [0; \mathrm{INT\_MAX}]) \wedge (\rho_3 = \rho_2[\textit{num} \mapsto v'] \wedge v' \in [1; \mathrm{INT\_MAX}]) \wedge (\rho_4 = \rho_3[\textit{balance} \mapsto \rho_3(\textit{balance}) - \rho_3(\textit{num})])\}$ consists of a very large number of traces. For example, $\langle \ell_1,\ \rho_1\rangle\langle \ell_2,\ \rho_2 = \rho_1[\textit{balance} \mapsto 0]\rangle\langle \ell_3,\ \rho_3 = \rho_2[\textit{num} \mapsto 1]\rangle\langle \ell_4, \rho_4 = \rho_3[\textit{balance} \mapsto \text{-}1]\rangle$ denotes a maximal trace such that the balance before the transaction is 0 and the withdrawal amount is 1; and $\langle \ell_1,\ \rho_1\rangle\langle \ell_2,\ \rho_2 = \rho_1[\textit{balance} \mapsto 5]\rangle\langle \ell_3,\ \rho_3 = \rho_2[\textit{num} \mapsto 9]\rangle\langle \ell_4,\ \rho_4 = \rho_3[\textit{balance} \mapsto \text{-}4]\rangle$ denotes a maximal trace such that the balance before the transaction is 5 and the withdrawal amount is 9. Both the above two traces have the negative balance problem.

(2) Build the lattice of system behaviors of interest. Since "negative balance" is the only behavior that we are interested here, we can build the lattice $\mathcal{L}^{\mathsf{Max}}$ with only four elements as in Fig. 6.2, where NB is the set of valid maximal traces where the value of *balance* is negative at point ℓ_4 (i.e. $\mathrm{NB} = \{\sigma \in [\![\mathrm{P}]\!]^{\mathsf{Max}} \mid \exists \rho \in \mathbb{M}.\ \sigma_{[3]} = \langle \ell_4,\ \rho\rangle \wedge \rho(\textit{balance}) < 0\}$), and $\neg$NB is its complement (i.e. $\neg\mathrm{NB} = [\![\mathrm{P}]\!]^{\mathsf{Max}} \backslash \mathrm{NB} = \{\sigma \in [\![\mathrm{P}]\!]^{\mathsf{Max}} \mid \exists \rho \in \mathbb{M}.\ \sigma_{[3]} = \langle \ell_4,\ \rho\rangle \wedge \rho(\textit{balance}) \geq 0\}$).

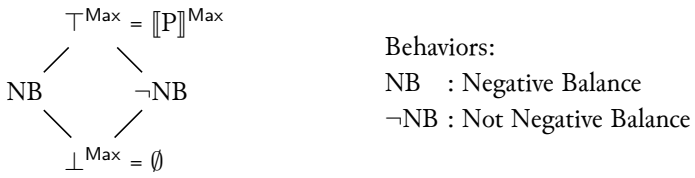

Figure 6.2: Lattice of System Behaviors regarding Negative Balance

(3) Create the observation function. Using the omniscient observer's cognizance $\mathbb{C}_o$ such that $\mathbb{C}_o(\sigma) = \{\sigma\}$, the observation function $\mathbb{O}$ can be easily derived from the lattice $\mathcal{L}^{\mathsf{Max}}$ of system behaviors, such that:

- $\mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}_o, \langle \ell_1,\ \rho_1 \rangle) = \top^{\mathsf{Max}}$, i.e. at the initial point ℓ_1, only the top behavior $\top^{\mathsf{Max}}$ can be guaranteed.
- $\mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}_o, \langle \ell_1,\ \rho_1 \rangle \langle \ell_2,\ \rho_2 = \rho_1[\mathit{balance} \mapsto 0] \rangle) = \mathrm{NB}$, i.e. if the balance before the transaction is 0, the occurrence of "negative balance" is guaranteed even before the withdrawal amount *num* is entered;
- $\mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}_o, \langle \ell_1,\ \rho_1 \rangle \langle \ell_2,\ \rho_2 = \rho_1[\mathit{balance} \mapsto v] \rangle) = \top^{\mathsf{Max}}$ where $v > 0$, i.e. if the balance before the transaction is strictly positive, whether "negative balance" occurs or not is uncertain at point ℓ_2;
- $\mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}_o, \langle \ell_1,\ \rho_1 \rangle \langle \ell_2,\ \rho_2 = \rho_1[\mathit{balance} \mapsto v] \rangle \langle \ell_3,\ \rho_3 = \rho_2[\mathit{num} \mapsto v'] \rangle) =$ NB where $v > 0$ and $v' > v$, i.e. "negative balance" is guaranteed to occur immediately after the value of *num* is set strictly greater than *balance*;
- $\mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}_o, \langle \ell_1,\ \rho_1 \rangle \langle \ell_2,\ \rho_2 = \rho_1[\mathit{balance} \mapsto v] \rangle \langle \ell_3,\ \rho_3 = \rho_2[\mathit{num} \mapsto v'] \rangle) =$ $\neg$NB where $v > 0$ and $v' \leq v$, i.e. "negative balance" is guaranteed not to occur immediately after the value of *num* is set less than or equal to *balance*.

(4) Lastly, by setting the behavior $\mathcal{B} = \mathrm{NB}$ and the analyzed traces $\mathcal{T} = [\![\mathrm{P}]\!]^{\mathsf{Max}}$, the abstraction $\alpha_R([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}_o, \mathcal{B}, \mathcal{T})$ can find: if the balance before the transaction is 0 (e.g. $\langle \ell_1,\ \rho_1 \rangle \langle \ell_2,\ \rho_2 = \rho_1[\mathit{balance} \mapsto 0] \rangle \langle \ell_3,\ \rho_3 = \rho_2[\mathit{num} \mapsto 1] \rangle \langle \ell_4,\ \rho_4 = \rho_3[\mathit{balance} \mapsto \text{-}1] \rangle$), no matter what the withdrawal amount is, the action $\mathit{balance} := [0; \mathrm{INT\_MAX}]$ is responsible for "negative balance"; otherwise, if the balance before the transaction is strictly positive (e.g. $\langle \ell_1,\ \rho_1 \rangle \langle \ell_2,\ \rho_2 = \rho_1[\mathit{balance} \mapsto$

$5]\rangle\langle \ell_3,\ \rho_3 = \rho_2[num \mapsto 9]\rangle\langle \ell_4,\ \rho_4 = \rho_3[balance \mapsto \text{-}4]\rangle$), then the action $num := [1; \text{INT\_MAX}]$ shall take the responsibility.

Using the responsibility analysis result above, we could prevent the "negative balance" behavior by configuring the program (e.g. a test guard for the withdrawal operation), such that the balance before the withdrawal transaction is ensured to be strictly positive, and the withdrawal amount is ensured to be less than or equal to the balance.

6.2 Example of Division by Zero / Login Attack

Consider the program in Fig. 6.3, in which there is obviously a potential division-by-zero error at point ℓ_5. Alternatively, the division-by-zero error can be interpreted as a behavior of "login attack success" by interpreting the program as a simplified login scenario of some complex system for a malicious user (e.g. an attacker attempts to login the account of a normal user in a website).

ℓ_1 : $pwd := [1; \text{INT\_MAX}];$ //The password stored in the system
ℓ_2 : $i1 := [1; \text{INT\_MAX}];$ //The first input from attacker
ℓ_3 : $i2 := [\text{INT\_MIN}; 0];$ //The second input from attacker
ℓ_4 : $res := (pwd - i1) * i2;$ //The attack result: 0 - success, otherwise - failure
ℓ_5 : $check := 1/res;$ //Error if $res = 0$
ℓ_6 :

Figure 6.3: The Program with Division by Zero / Login Attack Problem

More precisely, at point ℓ_1, the program reads the real password of a normal user that is stored in the system, and saves it in the variable pwd. Typically, in practice a password

of valid format consists of letters/numbers and meets the requirement of length, while a password of invalid format contains special characters or does not meet the length requirement. For the sake of simplicity, it is assumed that the passwords of valid format are represented by positive integers in this simplified program, while the passwords of invalid format are represented by zero or negative integers. At point ℓ_2, the input *i1* is used to mimic the attacker's attempt of entering a guessed password that is of valid format (i.e. a positive integer). If the guessed password coincides with the real password *pwd*, then the attacker succeeds to log into the normal user's account. Further, at point ℓ_3, the input *i2* is used to mimic the attacker's attempt of entering a password that is of invalid format (i.e. zero or a negative integer). Specially, the value zero represents a piece of malicious code (e.g. SQL statements) that could bypass the authentication. Thus, the attacker succeeds to log into the normal user's account, if the guessed password coincides with the real password (i.e. $pwd = i1$) or the attacker injects malicious code (i.e. $i2 = 0$). Such an attack is represented by the computation of *res* at point ℓ_4, and the division by zero error at point ℓ_5 represents the behavior of login attack success.

Now the question is: which action is responsible for "login attack success" (or say, "division by zero")? In the following, we illustrate the four steps of responsibility analysis for "login attack success". Different from the analysis of "negative balance" in section 6.1, in this example we shall take the cognizance of an non-omniscient observer.

(1) Collect the trace semantics $[\![\mathrm{P}]\!]^{\mathsf{Max}}$. For the program in Fig. 6.3, each maximal trace is of length 6, and $[\![\mathrm{P}]\!]^{\mathsf{Max}} = \{\langle \ell_1,\ \rho_1\rangle\langle \ell_2,\ \rho_2\rangle\langle \ell_3,\ \rho_3\rangle\langle \ell_4,\ \rho_4\rangle\langle \ell_5,\ \rho_5\rangle\langle \ell_6,\ \rho_6\rangle \mid (\rho_1 \in \mathbb{M}) \wedge (\rho_2 = \rho_1[pwd \mapsto v] \wedge v \in [1; \mathrm{INT\_MAX}]) \wedge (\rho_3 = \rho_2[i1 \mapsto v'] \wedge v' \in [1; \mathrm{INT\_MAX}]) \wedge (\rho_4 = \rho_3[i1 \mapsto v''] \wedge v'' \in [\mathrm{INT\_MIN}; 0]) \wedge (\rho_5 = \rho_4[res \mapsto$

$(\rho_4(\mathit{pwd}) - \rho_4(\mathit{i1})) * \rho_4(\mathit{i2})]) \wedge (\rho_6 = \rho_5[\mathit{check} \mapsto 1 \backslash \rho_5(\mathit{res})])\}$ consists of a large number of traces. For example, $\langle \ell_1,\ \rho_1 \rangle \langle \ell_2,\ \rho_2 = \rho_1[\mathit{pwd} \mapsto 911] \rangle \langle \ell_3,\ \rho_3 = \rho_2[\mathit{i1} \mapsto 911] \rangle \langle \ell_4,\ \rho_4 = \rho_3[\mathit{i2} \mapsto \text{-}5] \rangle \langle \ell_5,\ \rho_5 = \rho_4[\mathit{res} \mapsto 0] \rangle \langle \ell_6,\ \omega \rangle$ denotes a maximal trace such that the guessed password (*i1*) coincides with the real password (*pwd*), and the execution ends with an error state representing "login attack success"; and $\langle \ell_1,\ \rho_1 \rangle \langle \ell_2,\ \rho_2 = \rho_1[\mathit{pwd} \mapsto 911] \rangle \langle \ell_3,\ \rho_3 = \rho_2[\mathit{i1} \mapsto 123] \rangle \langle \ell_4,\ \rho_4 = \rho_3[\mathit{i2} \mapsto 0] \rangle \langle \ell_5,\ \rho_5 = \rho_4[\mathit{res} \mapsto 0] \rangle \langle \ell_6,\ \omega \rangle$ denotes a maximal trace such that the attacker enters a piece of malicious code that bypasses the authentication (i.e. $\mathit{i2} = 0$). Both the above two traces have the behavior of "login attack success".

(2) Build the lattice of system behaviors of interest. Here "login attack success" is the only behavior that we are interested in, and the corresponding lattice $\mathcal{L}^{\mathsf{Max}}$ consists of only four elements as in Fig. 6.4, where AS (login Attack Success) is the set of valid maximal traces where the value of *res* is zero at point ℓ_5 (i.e. $\text{AS} = \{\sigma \in [\![\text{P}]\!]^{\mathsf{Max}} \mid \exists \rho \in \mathbb{M}.\ \sigma_{[4]} = \langle \ell_5,\ \rho \rangle \wedge \rho(\mathit{res}) = 0\}$), and ¬AS (login Attack Failure) is its complement (i.e. $\neg\text{AS} = [\![\text{P}]\!]^{\mathsf{Max}} \backslash \text{AS} = \{\sigma \in [\![\text{P}]\!]^{\mathsf{Max}} \mid \exists \rho \in \mathbb{M}.\ \sigma_{[4]} = \langle \ell_4,\ \rho \rangle \wedge \rho(\mathit{res}) \neq 0\}$).

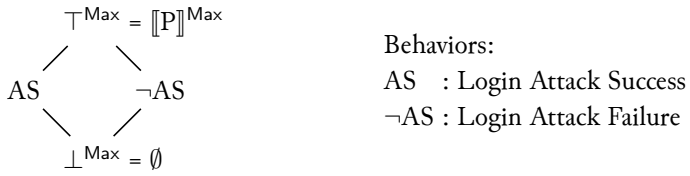

Figure 6.4: Lattice of System Behaviors regarding Login Attack

(3) Create the observation function. In this case, it is intuitive to adopt the cognizance of the attacker, and it is assumed that the attacker does not know the real password of

the normal user (otherwise there is no way to prevent the login attack). Hence, a non-omniscient cognizance shall be designed such that it cannot distinguish the value of *pwd*, e.g. $\langle \ell_1, \rho_1\rangle\langle \ell_2, \rho_2 = \rho_1[\mathit{pwd} \mapsto 123]\rangle \in \mathbb{C}(\langle \ell_1,\ \rho_1\rangle\langle \ell_2,\ \rho_2 = \rho_1[\mathit{pwd} \mapsto 911]\rangle)$ denotes that the attacker does not know whether the real password is 123 or 911. Then, the observation function $\mathbb{O}$ can be derived from the lattice $\mathcal{L}^{\mathsf{Max}}$ of system behaviors and the cognizance function $\mathbb{C}$, such that:

- $\mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \varepsilon) = \mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \langle \ell_1,\ \rho_1\rangle) = \mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \langle \ell_1,\ \rho_1\rangle\langle \ell_2,\ \rho_2 = \rho_1[\mathit{pwd} \mapsto 911]\rangle) = \top^{\mathsf{Max}}$, i.e. before the attacker takes any action at point ℓ_2, only the top behavior $\top^{\mathsf{Max}}$ can be guaranteed.
- $\mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \langle \ell_1,\ \rho_1\rangle\langle \ell_2,\ \rho_2 = \rho_1[\mathit{pwd} \mapsto 911]\rangle\langle \ell_3,\ \rho_3 = \rho_2[\mathit{i1} \mapsto 911]\rangle) = \mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \langle \ell_1,\ \rho_1\rangle\langle \ell_2,\ \rho_2 = \rho_1[\mathit{pwd} \mapsto 911]\rangle\langle \ell_3,\ \rho_3 = \rho_2[\mathit{i1} \mapsto 123]\rangle) = \top^{\mathsf{Max}}$, i.e. after the attacker enters the guessed password, no matter the guessed password coincides with the real password or not, only the top behavior $\top^{\mathsf{Max}}$ can be guaranteed to the cognizance of the attacker. The reason is that the attacker does not know the value of *pwd*, thus cannot ensure her/his guessed password is the same as the real password. More formally, $\mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \langle \ell_1,\ \rho_1\rangle\langle \ell_2,\ \rho_2 = \rho_1[\mathit{pwd} \mapsto 911]\rangle\langle \ell_3,\ \rho_3 = \rho_2[\mathit{i1} \mapsto 911]\rangle) = \mathbb{I}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \langle \ell_2,\ \rho_2 = \rho_1[\mathit{pwd} \mapsto 911]\rangle\langle \ell_3,\ \rho_3 = \rho_2[\mathit{i1} \mapsto 911]\rangle) \uplus \mathbb{I}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \langle \ell_2,\ \rho_2 = \rho_1[\mathit{pwd} \mapsto 123]\rangle\langle \ell_3,\ \rho_3 = \rho_2[\mathit{i1} \mapsto 911]\rangle) \uplus \ldots = \mathrm{AS} \uplus \top^{\mathsf{Max}} = \top^{\mathsf{Max}}$.
- $\mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \langle \ell_1,\ \rho_1\rangle\langle \ell_2,\ \rho_2 = \rho_1[\mathit{pwd} \mapsto 911]\rangle\langle \ell_3,\ \rho_3 = \rho_2[\mathit{i1} \mapsto 911]\rangle\langle \ell_4,\ \rho_4 = \rho_3[\mathit{i2} \mapsto \text{-}5]\rangle) = \top^{\mathsf{Max}}$, i.e. if the second input *i2* from the attacker is not zero, then to the cognizance of the attacker, the behavior of login attack success cannot be guaranteed, even if she/he guesses the correct password in reality.

– $\mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \langle \ell_1,\ \rho_1\rangle\langle \ell_2,\ \rho_2 = \rho_1[\mathit{pwd} \mapsto 911]\rangle\langle \ell_3,\ \rho_3 = \rho_2[\mathit{i1} \mapsto 123]\rangle\langle \ell_4,\ \rho_4 = \rho_3[\mathit{i2} \mapsto 0]\rangle) = \mathrm{AS}$, i.e. only after the attacker enters zero as the second input (or say, succeeds to inject malicious code), then to the cognizance of the attacker, the behavior of login attack success is guaranteed.

(4) Lastly, by setting the behavior $\mathcal{B} = \mathrm{AS}$ and the analyzed traces $\mathcal{T} = [\![\mathrm{P}]\!]^{\mathsf{Max}}$, the abstraction $\alpha_R([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \mathcal{B}, \mathcal{T})$ can find: only the action $\mathit{i2} := [\mathrm{INT\_MIN}; 0]$ representing entering passwords of invalid format is responsible for the behavior "login attack success", and the action $\mathit{i1} := [1; \mathrm{INT\_MAX}]$ representing entering passwords of valid format is not responsible.

Meanwhile, if we take $\neg$AS as the behavior of interest $\mathcal{B}$, then the corresponding responsibility analysis would find that there is no responsible action for $\neg$AS. That is to say, we cannot take any action to prevent the attacker from succeeding to login the system, since there is always a possibility (although it is low) that the attacker succeeds to guess the correct password.

Using the responsibility analysis result above, we could configure the program to exclude the value of zero from the range of second input (or say, we forbid the attacker to enter malicious code like SQL statements), so the attacker can never ensure to login the account of a normal user in the system.

6.3 Example of Information Leakage

From the example of access control in chapter 5 as well as the two examples in section 6.1 and 6.2, it is not hard to see that the responsibility analysis process is essentially the

same for all behaviors, and the only significant distinction among these examples is on defining the behaviors of interest and the cognizance function.

Non-interference. In this section, we consider the responsibility analysis of the behavior "information leakage", which is represented by the notion of *non-interference* [26]. More precisely, the inputs and outputs in the analyzed program are classified as either *Low* (public, low sensitivity) or *High* (private, high sensitivity). For any valid maximal trace $\sigma \in [\![\mathrm{P}]\!]^{\mathsf{Max}}$, if there is another valid maximal trace $\sigma' \in [\![\mathrm{P}]\!]^{\mathsf{Max}}$ such that they have the same low inputs but different low outputs, then the trace σ is said to leak private information, and the analyzed program is possibly insecure. If there is no valid maximal trace in the analyzed program that leaks private information (i.e. every two valid maximal traces with the same low inputs must have the same low outputs, regardless of the high inputs), then the program has the "non-interference" property, hence it is secure.

ℓ_1 : $\mathit{input\_h} := [1; \mathrm{INT\_MAX}];$ //High (private) input
ℓ_2 : $\mathit{input\_l} := [0; 1];$ //Low (public) input
ℓ_3 : $\mathit{output\_l} := [0; 0];$ //Initialization of low (public) output
ℓ_4 : while $(\mathit{input\_l} > 0 \wedge \mathit{input\_h} > 0)$ {
ℓ_5 : $\quad \mathit{output\_l} := \mathit{output\_l} + 1;$
ℓ_6 : $\quad \mathit{input\_h} := \mathit{input\_h} - 1;$ }
ℓ_7 : //Here we output $\mathit{output\_l}$ in public

Figure 6.5: The Program with Potential Information Leakage

Here we take the simple program in Fig. 6.5 as an example, which does not have the desired "non-interference" property. At point ℓ_1, a high (private) input of positive integer is read and saved in the variable $\mathit{input\_h}$. Similarly, at point ℓ_2, a low (public) input is

stored in the variable *input_ℓ*, which is assumed to be either zero or one. At point ℓ_3, a variable *output_ℓ* is initialized as zero. After the execution of the while loop between points ℓ_4 and ℓ_7, the value of *output_ℓ* is output as low (public). It is not hard to find that, although there is no direct data flow from *input_ℋ* to *output_ℓ* (e.g. an assignment *output_ℓ* := *input_ℋ*) in the program, the low output *output_ℓ* at point ℓ_7 is equal to the high input, if the value of low input *input_ℓ* is 1 at point ℓ_3. Therefore, there is a potential behavior of information leakage from *input_ℋ* to *output_ℓ* in this program.

Similar to previous examples, the responsibility analysis of information leakage consists of four steps, and we adopt the cognizance of omniscient observer.

(1) Collect the trace semantics $[\![\mathrm{P}]\!]^{\mathsf{Max}}$. For the program in Fig. 6.5, $[\![\mathrm{P}]\!]^{\mathsf{Max}}$ consists of $2 \times$ INT_MAX maximal traces, and here we take two of them as examples:

i) $\sigma = \langle \ell_1,\ \rho_1\rangle\langle \ell_2,\ \rho_2 = \rho_1[\mathit{input\_ℋ} \mapsto 2]\rangle\langle \ell_3,\ \rho_3 = \rho_2[\mathit{input\_ℓ} \mapsto 1]\rangle\langle \ell_4,\ \rho_4 = \rho_3[\mathit{output\_ℓ} \mapsto 0]\rangle\langle \ell_5,\ \rho_5 = \rho_4\rangle\langle \ell_6,\ \rho_6 = \rho_5[\mathit{output\_ℓ} \mapsto 1]\rangle\langle \ell_4,\ \rho'_4 = \rho_6[\mathit{input\_ℋ} \mapsto 1]\rangle\langle \ell_5, \rho'_5 = \rho'_4\rangle\langle \ell_6, \rho'_6 = \rho'_5[\mathit{output\_ℓ} \mapsto 2]\rangle\langle \ell_4, \rho''_4 = \rho'_6[\mathit{input\_ℋ} \mapsto 0]\rangle\langle \ell_7, \rho_7 = \rho''_4\rangle$. In this trace, the high input is 2, and the low input is 1. After two iterations of the while loop, the value of *output_ℓ* is assigned to 2, which is equal to the high input.

ii) $\sigma' = \langle \ell_1,\ \rho_1\rangle\langle \ell_2,\ \rho_2 = \rho_1[\mathit{input\_ℋ} \mapsto 2]\rangle\langle \ell_3,\ \rho_3 = \rho_2[\mathit{input\_ℓ} \mapsto 0]\rangle\langle \ell_4,\ \rho_4 = \rho_3[\mathit{output\_ℓ} \mapsto 0]\rangle\langle \ell_7,\ \rho_7 = \rho_4\rangle$. Different from the previous trace σ, the low input in this trace is 0, such that the while loop is never entered, and the value of *output_ℓ* remains as 0 at point ℓ_7.

(2) Build the lattice of system behaviors of interest. In general, for the responsibility analysis of information leakage, the corresponding lattice $\mathcal{L}^{\mathsf{Max}}$ of system behaviors

consists of four elements as shown in Fig. 6.6.

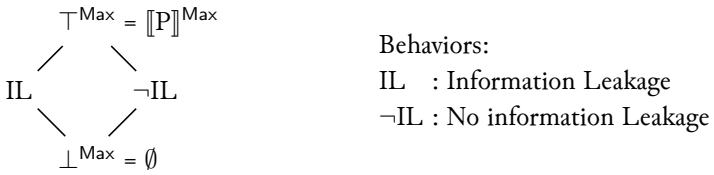

Figure 6.6: Lattice of Behaviors regarding Information Leakage

More specifically, the behavior of "Information Leakage" IL is represented as the set of valid maximal traces that leak private information, i.e. $\mathrm{IL} = \{\sigma \in [\![\mathrm{P}]\!]^{\mathsf{Max}} \mid \exists \sigma' \in [\![\mathrm{P}]\!]^{\mathsf{Max}}.\ \mathrm{low\_inputs}(\sigma) = \mathrm{low\_inputs}(\sigma') \wedge \mathrm{low\_outputs}(\sigma) \neq \mathrm{low\_outputs}(\sigma')\}$, where the functions low_inputs (respectively, low_outputs) collects the list of low inputs (respectively, low outputs) along the trace σ. In contrast, the behavior of "No information Leakage" $\neg$IL is the complement of IL, which is the set of valid maximal traces that do not leak private information, i.e. $\neg\mathrm{IL} = [\![\mathrm{P}]\!]^{\mathsf{Max}} \backslash \mathrm{IL} = \{\sigma \in [\![\mathrm{P}]\!]^{\mathsf{Max}} \mid \forall \sigma' \in [\![\mathrm{P}]\!]^{\mathsf{Max}}.\ \mathrm{low\_inputs}(\sigma) = \mathrm{low\_inputs}(\sigma') \Rightarrow \mathrm{low\_outputs}(\sigma) = \mathrm{low\_outputs}(\sigma')\}$.

For the program in Fig. 6.5, $\mathrm{IL} = \{\sigma \in [\![\mathrm{P}]\!]^{\mathsf{Max}} \mid \exists \rho, \rho' \in \mathbb{M}.\ \sigma_{[1]} = \langle \ell_2,\ \rho\rangle \wedge \sigma_{[|\sigma|-1]} = \langle \ell_7,\ \rho'\rangle \wedge \rho(\mathit{input\_h}) = \rho'(\mathit{output\_l})\} = \{\sigma \in [\![\mathrm{P}]\!]^{\mathsf{Max}} \mid \exists \rho.\ \sigma_{[2]} = \langle \ell_3,\ \rho\rangle \wedge \rho(\mathit{input\_l}) = 1\}$ (i.e. IL is the set of valid maximal traces where the value of *output_l* at ℓ_7 is equal to the high input, which is also the set of valid maximal traces where the value of *input_l* is 1 at ℓ_3); $\neg\mathrm{IL} = \{\sigma \in [\![\mathrm{P}]\!]^{\mathsf{Max}} \mid \exists \rho \in \mathbb{M}.\ \sigma_{[|\sigma|-1]} = \langle \ell_7,\ \rho\rangle \wedge \rho(\mathit{output\_l}) = 0\} = \{\sigma \in [\![\mathrm{P}]\!]^{\mathsf{Max}} \mid \exists \rho.\ \sigma_{[2]} = \langle \ell_3,\ \rho\rangle \wedge \rho(\mathit{input\_l}) = 0\}$ (i.e. $\neg$IL is the set of valid maximal traces where the value of *output_l* is 0 at ℓ_7, which is also the set of valid maximal traces where the value of *input_l* is 0 at ℓ_3).

(3) Create the observation function. Using the omniscient observer's cognizance $\mathbb{C}_o$, the observation function $\mathbb{O}$ can be easily derived from $\mathcal{L}^{\mathsf{Max}}$ such that:

- $\mathbb{O}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}_o, \langle \ell_1,\ \rho_1 \rangle) = \top^{\mathsf{Max}}$, i.e. at the initial point ℓ_1, it is uncertain if the information leakage occurs or not, hence only $\top^{\mathsf{Max}}$ is guaranteed.
- $\mathbb{O}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}_o, \langle \ell_1,\ \rho_1 \rangle \langle \ell_2,\ \rho_2 = \rho_1[\mathit{input\_h} \mapsto v] \rangle) = \top^{\mathsf{Max}}$, i.e. after the high input *input_h* is entered, no matter what value it is, only the top behavior $\top^{\mathsf{Max}}$ can be guaranteed before the low input *input_l* is entered.
- $\mathbb{O}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}_o, \langle \ell_1,\ \rho_1 \rangle \langle \ell_2,\ \rho_2 = \rho_1[\mathit{input\_h} \mapsto v] \rangle) \langle \ell_3,\ \rho_3 = \rho_2[\mathit{input\_l} \mapsto 1] \rangle = \mathrm{IL}$, i.e. the behavior of information leakage is guaranteed to occur immediately after the low input *input_l* is set as 1.
- $\mathbb{O}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}_o, \langle \ell_1,\ \rho_1 \rangle \langle \ell_2,\ \rho_2 = \rho_1[\mathit{input\_h} \mapsto v] \rangle) \langle \ell_3,\ \rho_3 = \rho_2[\mathit{input\_l} \mapsto 0] \rangle = \neg\mathrm{IL}$, i.e. the behavior of information leakage is guaranteed not to occur immediately after the low input *input_l* is set as 0.

(4) Lastly, by setting the behavior $\mathcal{B} = \mathrm{IL}$ and the analyzed traces $\mathcal{T} = \llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}$, the abstraction $\alpha_R(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}_o, \mathcal{B}, \mathcal{T})$ can find that only the action $\mathit{input\_l} := [0; 1]$ representing a low input is responsible for the information leakage, while the action $\mathit{input\_h} := [1; \mathrm{INT\_MAX}]$ representing a high input is not responsible.

After the responsibility analysis of information leakage completes, it is of interest to discuss the procedure of configuring the analyzed program, especially for the programs where the information leakage is acceptable or even desirable under certain circumstances. For instance, imagine a more complex analyzed program that is a social network, where every user can enter some public information (e.g. name, gender) as well as some private

information (e.g. birth date, photos). If the private information of any user called A flows to another user called B (e.g. the user B accesses a photo uploaded by A), then it can be viewed as a behavior "information leakage" IL defined above, and we would like to analyze the corresponding responsibility. After the responsibility analysis is finished, if the responsible entity is determined as an action of A who is the owner of the private information (e.g. A sets her/his own photos public, or A adds B as a friend) or an action of the system administrator, then this information leakage is safe and the corresponding responsible actions can be kept. In contrast, if the responsible entity is determined as an action of B or other unauthorized users (e.g. B exploits a bug of the system such that she/he can access the private information of any other user without authorization), then such an information leakage behavior is undesired, and the corresponding responsible actions shall be eliminated to fix the system.

Part III

Abstract Responsibility Analysis

PART III. ABSTRACT RESPONSIBILITY ANALYSIS

In general, the concrete trace semantics is not computable, thus the concrete responsibility analysis $\alpha_R([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \mathcal{B}, \mathcal{T})$ proposed in part II is undecidable, and we need to propose an abstract responsibility analysis to over-approximate the result of concrete responsibility analysis. In order to do so, the concrete trace semantics is abstracted by trace partitioning automata introduced in the chapter 3, and the behaviors of interest and the cognizance function are specified by abstract invariants as shown in chapter 7. Furthermore, chapter 8 proposes a detailed framework of abstract responsibility analysis, which is based on an iteration of over-approximating forward (possible success) reachability analysis with trace partitioning and under-approximating/over-approximating backward impossible failure accessibility analysis (defined in chapter 2). It is proved that every responsible entity in the concrete must be also found responsible by the abstract responsibility analysis, and the entities that are not found responsible in the abstract cannot be responsible in the concrete.

In practice, in order to improve the efficiency of responsibility analysis, we can preprocess the analyzed program of large size with classic dependency analysis [19, 51, 39, 15] / program slicing techniques [45, 25], and perform the responsibility analysis on the correspondingly generated program slice of smaller size.

Chapter 7

User Specification of Behaviors and Cognizance

In chapter 5, the responsibility is defined as an abstraction $\alpha_R([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \mathcal{B}, \mathcal{T})$, where $[\![\mathrm{P}]\!]^{\mathsf{Max}} \in \wp(\mathbb{S}^{*\infty})$ is the concrete maximal trace semantics, $\mathcal{L}^{\mathsf{Max}} \in \wp(\wp(\mathbb{S}^{*\infty}))$ is a lattice of system behaviors (i.e. trace properties), $\mathbb{C} \in \mathbb{S}^{*\infty} \mapsto \wp(\mathbb{S}^{*\infty})$ is the cognizance function of a given observer, $\mathcal{B} \in \mathcal{L}^{\mathsf{Max}}$ is the behavior whose responsibility is of interest, and $\mathcal{T} \in \wp([\![\mathrm{P}]\!]^{\mathsf{Max}})$ is the set of valid traces to be analyzed.

Among these parameters, the maximal trace semantics $[\![\mathrm{P}]\!]^{\mathsf{Max}}$ is inherent in the given program P, which can be soundly over-approximated by the abstract trace partitioning automata introduced in chapter 3. Meanwhile, all the other parameters indicate the objective of responsibility analysis and can be specified only by users. However, it is difficult, if not impossible, to require users to explicitly specify system behaviors and the cognizance function in the concrete. Therefore, in order to implement the static responsibility analysis, the very first step is to specify $\mathcal{L}^{\mathsf{Max}}$, $\mathbb{C}$, $\mathcal{B}$ and $\mathcal{T}$ in the abstract.

For the sake of simplicity, here it is assumed that we would like to analyze all the maximal traces of P, thus $\mathcal{T} = [\![\mathrm{P}]\!]^{\mathsf{Max}}$ and there is no need for the users to explicitly designate the traces to be analyzed. As for the behavior $\mathcal{B}$ of interest, the lattice $\mathcal{L}^{\mathsf{Max}}$ of behaviors and the cognizance function $\mathbb{C}$, this chapter discusses how to specify them with the abstract invariant domain $\mathcal{D}^\sharp_{\mathbb{I}} = \langle \mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}, \dot{\sqsubseteq}^\sharp_{\mathbb{M}} \rangle$ introduced in section 2.2.3.

7.1 User Specification of Behaviors

7.1.1 The Abstract Behavior of Interest

The behavior of interest is specified by an abstract invariant $\mathcal{B}^\sharp \in \mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}$, which associate every program point with an abstract environment element. The corresponding behavior $\mathcal{B}$ in the concrete is $[\![\mathrm{P}]\!]^{\mathsf{Max}} \cap \gamma_{\mathbb{I}} \circ \dot{\gamma}_{\mathbb{M}}(\mathcal{B}^\sharp) = \{\sigma \in [\![\mathrm{P}]\!]^{\mathsf{Max}} \mid \forall \langle \ell,\ \rho \rangle \in \sigma.\ \rho \in \gamma_{\mathbb{M}}(\mathcal{B}^\sharp(\ell))\}$, i.e. the set of concrete valid maximal traces such that every state satisfies the abstract environment assigned by $\mathcal{B}^\sharp$ at the corresponding program point.

In practice, the user can explicitly designate the chosen program points with some non-trivial abstract environment elements from $\mathcal{D}^\sharp_{\mathbb{M}}$, while all the other program points are implicitly associated with $\top^\sharp_{\mathbb{M}}$.

Example 20 (Access Control, Continued) *Let us consider the access control program in Fig.1.4 again, there are a few behaviors that the user may be interested in: (1) If the user is interested in "the access to o fails", like the abstract postcondition* $\mathsf{I}^\sharp_{\mathsf{post}}$ *defined in example 8, the abstract behavior* $\mathcal{B}^\sharp \in \mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}$ *can be defined such that* $\mathcal{B}^\sharp(\ell_8)$ *is explicitly designated as "acs* $\in [-\infty; 0]$*", while* $\mathcal{B}^\sharp(\ell)$ *is implicitly assigned to* $\top^\sharp_{\mathbb{M}}$ *for other program points* $\ell \neq \ell_8$*. (2) As we have discussed in part II, the responsibility for the complement behavior "the access*

to o succeeds" is different from the one for "the access to o fails". Thus, if the user is interested in "the access to o succeeds" instead, the abstract behavior shall be specified such that $\mathcal{B}^\sharp(\ell_8)$ *is "acs* $\in [1;\infty]$*", while* $\mathcal{B}^\sharp(\ell)$ *is* $\top^\sharp_{\mathbb{M}}$ *for other program points* $\ell \neq \ell_8$*. (3) Similarly, in order to analyze "the read and write access to o is granted" that requires the value of acs is greater than or equal to 2 at point* ℓ_8*, the corresponding abstract behavior* $\mathcal{B}^\sharp$ *shall be specified such that* $\mathcal{B}^\sharp(\ell_8)$ *is "acs* $\in [2;\infty]$*", while* $\mathcal{B}^\sharp(\ell) = \top^\sharp_{\mathbb{M}}$ *for* $\ell \neq \ell_8$*.* □

It is worthy mentioning that, although in the above example there is only one program point that is assigned with non-trivial abstract environment elements, in general the user can express behaviors that are related to multiple program points. However, we have to admit that the expressiveness of abstract behaviors depends on the abstract environment domain $\mathcal{D}^\sharp_{\mathbb{M}}$, and not every concrete behavior (i.e. a set of concrete traces) can be expressed by an abstract behavior. For instance, we cannot express the relation of variables by the interval domain, and it is impossible to express behaviors like "the value of χ is increasing along the execution" by the numerical invariance abstract domains.

In addition, the user specified behavior $\mathcal{B}^\sharp$ is not directly used in the following backward accessibility analysis. Instead, as what we have done for $\mathsf{I}^\sharp_{\mathsf{post}}$ in example 8, the abstract behavior will be refined by the intersection with the abstract forward reachability semantics, which will be further illustrated in chapter 8.

7.1.2 The Lattice of System Behaviors

For the sake of conciseness, it is assumed that the user is interested in analyzing the responsibility of only one behavior, and the corresponding lattice of behaviors in the concrete consists of four elements: the top, the bottom, the behavior of interest, and the

corresponding complement behavior. However, for an abstract behavior $\mathcal{B}^\sharp \in \mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}$, its complement may not be expressible by the abstract invariant domain $\mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}$, since most abstract environment domains (e.g. intervals, octagons, polyhedra) do not support complements. For instance, in general the complement of an interval (e.g. $x \in [0; 9]$) is a disjunction of two intervals; the complement of a polyhedron is a disjunction of affine inequalities, which cannot be expressed by a polyhedron. Therefore, for any lattice of behaviors in the concrete, it may be impossible to construct the corresponding lattice of abstract behaviors, and we cannot require the user to specify such a lattice.

Fortunately, the abstract responsibility analysis introduced latter in chapter 8 does not directly use the lattice of abstract behaviors, and it is sufficient to provide only the abstract behavior $\mathcal{B}^\sharp$ of interest to the analyzer. Nevertheless, in order to prove the soundness of abstract responsibility analysis for a given abstract behavior $\mathcal{B}^\sharp$, the corresponding lattice $\mathcal{L}^{\mathsf{Max}}$ of behaviors in the concrete can be easily built as in Fig. 7.1.

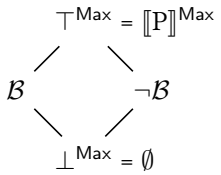

Figure 7.1: The Lattice $\mathcal{L}^{\mathsf{Max}}$ of Behaviors in the Concrete

More precisely, the lattice $\mathcal{L}^{\mathsf{Max}}$ of concrete behaviors consists of four elements: the top $\top^{\mathsf{Max}}$ is the maximal trace semantics $[\![\mathrm{P}]\!]^{\mathsf{Max}}$, the bottom $\bot^{\mathsf{Max}}$ is the empty set, the behavior $\mathcal{B} = [\![\mathrm{P}]\!]^{\mathsf{Max}} \cap \gamma_{\mathbb{I}} \circ \dot{\gamma}_{\mathbb{M}}(\mathcal{B}^\sharp) = \{\sigma \in [\![\mathrm{P}]\!]^{\mathsf{Max}} \mid \forall \langle \ell,\ \rho \rangle \in \sigma.\ \rho \in \gamma_{\mathbb{M}}(\mathcal{B}^\sharp(\ell))\}$, and the complement behavior $\neg\mathcal{B} = [\![\mathrm{P}]\!]^{\mathsf{Max}} \backslash \mathcal{B} = \{\sigma \in [\![\mathrm{P}]\!]^{\mathsf{Max}} \mid \exists \langle \ell,\ \rho \rangle \in \sigma.\ \rho \notin \gamma_{\mathbb{M}}(\mathcal{B}^\sharp(\ell))\}$ is the set of valid maximal traces, in each of which there exist at least one state that do not satisfy the abstract environment assigned by $\mathcal{B}^\sharp$.

Example 21 (Access Control, Continued) *For the access control program, its maximal trace semantics* $[\![\mathrm{P}]\!]^{\mathsf{Max}}$ *is given in example 2. If the behavior of interest is "the access to o fails" (i.e.* $\mathcal{B}^\sharp$ *is specified such that* $\mathcal{B}^\sharp(\ell_8) = \mathit{acs} \in [\text{-}\infty; 0]$*" and* $\mathcal{B}^\sharp(\ell) = \top^\sharp_{\mathbb{M}}$ *for* $\ell \neq \ell_8$*), then the corresponding concrete behavior* $\mathcal{B} = \{\sigma \in [\![\mathrm{P}]\!]^{\mathsf{Max}} \mid \exists \rho \in \mathbb{M}.\ \sigma_{[7]} = \langle \ell_8,\ \rho\rangle \wedge \rho(\mathit{acs}) \leq 0\}$*, and the complement behavior* $\neg\mathcal{B} = \{\sigma \in [\![\mathrm{P}]\!]^{\mathsf{Max}} \mid \exists \rho \in \mathbb{M}.\ \sigma_{[7]} = \langle \ell_8,\ \rho\rangle \wedge \rho(\mathit{acs}) > 0\}$*. Together with the empty set, the four elements form the lattice of behaviors in the concrete.* □

7.2 User Specification of the Cognizance

In the concrete, the cognizance function $\mathbb{C} \in \mathbb{S}^{*\infty} \mapsto \wp(\mathbb{S}^{*\infty})$ of an observer essentially maps a trace σ to an equivalence class $\mathbb{C}(\sigma)$ of traces such that every trace in $\mathbb{C}(\sigma)$ is equivalent (or say, indistinguishable) to σ according to the cognizance of that observer. Specially, for an omniscient observer, every trace is distinguishable from other traces, thus the equivalence class for each trace is a singleton (i.e. $\forall\sigma \in \mathbb{S}^{*\infty}.\ \mathbb{C}_o(\sigma) = \{\sigma\}$). However, it is infeasible to require users to directly provide a cognizance function or an equivalence relation on concrete traces, hence the cognizance function needs to be specified in the abstract instead.

7.2.1 The Abstract Cognizance Function

Formally, the *abstract cognizance function* $\mathbb{C}^\sharp \in \mathbb{L} \mapsto \wp(\mathcal{D}^\sharp_{\mathbb{M}})$ is defined as a function mapping the program point to a set of *cognizance directives* d_c, each of which is an element of the numerical abstract domain $\mathcal{D}^\sharp_{\mathbb{M}}$. It is important to note that, although both the abstract environment element $\mathrm{M}^\sharp$ and the cognizance directive d_c are from the

same abstract domain $\mathcal{D}^\sharp_{\mathbb{M}}$ (e.g. intervals, octagons, polyhedra), their meanings in the concrete are completely different: $\mathrm{M}^\sharp$ represents a set of concrete environments that satisfy a certain property, while d_c essentially defines an equivalence relation on concrete environments, which is further used to define an equivalence relation on concrete traces.

To start with, we give several examples of the abstract cognizance functions and explain their concrete meanings in an informal but intuitive way, while its formal concretization back to the concrete cognizance function is defined in the next paragraphs.

i) Consider an abstract cognizance function $\mathbb{C}^\sharp$ such that $\mathbb{C}^\sharp(\ell) = \{\chi \in [\text{-}\infty; \infty]\}$. When $\chi \in [\text{-}\infty; \infty]$ is treated as an abstract environment $\mathrm{M}^\sharp$, then it represents a set of concrete environments, i.e. $\gamma_{\mathbb{M}}(\mathrm{M}^\sharp) = \mathbb{M}$, which does not provide any non-trivial information. In contrary, if we take $\chi \in [\text{-}\infty; \infty]$ as a cognizance directive, then it actually defines an equivalence relation on environments, such that two environments are equivalent even if their values of χ are different, as long as the values of any other variable (e.g. z) are the same in those two environments. Thus, such an abstract cognizance function $\mathbb{C}^\sharp$ indicates that the observer does not know the value of χ at the program point ℓ, but the value of any other variable.

ii) For another abstract cognizance function such that $\mathbb{C}^\sharp(\ell) = \{\chi \in [\text{-}\infty; -1], \chi \in [0; \infty]\}$, there are two cognizance directives assigned to point ℓ. Take $\chi \in [0; \infty]$ as an example, it does not mean the value of χ is positive or zero at point ℓ. Instead, it means that any two environments ρ and ρ' at point ℓ are equivalent (or indistinguishable), if and only if, the value of χ in both ρ and ρ' are positive or zero (e.g. $\rho(\chi) = 0$ and $\rho'(\chi) = 5$), and the values of any other variable are the same. Similarly, $\chi \in [\text{-}\infty; -1]$, as a cognizance directive, means that two environments ρ and ρ' at ℓ are equivalent, as

long as their values of x are negative (e.g. $\rho(x) = -2$ and $\rho'(x) = -5$) and the values of any other variable are the same. Together, the abstract cognizance function $\mathbb{C}^\sharp$ indicates that the observer does not know the exact value of x at point ℓ, but only the sign of x (i.e. positive or zero, or negative), as well as the exact value of other variables.

iii) The numerical abstract domain used in the previous two examples is the interval domain, and now we consider another example with the octagon/polyhedron domain. Suppose the abstract cognizance function $\mathbb{C}^\sharp$ is specified such that $\mathbb{C}^\sharp(\ell) = \{x \leq y, y < x\}$, then the cognizance directive $x \leq y$ (respectively, $y < x$) means that two environments ρ and ρ' are equivalent, if and only if $\rho(x) \leq \rho(y)$ and $\rho'(x) \leq \rho'(y)$ (respectively, $\rho(y) < \rho(x)$ and $\rho'(y) < \rho'(x)$) hold, and the values of any other variable in ρ and ρ' are the same. That is to say, the observer does not know the exact value of x and y at point ℓ, but the relation between x and y, as well as the exact value of other variables.

In the following, we formalize the equivalence relations introduced by the abstract cognizance function, and define the concretization from the abstract cognizance $\mathbb{C}^\sharp \in \mathbb{L} \mapsto \wp(\mathcal{D}^\sharp_{\mathbb{M}})$ back to the corresponding concrete cognizance $\mathbb{C} \in \mathbb{S}^{*\infty} \mapsto \wp(\mathbb{S}^{*\infty})$.

Equivalence Relation on Environments. Suppose $\mathcal{D}^\sharp_{\mathbb{M}}$ is a numerical abstract domain (e.g. intervals, octagons, polyhedra). For any cognizance directive $d_c \in \mathcal{D}^\sharp_{\mathbb{M}}$, let vars($d_c$) be the set of variables used in d_c. For instance, vars($x \in [-\infty; \infty]$) $= \{x\}$, and vars($x \leq y$) $= \{x, y\}$. Then, for every cognizance directive $d_c \in \mathcal{D}^\sharp_{\mathbb{M}}$, we can define an equivalence relation $\overset{d_c}{\sim}$ on concrete environments as follows:

$$\overset{d_c}{\sim} \quad \in \quad \wp(\mathbb{M} \times \mathbb{M}) \qquad \text{equivalence relation on environments}$$

$$\rho \overset{d_c}{\sim} \rho' \quad \Leftrightarrow \quad \rho = \rho' \vee (\rho \in \gamma_{\mathbb{M}}(d_c) \wedge \rho' \in \gamma_{\mathbb{M}}(d_c) \wedge \forall x \in \mathbb{X} \backslash \text{vars}(d_c).\, \rho(x) = \rho'(x)).$$

That is to say, two environments are equivalent (indistinguishable) according to a

cognizance directive d_c, if and only if, either they are equal to each other, or both of them belong to $\gamma_{\mathbb{M}}(d_c)$ and the values of any variable not used in d_c are the same.

For example, suppose the set of all variables in a program is $\mathbb{X} = \{\mathcal{x}, y\}$, and the cognizance directive d_c is $\mathcal{x} \in [0; \infty]$ from the interval domain such that $\text{vars}(d_c) = \{\mathcal{x}\}$. Let $[\mathcal{x} \mapsto v, y \mapsto v']$ be an environment such that the value of $\mathcal{x}$ is v and the value of y is v'. Then, it is not hard to see that $[\mathcal{x} \mapsto 0, y \mapsto 1] \overset{d_c}{\sim} [\mathcal{x} \mapsto 5, y \mapsto 1]$, since the values of $\mathcal{x}$ in both environments are positive or zero, and the values of y are the same in those two environments. Besides, we have $[\mathcal{x} \mapsto \text{-}1, y \mapsto 1] \overset{d_c}{\not\sim} [\mathcal{x} \mapsto 5, y \mapsto 1]$, since the value of $\mathcal{x}$ is negative in the first environment; and $[\mathcal{x} \mapsto 0, y \mapsto 1] \overset{d_c}{\not\sim} [\mathcal{x} \mapsto 5, y \mapsto 2]$, because the values of y in those two environments are different.

Specially, for the cognizance directive $\bot^\sharp_{\mathbb{M}} \in \mathcal{D}^\sharp_{\mathbb{M}}$, the set of used variables $\text{vars}(\bot^\sharp_{\mathbb{M}})$ is empty, thus two environments cannot be equivalent unless they are equal to each other. That is to say, the special cognizance directive $\bot^\sharp_{\mathbb{M}}$ indicates that every concrete environment is distinguishable from each other.

Equivalence Relation on Traces. Given an abstract cognizance function $\mathbb{C}^\sharp \in \mathbb{L} \mapsto \wp(\mathcal{D}^\sharp_{\mathbb{M}})$, an equivalence relation $\overset{\mathbb{C}^\sharp}{\sim}$ on concrete traces can be defined as follows (where $|\sigma|$ denotes the length of σ, and it is ∞ when the trace σ is infinite):

$$\begin{array}{rcll} \overset{\mathbb{C}^\sharp}{\sim} & \in & \wp(\mathbb{S}^{*\infty} \times \mathbb{S}^{*\infty}) & \text{equivalence relation on traces} \\ \sigma \overset{\mathbb{C}^\sharp}{\sim} \sigma' & \Leftrightarrow & |\sigma| = |\sigma'| \wedge \forall i \in [0, |\sigma|).\ (\sigma_{[i]} = \langle \ell,\ \rho\rangle \wedge \sigma'_{[i]} = \langle \ell',\ \rho'\rangle) & \\ & & \qquad \Rightarrow (\ell = \ell' \wedge (\exists d_c \in \mathbb{C}^\sharp(\ell).\ \rho \overset{d_c}{\sim} \rho')). & \end{array}$$

That is to say, two concrete traces are equivalent (indistinguishable) according to the abstract cognizance $\mathbb{C}^\sharp$, if and only if, they are of the same length and have the same

control flow, and the environments at the same location are equivalent according to some cognizance directive assigned to that point.

For instance, suppose the set of all variables in a program is $\mathbb{X} = \{\mathcal{x}, y\}$, and the abstract cognizance function $\mathbb{C}^\sharp$ is defined such that $\mathbb{C}^\sharp(\ell_1) = \{\bot^\sharp_{\mathbb{M}}\}$ and $\mathbb{C}^\sharp(\ell_2) = \{\mathcal{x} \in [0; \infty]\}$. Then, a trace $\langle \ell_1,\ [\mathcal{x} \mapsto \text{-1}, y \mapsto 1]\rangle \to \langle \ell_2,\ [\mathcal{x} \mapsto 0, y \mapsto 1]\rangle$ is equivalent to another trace $\langle \ell_1,\ [\mathcal{x} \mapsto \text{-1}, y \mapsto 1]\rangle \to \langle \ell_2,\ [\mathcal{x} \mapsto 5, y \mapsto 1]\rangle$, because the two traces have the same control flow, the two environments at point ℓ_1 are equal, and the two environments at point ℓ_2 are equivalent according to the cognizance directive $\mathcal{x} \in [0; \infty]$.

Concretization to the Concrete Cognizance Function. Using the equivalence relation $\overset{\mathbb{C}^\sharp}{\sim}$ introduced by the abstraction $\mathbb{C}^\sharp$, we can define the concretization function:

$$\begin{array}{rcll} \gamma_{\mathbb{C}} & \in & (\mathbb{L} \mapsto \wp(\mathcal{D}^\sharp_{\mathbb{M}})) \mapsto (\mathbb{S}^{*\infty} \mapsto \wp(\mathbb{S}^{*\infty})) & \text{cognizance concretization} \\ \gamma_{\mathbb{C}}(\mathbb{C}^\sharp) & \triangleq & \lambda\sigma \in \mathbb{S}^{*\infty}.\ [\sigma]_{\underset{\sim}{\mathbb{C}^\sharp}} & \\ & = & \lambda\sigma \in \mathbb{S}^{*\infty}.\ \{\sigma' \in \mathbb{S}^{*\infty} \mid \sigma \overset{\mathbb{C}^\sharp}{\sim} \sigma'\}. & \end{array}$$

According to the above definition, for any abstract cognizance function $\mathbb{C}^\sharp$, the corresponding concrete cognizance function maps a trace σ to its equivalence class $[\sigma]_{\underset{\sim}{\mathbb{C}^\sharp}}$, i.e. the set of traces that are $\overset{\mathbb{C}^\sharp}{\sim}$ equivalent to σ.

Here we have to admit that, compared with the concrete cognizance function that could map a trace to an arbitrary set of traces, the expressiveness of our abstract cognizance function is restricted: only traces with the same control flow can be specified as equivalent in the abstract, but it is expressive enough to cover many interesting cases. An alternative way to specify the abstract cognizance function is to use abstract relational invariants, which could express relational properties about two executions of a single program on different inputs [40, 37].

7.2.2 Validating Partitioning Directives with Cognizance

As discussed in chapter 3, the program's trace semantics is soundly over-approximated by trace partitioning automata, which can be computed by the abstract forward (possible success) reachability analysis with trace partitioning. Hence, every valid maximal trace is represented by at least one (and possibly more than one) paths in the automaton, and every path in the automaton represents a set of concrete traces, which may include invalid concrete trace due to the over-approximation.

In order to implement the cognizance function $\mathbb{C}^\sharp$ in the abstract responsibility analysis, the key is to guarantee that: for any two concrete traces σ and σ' that are equivalent (indistinguishable) to each other according to $\mathbb{C}^\sharp$ (i.e. $\sigma \overset{\mathbb{C}^\sharp}{\sim} \sigma'$), they must be represented by the same path in the trace partitioning automaton.

Since the structure of trace partitioning automata is decided by the partitioning directives, we need to make sure that during the execution of any two equivalent traces, every time when a partitioning directive d_p is encountered, the two traces must belong to the same partition (i.e. both of them are in the partition generated by d_p, or neither of them are in the partition generated by d_p). If such a property holds, then the partitioning directive d_p is said to be *valid with respect to the cognizance* $\mathbb{C}^\sharp$ and will be used to generate trace partitioning automata; otherwise, it is *invalid*, and will be either removed or revised before it is used in generating trace partitioning automata.

By the definition of $\overset{\mathbb{C}^\sharp}{\sim}$, it is assumed that two equivalent traces must have the same control flow. Thus, for all partitioning directives related with the control states (e.g. a partitioning directive part$\langle \text{If}, \ell, b\rangle$ that partitions traces by the branch of a conditional), every two equivalent traces are ensured to belong to the same partition. That is to say,

for any cognizance function, all the control state related partitioning directives are valid. Therefore, when implementing the cognizance function in the abstract responsibility analysis, we only need to check the validity of partitioning directives related with memory states (i.e. environments) that is of the form "part$\langle$Inv, ℓ, $\mathrm{M}^\sharp\rangle$", while the directive of the form "part$\langle$Val, ℓ, $\chi = n\rangle$" can be treated as a special case of "part$\langle$Inv, ℓ, $\mathrm{M}^\sharp\rangle$".

In this section, we give a formal definition of the validity of a partitioning directive d_p with respect to a given cognizance directive d_c, and propose a sound approach to check the validity in the abstract.

7.2.2.1 The Definition of Validity of Partitioning Directives

As explained above, all the control state related partitioning directives in Fig. 3.2 are always valid, here we only need to consider the validity of partitioning directives that are related with environments. Intuitively, a partitioning directive $d_p = \mathrm{part}\langle\mathrm{Inv},\ \ell,\ \mathrm{M}_p^\sharp\rangle$ creates a partition at point ℓ such that the environment property $\mathrm{M}_p^\sharp$ holds, and this partition is valid if and only if it does not partition any equivalence class of environments into two separate parts. That is to say, every equivalence class of environments must be either a subset of $\gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp)$ or completely disjoint from $\gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp)$.

Definition 2 *A partitioning directive* $\mathrm{d}_p = \mathit{part}\langle\mathit{Inv},\ \ell,\ \mathrm{M}_p^\sharp\rangle$ *is valid with respect to a cognizance directive* $\mathrm{d}_c \in \mathcal{D}_{\mathbb{M}}^\sharp$ *if and only if*

$$\forall \rho \in \mathbb{M}.\ [\rho]_{\underset{\sim}{\mathrm{d}_c}} \subseteq \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp)\ \vee\ [\rho]_{\underset{\sim}{\mathrm{d}_c}} \cap \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp) = \emptyset \tag{7.1}$$

where $[\rho]_{\underset{\sim}{\mathrm{d}_c}} = \{\rho' \in \mathbb{M} \mid \rho \overset{\mathrm{d}_c}{\sim} \rho'\}$ *and* $\rho \overset{\mathrm{d}_c}{\sim} \rho' \Leftrightarrow \rho = \rho' \vee (\rho \in \gamma_{\mathbb{M}}(\mathrm{d}_c) \wedge \rho' \in \gamma_{\mathbb{M}}(\mathrm{d}_c) \wedge \forall \chi \in \mathbb{X} \backslash \mathit{vars}(\mathrm{d}_c).\ \rho(\chi) = \rho'(\chi))$.

For example, for a cognizance directive $d_c = \mathcal{x} \in [0; \infty]$, the partitioning directives part$\langle$Inv, $\mathcal{l}$, $\mathcal{x} \in$ [-1; ∞]$\rangle$, part$\langle$Inv, $\mathcal{l}$, $\mathcal{x} \in$ [-∞; -2]$\rangle$ and part$\langle$Inv, $\mathcal{l}$, $\mathcal{y} \in [1; \infty]\rangle$ are valid, since none of these partitioning directives would partition any equivalence class incurred by $\overset{d_c}{\sim}$. Meanwhile, partitioning directives part$\langle$Inv, $\mathcal{l}$, $\mathcal{x} \in [1; \infty]\rangle$ and part$\langle$Inv, $\mathcal{l}$, $\mathcal{x} \in$ [-9; 9]$\rangle$ are invalid: for example, $[\mathcal{x} \mapsto 0, \mathcal{y} \mapsto 1]$ is equivalent to $[\mathcal{x} \mapsto 5, \mathcal{y} \mapsto 1]$ according to $\overset{d_c}{\sim}$, but $[\mathcal{x} \mapsto 5, \mathcal{y} \mapsto 1]$ belongs to the partition generated by part$\langle$Inv, $\mathcal{l}$, $\mathcal{x} \in [1; \infty]\rangle$ while $[\mathcal{x} \mapsto 0, \mathcal{y} \mapsto 1]$ does not belong to it.

In practice, it is difficult or even impossible to directly check if the condition (7.1) holds or not, since the number of equivalence classes (or say, the size of quotient set of $\mathbb{M}$ by the equivalence relation $\overset{d_c}{\sim}$) is huge, making the cost of directly checking the condition (7.1) prohibitive. In the following, we try to transfer (7.1) into equivalent forms, which are easier to check in practice.

By the definition of $\overset{d_c}{\sim}$, it is trivial that: for every environment $\rho \in \mathbb{M} \backslash \gamma_{\mathbb{M}}(d_c)$, its equivalence class $[\rho]_{\overset{d_c}{\sim}} = \{\rho\}$. Since a singleton is either a subset of another set or completely disjoint from that set, the condition "$[\rho]_{\overset{d_c}{\sim}} \subseteq \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp) \ \vee \ [\rho]_{\overset{d_c}{\sim}} \cap \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp) = \emptyset$" trivially holds for every partitioning directive part$\langle$Inv, $\mathcal{l}$, $\mathrm{M}_p^\sharp\rangle$ where $\mathrm{M}_p^\sharp \in \mathcal{D}_{\mathbb{M}}^\sharp$.

Therefore, the condition (7.1) is equivalent to the the following simplified one:

$$\forall \rho \in \gamma_{\mathbb{M}}(d_c).\ [\rho]_{\overset{d_c}{\sim}} \subseteq \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp) \ \vee \ [\rho]_{\overset{d_c}{\sim}} \cap \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp) = \emptyset \tag{7.2}$$

Compared with checking the condition (7.1), the cost of checking the condition (7.2) is lower: instead of checking the quotient set of $\mathbb{M}$ by $\overset{d_c}{\sim}$, now we need to check only the quotient set of $\gamma_{\mathbb{M}}(d_c)$ by $\overset{d_c}{\sim}$, whose size is reduced.

Further Refinement on the Definition. First, it is not hard to find that, for any abstract environment element $\mathrm{M}_p^\sharp \in \mathcal{D}_{\mathbb{M}}^\sharp$, we have:

$$\forall \rho \in \mathbb{M}.\ (\forall \mathcal{x} \in \text{vars}(\mathrm{M}_p^\sharp).\ \rho(\mathcal{x}) = \rho'(\mathcal{x})) \Rightarrow (\rho \in \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp) \Leftrightarrow \rho' \in \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp)) \quad (7.3)$$

The intuition is that, whether an environment belongs to $\gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp)$ or not (or say, whether an environment property $\mathrm{M}_p^\sharp$ holds or not) is not affected by the value of variables that are not used in $\mathrm{M}_p^\sharp$. For example, suppose $\mathrm{M}_p^\sharp = \mathcal{x} \in [0; \infty]$ (where trivial constraints like "$y \in [\text{-}\infty; \infty]$" are assumed to be omitted in the abstract environment element), then whether an environment belongs to $\gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp)$ or not is solely decided by the value of $\mathcal{x}$. Hence, if two environments have the same value of $\mathcal{x}$ and may have different values of other variables, then both of them or neither of them belong to $\gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp)$.

Second, given a cognizance directive $d_c \in \mathcal{D}_{\mathbb{M}}^\sharp$ and a partitioning directive $d_p = \text{part}\langle \text{Inv},\ \mathcal{l},\ \mathrm{M}_p^\sharp \rangle$ where $\mathrm{M}_p^\sharp \in \mathcal{D}_{\mathbb{M}}^\sharp$, we define a new equivalence relation $\sim_{\mathrm{M}_p^\sharp \backslash d_c}$ on environments:

$$\begin{array}{rcll} \sim_{\mathrm{M}_p^\sharp \backslash d_c} & \in & \wp(\mathbb{M} \times \mathbb{M}) & \text{equivalence relation on environments} \\ \rho \sim_{\mathrm{M}_p^\sharp \backslash d_c} \rho' & \Leftrightarrow & \rho = \rho' \vee (\rho \in \gamma_{\mathbb{M}}(d_c) \wedge \rho' \in \gamma_{\mathbb{M}}(d_c) \wedge & \\ & & \quad \forall \mathcal{x} \in \text{vars}(\mathrm{M}_p^\sharp) \backslash \text{vars}(d_c).\ \rho(\mathcal{x}) = \rho'(\mathcal{x})). & \end{array}$$

It is obvious that the size of each equivalence class by $\sim_{\mathrm{M}_p^\sharp \backslash d_c}$ is greater than $\overset{d_c}{\sim}$:

$$\forall \rho \in \mathbb{M}.\ [\rho]_{\overset{d_c}{\sim}} \subseteq [\rho]_{\sim_{\mathrm{M}_p^\sharp \backslash d_c}} \quad (7.4)$$

where $[\rho]_{\overset{d_c}{\sim}} = \{\rho' \in \mathbb{M} \mid \rho \overset{d_c}{\sim} \rho'\}$ and $[\rho]_{\sim_{\mathrm{M}_p^\sharp \backslash d_c}} = \{\rho' \in \mathbb{M} \mid \rho \sim_{\mathrm{M}_p^\sharp \backslash d_c} \rho'\}$.

Corollary 8 $\forall \rho \in \mathbb{M}.\ \forall \rho' \in [\rho]_{\sim_{\mathrm{M}_p^\sharp \backslash \mathrm{d}_c}}.\ \exists \rho'' \in [\rho]_{\overset{d_c}{\sim}}.\ \forall \mathcal{x} \in \mathit{vars}(\mathrm{M}_p^\sharp).\ \rho'(\mathcal{x}) = \rho''(\mathcal{x})$.

Proof. The key is to prove there exists an environment ρ'' in $[\rho]_{\overset{d_c}{\sim}}$ which satisfies all the requirements. Here we construct $\rho'' = \rho[\forall \mathcal{x} \in \text{vars}(\mathrm{M}_p^\sharp) \cup \text{vars}(d_c).\ \mathcal{x} \mapsto \rho'(\mathcal{x})]$ such that (i) $\forall \mathcal{x} \in \text{vars}(\mathrm{M}_p^\sharp) \cup \text{vars}(d_c).\ \rho'(\mathcal{x}) = \rho''(\mathcal{x})$ and (ii) $\forall \mathcal{x} \in \mathbb{X} \backslash (\text{vars}(\mathrm{M}_p^\sharp) \cup$

$\mathrm{vars}(d_c))$. $\rho(\chi) = \rho''(\chi)$. Thus, the constructed environment ρ'' satisfies the requirement $\forall \chi \in \mathrm{vars}(\mathrm{M}_p^\sharp)$. $\rho'(\chi) = \rho''(\chi)$.

Now we only need to prove that $\rho'' \in [\rho]_{\overset{d_c}{\sim}}$. Since $\rho' \in [\rho]_{\sim_{\mathrm{M}_p^\sharp \backslash d_c}}$, by the definition of $\sim_{\mathrm{M}_p^\sharp \backslash d_c}$, we know that there are two possible cases: the first case is $\rho = \rho'$, then ρ'' is also equal to ρ, which makes $\rho'' \in [\rho]_{\overset{d_c}{\sim}}$ trivial; the second case is $\rho \in \gamma_{\mathbb{M}}(d_c) \wedge \rho' \in \gamma_{\mathbb{M}}(d_c)$ and (iii) $\forall \chi \in \mathrm{vars}(\mathrm{M}_p^\sharp) \backslash \mathrm{vars}(d_c)$. $\rho(\chi) = \rho'(\chi)$. Since $\forall \chi \in \mathrm{vars}(d_c)$. $\rho'(\chi) = \rho''(\chi)$, by (7.3) we can prove that $\rho'' \in \gamma_{\mathbb{M}}(d_c)$ holds. Moreover, combining (i) and (iii) together, we get $\forall \chi \in \mathrm{vars}(\mathrm{M}_p^\sharp) \backslash \mathrm{vars}(d_c)$. $\rho(\chi) = \rho''(\chi)$, which further implies that $\forall \chi \in \mathbb{X} \backslash \mathrm{vars}(d_c)$. $\rho(\chi) = \rho''(\chi)$. By the definition of $\overset{d_c}{\sim}$, we have proved that $\rho'' \in [\rho]_{\overset{d_c}{\sim}}$. □

Last, using the corollary 8 and (7.3), we can prove that the condition (7.2) is equivalent to the condition (7.5), and get the following lemma.

Lemma 4 *A partitioning directive* $\mathrm{d}_p = part\langle Inv, \ell, \mathrm{M}_p^\sharp \rangle$ *is valid with respect to a cognizance directive* $\mathrm{d}_c \in \mathcal{D}_{\mathbb{M}}^\sharp$ *if and only if*

$$\forall \rho \in \gamma_{\mathbb{M}}(\mathrm{d}_c).\ [\rho]_{\sim_{\mathrm{M}_p^\sharp \backslash \mathrm{d}_c}} \subseteq \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp) \ \vee \ [\rho]_{\sim_{\mathrm{M}_p^\sharp \backslash \mathrm{d}_c}} \cap \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp) = \emptyset \tag{7.5}$$

where $[\rho]_{\sim_{\mathrm{M}_p^\sharp \backslash \mathrm{d}_c}} = \{\rho' \in \mathbb{M} \mid \rho \sim_{\mathrm{M}_p^\sharp \backslash \mathrm{d}_c} \rho'\}$ *and* $\rho \sim_{\mathrm{M}_p^\sharp \backslash \mathrm{d}_c} \rho' \Leftrightarrow \rho = \rho' \vee (\rho \in \gamma_{\mathbb{M}}(\mathrm{d}_c) \wedge \rho' \in \gamma_{\mathbb{M}}(\mathrm{d}_c) \wedge \forall \chi \in vars(\mathrm{M}_p^\sharp) \backslash vars(\mathrm{d}_c).\ \rho(\chi) = \rho'(\chi))$.

Proof. To prove that the condition (7.2) is equivalent to the condition (7.5), we first need to show that: $\forall d_c, \mathrm{M}_p^\sharp \in \mathcal{D}_{\mathbb{M}}^\sharp$. $\forall \rho \in \mathbb{M}$. $[\rho]_{\overset{d_c}{\sim}} \subseteq \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp) \Leftrightarrow [\rho]_{\sim_{\mathrm{M}_p^\sharp \backslash d_c}} \subseteq \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp)$. The proof of this statement from right to left is trivial, since $[\rho]_{\overset{d_c}{\sim}} \subseteq [\rho]_{\sim_{\mathrm{M}_p^\sharp \backslash d_c}}$ (7.4). Here we consider the opposite direction: $[\rho]_{\overset{d_c}{\sim}} \subseteq \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp) \Rightarrow [\rho]_{\sim_{\mathrm{M}_p^\sharp \backslash d_c}} \subseteq \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp)$. By the corollary (8), we have $\forall \rho' \in [\rho]_{\sim_{\mathrm{M}_p^\sharp \backslash d_c}}$. $\exists \rho'' \in [\rho]_{\overset{d_c}{\sim}}$. $\forall \chi \in \mathrm{vars}(\mathrm{M}_p^\sharp)$. $\rho'(\chi) = \rho''(\chi)$. Since

the assumption $[\rho]_{\overset{d_c}{\sim}} \subseteq \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp)$ implies that $\rho'' \in \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp)$, then by (7.3), we prove that $\rho' \in \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp)$, which implies that $[\rho]_{\sim_{\mathrm{M}_p^\sharp \backslash d_c}} \subseteq \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp)$.

Similarly, we can prove that $[\rho]_{\overset{d_c}{\sim}} \cap \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp) = \emptyset \Leftrightarrow [\rho]_{\sim_{\mathrm{M}_p^\sharp \backslash d_c}} \cap \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp) = \emptyset$.

Together, we have proved that $\forall d_c, \mathrm{M}_p^\sharp \in \mathcal{D}_{\mathbb{M}}^\sharp.\ \forall \rho \in \mathbb{M}.\ ([\rho]_{\overset{d_c}{\sim}} \subseteq \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp) \vee [\rho]_{\overset{d_c}{\sim}} \cap \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp) = \emptyset) \Leftrightarrow ([\rho]_{\sim_{\mathrm{M}_p^\sharp \backslash d_c}} \subseteq \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp) \vee [\rho]_{\sim_{\mathrm{M}_p^\sharp \backslash d_c}} \cap \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp) = \emptyset)$. □

Intuitively, compared with checking the condition (7.2), the cost of checking (7.5) is further reduced. Essentially, for both conditions, we need to partition the set of environments $\gamma_{\mathbb{M}}(d_c)$ into equivalence classes, and check if there exists any equivalence class that overlaps with $\gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp)$. Since the definition of $\sim_{\mathrm{M}_p^\sharp \backslash d_c}$ is looser than $\overset{d_c}{\sim}$, the size of each equivalence class created by $\sim_{\mathrm{M}_p^\sharp \backslash d_c}$ is larger, thus the number of equivalence classes that need to be checked is smaller.

7.2.2.2 Checking the Validity of Partitioning Directives in the Abstract

In the last section, we have formally defined the validity of a partitioning directive $d_p = \mathrm{part}\langle \mathrm{Inv},\ \ell,\ \mathrm{M}_p^\sharp \rangle$ with respect to a cognizance directive $d_c \in \mathcal{D}_{\mathbb{M}}^\sharp$. However, it is impractical to directly use those definitions to check the validity of partitioning directives, since it requires to compare sets of environments in the concrete. The objective of this section is to propose a sound checking approach, which guarantees that if a partitioning directive is determined as valid in the abstract, then it is indeed valid in the concrete.

To begin with, we consider the abstract environment domains $\mathcal{D}_{\mathbb{M}}^\sharp$ that have a Galois connection with the concrete environment domain, i.e. $\langle \wp(\mathbb{M}),\ \subseteq \rangle \underset{\alpha_{\mathbb{M}}}{\overset{\gamma_{\mathbb{M}}}{\leftrightarrows}} \langle \mathcal{D}_{\mathbb{M}}^\sharp,\ \sqsubseteq_{\mathbb{M}}^\sharp \rangle$. Such abstract domains include but are not limited to the interval domain and the octagon domain. In this case, we have: $\alpha_{\mathbb{M}}([\rho]_{\sim_{\mathrm{M}_p^\sharp \backslash d_c}}) \sqsubseteq_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp \Leftrightarrow [\rho]_{\sim_{\mathrm{M}_p^\sharp \backslash d_c}} \subseteq \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp)$ and

$\alpha_{\mathbb{M}}([\rho]_{\sim_{\mathrm{M}_p^\sharp \backslash d_c}}) \sqcap^\sharp_{\mathbb{M}} \mathrm{M}_p^\sharp = \bot^\sharp_{\mathbb{M}} \Rightarrow [\rho]_{\sim_{\mathrm{M}_p^\sharp \backslash d_c}} \cap \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp) = \emptyset$. Therefore, we can infer a sufficient condition for (7.5) to hold:

$$\forall \rho \in \gamma_{\mathbb{M}}(d_c).\ \alpha_{\mathbb{M}}([\rho]_{\sim_{\mathrm{M}_p^\sharp \backslash d_c}}) \sqsubseteq^\sharp_{\mathbb{M}} \mathrm{M}_p^\sharp \ \vee\ \alpha_{\mathbb{M}}([\rho]_{\sim_{\mathrm{M}_p^\sharp \backslash d_c}}) \sqcap^\sharp_{\mathbb{M}} \mathrm{M}_p^\sharp = \bot^\sharp_{\mathbb{M}} \tag{7.6}$$

More generally, for abstract domains (e.g. the polyhedron domain) that do not have a corresponding abstraction function $\alpha_{\mathbb{M}} \in \wp(\mathbb{M}) \mapsto \mathcal{D}^\sharp_{\mathbb{M}}$, we can use the following condition instead as a sufficient condition to check (7.5):

$$\forall \rho \in \gamma_{\mathbb{M}}(d_c).\ \exists d'_c \in \mathcal{D}^\sharp_{\mathbb{M}}.\ [\rho]_{\sim_{\mathrm{M}_p^\sharp \backslash d_c}} \subseteq \gamma_{\mathbb{M}}(d'_c) \wedge (d'_c \sqsubseteq^\sharp_{\mathbb{M}} \mathrm{M}_p^\sharp \ \vee\ d'_c \sqcap^\sharp_{\mathbb{M}} \mathrm{M}_p^\sharp = \bot^\sharp_{\mathbb{M}}) \tag{7.7}$$

Now the question is: how to find $d'_c \in \mathcal{D}^\sharp_{\mathbb{M}}$ such that $[\rho]_{\sim_{\mathrm{M}_p^\sharp \backslash d_c}} \subseteq \gamma_{\mathbb{M}}(d'_c)$? Suppose $\mathcal{D}^\sharp_{\mathbb{M}}$ is a classic numerical domain (including intervals, octagons, and polyhedra), $\mathrm{vars}(\mathrm{M}_p^\sharp) \backslash \mathrm{vars}(d_c) = \{x_1, \ldots, x_n\}$ that are denoted as $\vec{x}$. Then, for any environment $\rho \in \gamma_{\mathbb{M}}(d_c)$, its equivalence class $[\rho]_{\sim_{\mathrm{M}_p^\sharp \backslash d_c}}$ can be soundly over-approximated by $d'_c = d_c \sqcap^\sharp_{\mathbb{M}} (\vec{x} = \vec{v})$, where $\vec{v}$ is the values of $\vec{x}$ in ρ. Therefore, we can infer another sufficient condition for (7.5) to hold, which is more convenient to check.

Lemma 5 *A partitioning directive* $\mathrm{d}_p = \mathit{part}\langle \mathit{Inv}, \ell, \mathrm{M}_p^\sharp \rangle$ *is valid with respect to a cognizance directive* $\mathrm{d}_c \in \mathcal{D}^\sharp_{\mathbb{M}}$ *if*

$$\forall \vec{v} \in \mathbb{V}^n.\ \mathrm{d}'_c = (\mathrm{d}_c \sqcap^\sharp_{\mathbb{M}} \vec{x} = \vec{v}) \wedge (\mathrm{d}'_c \sqsubseteq^\sharp_{\mathbb{M}} \mathrm{M}_p^\sharp \vee \mathrm{d}'_c \sqcap^\sharp_{\mathbb{M}} \mathrm{M}_p^\sharp = \bot^\sharp_{\mathbb{M}}) \tag{7.8}$$

where $\vec{x} = \mathit{vars}(\mathrm{M}_p^\sharp) \backslash \mathit{vars}(\mathrm{d}_c) = \{x_1, \ldots, x_n\}$.

More specifically, $\vec{x} = \vec{v}$ is expressed as "$x_1 \in [v_1; v_1] \wedge \ldots \wedge x_n \in [v_n; v_n]$" in the interval domain, and as "$x_1 \leq v_1 \wedge -x_1 \leq -v_1 \wedge \ldots \wedge x_n \leq v_n \wedge -x_n \leq -v_n$" in the octagon/polyhedron domain.

However, directly checking the condition (7.8) is still costly, thus we discuss a few special cases that are common and easy to check in practice:

(S1) If $\text{vars}(\mathrm{M}_p^\sharp) \cap \text{vars}(d_c) = \emptyset$ (or say, $\mathrm{M}_p^\sharp$ and d_c do not have commonly used variables, e.g. $\mathrm{M}_p^\sharp = x \leq 1$ and $d_c = y \leq 0$): in this case, $\vec{x} = \text{vars}(\mathrm{M}_p^\sharp) \backslash \text{vars}(d_c) = \text{vars}(\mathrm{M}_p^\sharp)$ includes all the variables used in $\mathrm{M}_p^\sharp$, hence we have $\forall \vec{v} \in \mathbb{V}^n.\ (\vec{x} = \vec{v} \sqsubseteq_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp) \vee (\vec{x} = \vec{v} \sqcap_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp = \bot_{\mathbb{M}}^\sharp)$. Since $(d_c \sqcap_{\mathbb{M}}^\sharp \vec{x} = \vec{v}) \sqsubseteq_{\mathbb{M}}^\sharp \vec{x} = \vec{v}$, the condition (7.8) always holds. Thus, if $\text{vars}(\mathrm{M}_p^\sharp) \cap \text{vars}(d_c) = \emptyset$, then the partitioning directive $d_p = \text{part}\langle \text{Inv}, \ell, \mathrm{M}_p^\sharp \rangle$ is valid with respect to the cognizance directive $d_c \in \mathcal{D}_{\mathbb{M}}^\sharp$.

(S2) If $\text{vars}(\mathrm{M}_p^\sharp) \backslash \text{vars}(d_c) = \emptyset$ (or say, every variable used in $\mathrm{M}_p^\sharp$ is also used in d_c, e.g. $\mathrm{M}_p^\sharp = x \leq 1$ and $d_c = x \leq 0 \wedge y \leq 0$): in this case, $\vec{x} = \text{vars}(\mathrm{M}_p^\sharp) \backslash \text{vars}(d_c) = \emptyset$, hence $d_c' = d_c$ in the condition (7.8). It is obvious that, the condition (7.8) is equivalent to $d_c \sqsubseteq_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp \vee d_c \sqcap_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp = \bot_{\mathbb{M}}^\sharp$. Thus, when $\text{vars}(\mathrm{M}_p^\sharp) \backslash \text{vars}(d_c) = \emptyset$, the partitioning directive $d_p = \text{part}\langle \text{Inv}, \ell, \mathrm{M}_p^\sharp \rangle$ is valid with respect to the cognizance directive $d_c \in \mathcal{D}_{\mathbb{M}}^\sharp$, if and only if, $d_c \sqsubseteq_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp \vee d_c \sqcap_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp = \bot_{\mathbb{M}}^\sharp$ holds.

(S3) If $d_c \sqsubseteq_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp \vee d_c \sqcap_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp = \bot_{\mathbb{M}}^\sharp$ holds: since $d_c' = (d_c \sqcap_{\mathbb{M}}^\sharp \vec{x} = \vec{v}) \sqsubseteq_{\mathbb{M}}^\sharp d_c$, we always have $d_c' \sqsubseteq_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp \vee d_c' \sqcap_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp = \bot_{\mathbb{M}}^\sharp$. Thus, If $d_c \sqsubseteq_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp \vee d_c \sqcap_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp = \bot_{\mathbb{M}}^\sharp$, then the partitioning directive $d_p = \text{part}\langle \text{Inv}, \ell, \mathrm{M}_p^\sharp \rangle$ is valid with respect to the cognizance directive $d_c \in \mathcal{D}_{\mathbb{M}}^\sharp$.

To sum up the lemma 5 and special cases (S1-S3), here we propose a sound approach to check if a partitioning directive $d_p = \text{part}\langle \text{Inv}, \ell, \mathrm{M}_p^\sharp \rangle$ is valid with respect to the cognizance directive $d_c \in \mathcal{D}_{\mathbb{M}}^\sharp$, and formalize it as a function $\text{isValid}_d \in \mathcal{D}_{\mathbb{M}}^\sharp \mapsto (\mathcal{D}_{\mathbb{M}}^\sharp \mapsto \mathbb{B})$ such that $\text{isValid}_d(d_c, \mathrm{M}_p^\sharp)$ returns whether the partitioning directive is valid or not.

bool $\text{isValid}_d(d_c, \mathrm{M}_p^\sharp)$ {

If $(\text{vars}(\mathrm{M}_p^\sharp) \cap \text{vars}(d_c) = \emptyset)$ return true; // Case (S1)

If $(d_c \sqsubseteq_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp \vee d_c \sqcap_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp = \bot_{\mathbb{M}}^\sharp)$ return true; // Case (S3)

If ($\text{vars}(\mathrm{M}_p^\sharp) \backslash \text{vars}(d_c) = \emptyset$) return false; // Case (S2)

Check (7.8) and return the result. // Lemma 5

}

By the proof of lemma 5 and the explanation of (S1-S3), we know that the above approach is sound. More precisely, if the function $\text{isValid}_d(d_c, \mathrm{M}_p^\sharp)$ returns true, then the partitioning directive $d_p = \text{part}\langle \text{Inv}, \ell, \mathrm{M}_p^\sharp \rangle$ must be valid with respect to the cognizance directive $d_c \in \mathcal{D}_{\mathbb{M}}^\sharp$ in the concrete (def. 2).

Special Case of the Interval Domain. Specially, the implementation of $\text{isValid}_d(d_c, \mathrm{M}_p^\sharp)$ can be further simplified, if the abstract environment domain $\mathcal{D}_{\mathbb{M}}^\sharp$ is the interval domain. Since the interval domain cannot express the relation among variables and every element in the interval domain is simply a conjunction of interval constraints on a set of variables, for any $\mathrm{M}_p^\sharp, d_c \in \mathcal{D}_{\mathbb{M}}^\sharp$, the constraints in $\mathrm{M}_p^\sharp$ can be split into two parts: $\mathrm{M}_p^\sharp|_{\text{vars}(\mathrm{M}_p^\sharp)\backslash\text{vars}(d_c)}$ denotes the constraints on the variables in $\text{vars}(\mathrm{M}_p^\sharp)\backslash\text{vars}(d_c)$, and $\mathrm{M}_p^\sharp|_{\text{vars}(\mathrm{M}_p^\sharp)\cap\text{vars}(d_c)}$ denotes the constraints on the variables in $\text{vars}(\mathrm{M}_p^\sharp) \cap \text{vars}(d_c)$. When the set $\text{vars}(\mathrm{M}_p^\sharp)\backslash\text{vars}(d_c)$ (respectively, $\text{vars}(\mathrm{M}_p^\sharp) \cap \text{vars}(d_c)$) is empty, $\mathrm{M}_p^\sharp|_{\text{vars}(\mathrm{M}_p^\sharp)\backslash\text{vars}(d_c)}$ (respectively, $\mathrm{M}_p^\sharp|_{\text{vars}(\mathrm{M}_p^\sharp)\cap\text{vars}(d_c)}$) denotes $\top_{\mathbb{M}}^\sharp$. Then, the condition (7.8) is equivalent to: $\forall \vec{v} \in \mathbb{V}^n.\ (d_c \sqsubseteq_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp|_{\text{vars}(\mathrm{M}_p^\sharp)\cap\text{vars}(d_c)} \wedge \vec{\mathcal{X}} = \vec{v} \sqsubseteq_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp|_{\text{vars}(\mathrm{M}_p^\sharp)\backslash\text{vars}(d_c)}) \vee (d_c \sqcap_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp|_{\text{vars}(\mathrm{M}_p^\sharp)\cap\text{vars}(d_c)} = \bot_{\mathbb{M}}^\sharp \wedge \vec{\mathcal{X}} = \vec{v} \sqcap_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp|_{\text{vars}(\mathrm{M}_p^\sharp)\backslash\text{vars}(d_c)} = \bot_{\mathbb{M}}^\sharp)$.

Since $(\vec{\mathcal{X}} = \vec{v} \sqsubseteq_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp|_{\text{vars}(\mathrm{M}_p^\sharp)\backslash\text{vars}(d_c)}) \vee (\vec{\mathcal{X}} = \vec{v} \sqcap_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp|_{\text{vars}(\mathrm{M}_p^\sharp)\backslash\text{vars}(d_c)} = \bot_{\mathbb{M}}^\sharp)$ always hold in the above condition, the condition (7.8) is equivalent to:

$$d_c \sqsubseteq_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp|_{\text{vars}(\mathrm{M}_p^\sharp)\cap\text{vars}(d_c)} \vee d_c \sqcap_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp|_{\text{vars}(\mathrm{M}_p^\sharp)\cap\text{vars}(d_c)} = \bot_{\mathbb{M}}^\sharp \tag{7.9}$$

and the implementation of $\text{isValid}_d(d_c, \mathrm{M}_p^\sharp)$ for the interval domain could be simplified into checking if the condition (7.9) holds.

For example, if $d_c = \varkappa \in [0;\infty] \wedge y \in [0;\infty]$ and $d_p = \text{part}\langle \text{Inv}, \ell, \mathrm{M}_p^\sharp = y \in [\text{-}5;5] \wedge z \in [\text{-}5;5]\rangle$, then $\mathrm{M}_p^\sharp|_{\text{vars}(\mathrm{M}_p^\sharp)\cap\text{vars}(d_c)} = y \in [\text{-}5;5]$, since $\text{vars}(\mathrm{M}_p^\sharp) \cap \text{vars}(d_c) = \{y\}$. It is not hard to see that $d_c \not\sqsubseteq_{\mathbb{M}}^\sharp y \in [\text{-}5;5]$ and $d_c \sqcap_{\mathbb{M}}^\sharp y \in [\text{-}5;5] = \varkappa \in [0;\infty] \wedge y \in [0;5] \neq \bot_{\mathbb{M}}^\sharp$, thus the condition (7.9) does not hold, and d_p is invalid with respect to d_c.

Example 22 (Checking the Validity of Partitioning Directives) *Here we give some examples of checking the validity of partitioning directive* d_p *with respect to some cognizance directive* d_c *by the approach proposed in this section.*

(1) $\mathrm{d}_c = \varkappa \leq \text{-}1$ *and* $\mathrm{d}_p = \textit{part}\langle \textit{Inv}, \ell, \mathrm{M}_p^\sharp = y \leq 0\rangle$*:* d_c *indicates that the observer does not know the exact value of* $\varkappa$ *if it is negative, and* d_p *would like to generate a partition such that the value of* y *is less than 0. Since* $\textit{vars}(\mathrm{M}_p^\sharp) \cap \textit{vars}(\mathrm{d}_c) = \emptyset$ *(Case (S1)) holds, the partitioning directive* d_p *is valid with respect to* d_c*.*

(2) $\mathrm{d}_c = \varkappa \leq \text{-}1$ *and* $\mathrm{d}_p = \textit{part}\langle \textit{Inv}, \ell, \mathrm{M}_p^\sharp = \varkappa \leq 0\rangle$*:* d_c *indicates that the observer does not know the exact value of* $\varkappa$ *if it is negative, and* d_p *would like to generate a partition such that the value of* $\varkappa$ *is less than 0. It is obvious that* $\mathrm{d}_c \sqsubseteq_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp$*, thus this is the case (S3), and the partitioning directive* d_p *is valid.*

(3) $\mathrm{d}_c = \varkappa \leq 0$ *and* $\mathrm{d}_p = \textit{part}\langle \textit{Inv}, \ell, \mathrm{M}_p^\sharp = \varkappa \leq \text{-}1\rangle$*:* d_c *indicates that the observer does not know the exact value of* $\varkappa$ *if it is negative or zero, and* d_p *would like to generate a partition such that the value of* $\varkappa$ *is negative. In this example,* $\textit{vars}(\mathrm{M}_p^\sharp) \backslash \textit{vars}(\mathrm{d}_c) = \emptyset$*, and It is easy to see that* $\mathrm{d}_c \not\sqsubseteq_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp$ *and* $\mathrm{d}_c \sqcap_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp \neq \bot_{\mathbb{M}}^\sharp$*, thus this is the case (S2), and the partitioning directive* d_p *is invalid with respect to* d_c*.*

(4) $\mathrm{d}_c = \varkappa \leq y$ *and* $\mathrm{d}_p = \textit{part}\langle \textit{Inv}, \ell, \mathrm{M}_p^\sharp = \varkappa \leq z\rangle$*:* d_c *indicates that the observer does not know the exact value of* $\varkappa$ *and* y *when* $\varkappa \leq y$*, but knows the relation between* $\varkappa$ *and* y*; and* d_p *would like to generate a partition such that* $\varkappa \leq z$*. It is not hard to see that none*

of (S1-S3) holds in this example, thus we need to directly check the condition (7.8), which is $\forall v \in \mathbb{V}.\ \mathrm{d}'_c = (x \leq y \wedge z = v) \wedge (\mathrm{d}'_c \sqsubseteq^\sharp_{\mathbb{M}} x \leq z \vee \mathrm{d}'_c \sqcap^\sharp_{\mathbb{M}} x \leq z = \bot^\sharp_{\mathbb{M}})$. *Such a condition does not hold: for example, if* $v = 0$, *then* $\mathrm{d}'_c = (x \leq y \wedge z = 0)$, *hence we have* $\mathrm{d}_c \not\sqsubseteq^\sharp_{\mathbb{M}} x \leq z$ *and* $\mathrm{d}_c \sqcap^\sharp_{\mathbb{M}} x \leq z = (x \leq y \wedge z = 0 \wedge x \leq 0) \neq \bot^\sharp_{\mathbb{M}}$. *Therefore, the partitioning directive* d_p *is invalid with respect to* d_c.

(5) $\mathrm{d}_c = x \leq y \wedge y \leq z$ *and* $\mathrm{d}_p = part\langle Inv,\ \ell,\ \mathrm{M}^\sharp_p = z < x \wedge w \leq 0\rangle$*: in this example,* $vars(\mathrm{M}^\sharp_p) \backslash vars(\mathrm{d}_c) = \{w\}$, *and none of (S1-S3) holds in this example, thus we need to directly check the condition (7.8), which is always true because* $\forall v \in \mathbb{V}.\ (x \leq y \wedge y \leq z \wedge w = v) \sqcap^\sharp_{\mathbb{M}} (z < x \wedge w \leq 0) = \bot^\sharp_{\mathbb{M}}$. *Therefore, the partitioning directive* d_p *is valid with respect to* d_c. □

7.2.2.3 Checking the Validity of a Partition Function in the Abstract

Up to now, we have discussed how to check if a single partitioning directive is valid with respect to a cognizance directive. For a program, the user specifies an abstract cognizance function $\mathbb{C}^\sharp \in \mathbb{L} \mapsto \wp(\mathcal{D}^\sharp_{\mathbb{M}})$, and there are typically more than one partitioning directive of the form $\mathrm{part}\langle \mathrm{Inv},\ \ell,\ \mathrm{M}^\sharp_p\rangle$, hence we need to check the validity of all these partitioning directives with respect to the whole cognizance function. For the sake of clarity, here we rephrase the set of partitioning directives of the form $\mathrm{part}\langle \mathrm{Inv},\ \ell,\ \mathrm{M}^\sharp_p\rangle$ as a *partition function* $\mathbb{P}^\sharp \in \mathbb{L} \mapsto \wp(\mathcal{D}^\sharp_{\mathbb{M}})$, such that $\forall \ell \in \mathbb{L}.\ \forall \mathrm{M}^\sharp_p \in \mathbb{P}^\sharp(\ell).\ \mathrm{part}\langle \mathrm{Inv},\ \ell,\ \mathrm{M}^\sharp_p\rangle$ is a partitioning directive in the program.

Formally, here we define a function $\mathrm{isValid}_{\mathbb{P}}$ that checks if a partition function $\mathbb{P}^\sharp$ is valid with respect to a cognizance function $\mathbb{C}^\sharp$:

$$\mathrm{isValid}_{\mathbb{P}} \quad \in \quad (\mathbb{L} \mapsto \wp(\mathcal{D}^\sharp_{\mathbb{M}})) \mapsto ((\mathbb{L} \mapsto \wp(\mathcal{D}^\sharp_{\mathbb{M}})) \mapsto \mathbb{B}) \qquad \text{Validity of Partition}$$

$$\text{isValid}_{\mathbb{P}}(\mathbb{C}^\sharp, \mathbb{P}^\sharp) \triangleq \begin{cases} \text{true} & \text{if } \forall \ell \in \mathbb{L}.\ \forall d_c \in \mathbb{C}^\sharp(\ell), \mathrm{M}_p^\sharp \in \mathbb{P}^\sharp(\ell).\ \text{isValid}_d(d_c, \mathrm{M}_p^\sharp) \\ \text{false} & \text{otherwise.} \end{cases}$$

That is to say, a partition function $\mathbb{P}^\sharp$ is valid with respect to an abstract cognizance function $\mathbb{C}^\sharp$, if and only if, at each program point ℓ, every partitioning directive specified by $\mathbb{P}^\sharp$ is valid with respect to every cognizance directive assigned by $\mathbb{C}^\sharp$.

Recall that the partitioning directives are designed to create new partitions when constructing trace partitioning automata, and the sole purpose of checking if a partition function $\mathbb{P}^\sharp$ is valid with respect to an abstract cognizance function $\mathbb{C}^\sharp$ is to ensure that any two indistinguishable traces would not be partitioned into different partitions, thus are always represented by the same path in the constructed trace partitioning automaton.

Theorem 2 *If the partition function $\mathbb{P}^\sharp$ is valid with respect to the cognizance function $\mathbb{C}^\sharp$, then every two indistinguishable traces $\sigma \overset{\mathbb{C}^\sharp}{\sim} \sigma'$ must belong to the same partition created by $\mathbb{P}^\sharp$ at every program point along the execution.*

Formally, $\forall \mathbb{C}^\sharp, \mathbb{P}^\sharp \in \mathbb{L} \mapsto \wp(\mathcal{D}_{\mathbb{M}}^\sharp).$ *isValid*$_{\mathbb{P}}(\mathbb{C}^\sharp, \mathbb{P}^\sharp) \Rightarrow (\forall \sigma, \sigma' \in \mathbb{S}^{*\infty}.\ \sigma \overset{\mathbb{C}^\sharp}{\sim} \sigma' \Rightarrow (\forall i \in [0, |\sigma|).\ \exists \ell \in \mathbb{L}, \rho, \rho' \in \mathbb{M}.\ \sigma_{[i]} = \langle \ell,\ \rho \rangle \wedge \sigma'_{[i]} = \langle \ell,\ \rho' \rangle \wedge \forall \mathrm{M}_p^\sharp \in \mathbb{P}^\sharp(\ell).\ \rho \in \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp) \Leftrightarrow \rho' \in \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp)))$.

Proof. The contraposition of this theorem states that, suppose $\mathbb{P}^\sharp$ is valid with respect to $\mathbb{C}^\sharp$, if two traces do not belong to the same partition created by $\mathbb{P}^\sharp$ at some program point along the execution, then these two traces cannot be equivalent according to $\mathbb{C}^\sharp$. More formally, $\forall \mathbb{C}^\sharp, \mathbb{P}^\sharp \in \mathbb{L} \mapsto \wp(\mathcal{D}_{\mathbb{M}}^\sharp).\ \text{isValid}_{\mathbb{P}}(\mathbb{C}^\sharp, \mathbb{P}^\sharp) \Rightarrow (\forall \sigma, \sigma' \in \mathbb{S}^{*\infty}.\ (\exists i \in [0, |\sigma|), \ell \in \mathbb{L}, \rho, \rho' \in \mathbb{M}, \mathrm{M}_p^\sharp \in \mathbb{P}^\sharp(\ell).\ \sigma_{[i]} = \langle \ell, \rho \rangle \wedge \sigma'_{[i]} = \langle \ell, \rho' \rangle \wedge \rho \in \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp) \wedge \rho' \notin \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp)) \Rightarrow \sigma \overset{\mathbb{C}^\sharp}{\not\sim} \sigma')$.

Here we prove by contradiction. Assume that there exist two traces $\sigma \overset{\mathbb{C}^\sharp}{\sim} \sigma'$ such that they do not belong to the same partition at some location i, i.e. $\mathrm{M}_p^\sharp \in \mathbb{P}^\sharp(\ell) \wedge \sigma_{[i]} = \langle \ell, \rho \rangle \wedge \sigma'_{[i]} = \langle \ell,\ \rho' \rangle \wedge \rho \in \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp) \wedge \rho' \notin \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp)$.

Since $\sigma \overset{\mathbb{C}^\sharp}{\sim} \sigma'$, there must exists some $d_c \in \mathbb{C}^\sharp(\ell)$ such that $\rho \overset{d_c}{\sim} \rho'$. By the definition of $\overset{d_c}{\sim}$, there are two possible cases:

(1) $\rho = \rho'$. In this case, it is impossible to have $\rho \in \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp) \wedge \rho' \notin \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp)$, which simply introduces a contradiction.

(2) $\rho \in \gamma_{\mathbb{M}}(d_c) \wedge \rho' \in \gamma_{\mathbb{M}}(d_c) \wedge \forall \mathcal{x} \in \mathbb{X} \backslash \mathrm{vars}(d_c).\ \rho(\mathcal{x}) = \rho'(\mathcal{x})$. Since $\mathrm{isValid}_{\mathbb{P}}(\mathbb{C}^\sharp, \mathbb{P}^\sharp)$ is true, we know $\mathrm{isValid}_d(d_c, \mathrm{M}_p^\sharp)$ must hold, which further implies $[\rho]_{\underset{\sim}{d_c}} \subseteq \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp) \ \vee\ [\rho]_{\underset{\sim}{d_c}} \cap \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp) = \emptyset$ (7.1). By the assumption $\rho \in \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp)$ and the fact that $\rho \in [\rho]_{\underset{\sim}{d_c}}$, we know $[\rho]_{\underset{\sim}{d_c}} \cap \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp) \neq \emptyset$, thus $[\rho]_{\underset{\sim}{d_c}} \subseteq \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp)$ must hold. Since $\rho \overset{d_c}{\sim} \rho'$, we have $\rho' \in [\rho]_{\underset{\sim}{d_c}}$, thus $\rho' \in \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp)$, which contradicts with the assumption $\rho' \notin \gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp)$. $\square$

7.2.2.4 Revising Partitioning Directives to be Valid

In the previous sections, we have introduced the method to check the validity of partitioning directives (or say, the partition function), while the approach of creating partitioning directives will be discussed in chapter 8. Intuitively, we could create partitioning directives based on the information provided by the cognizance function, such that the created partitioning directives are always valid. For example, if the cognizance function $\mathbb{C}^\sharp(\ell) = \{\mathcal{x} < 0, \mathcal{x} \geq 0\}$ indicates that the observer knows the sign of $\mathcal{x}$ at point ℓ, but not the exact value of $\mathcal{x}$. It is intuitive to create two partitions according to the sign of $\mathcal{x}$ at point ℓ: $\mathrm{part}\langle \mathrm{Inv},\ \ell,\ \mathcal{x} < 0 \rangle$ and $\mathrm{part}\langle \mathrm{Inv},\ \ell,\ \mathcal{x} \geq 0 \rangle$, both of which can be simply proved to be valid with respect to $\mathbb{C}^\sharp$. However, this is not always the case,

and we may want to create partitioning directives based on some other criteria, which may bring us invalid partitioning directives. Thus, a missing part here is: what shall we do if a certain partitioning directive $d_p = \text{part}\langle \text{Inv}, \ell, \mathrm{M}_p^\sharp \rangle$ (or $\mathrm{M}_p^\sharp$ for short) is found invalid with respect to a cognizance directive d_c at point ℓ (i.e. $\text{isValid}_d(d_c, \mathrm{M}_p^\sharp) = \text{false}$)?

Obviously, we can simply discard the partitioning directive d_p, and the correspondingly constructed trace partitioning automaton is still guaranteed to be sound. However, this may incur the loss of precision in the forward reachability analysis, which further affects the result of abstract responsibility analysis.

Alternatively, we can retrieve the validity by revising $\mathrm{M}_p^\sharp$. By the definition of $\text{isValid}_d(d_c, \mathrm{M}_p^\sharp)$, we know that $d_c \sqsubseteq_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp \vee d_c \sqcap_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp = \bot_{\mathbb{M}}^\sharp$ does not hold. That is to say, $d_c \not\sqsubseteq_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp$ and $d_c \sqcap_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp \neq \bot_{\mathbb{M}}^\sharp$, thus there are two possible cases:

1. $\mathrm{M}_p^\sharp \sqsubset_{\mathbb{M}}^\sharp d_c$: $\mathrm{M}_p^\sharp$ is strictly less than d_c, or $\gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp) \subsetneq \gamma_{\mathbb{M}}(d_c)$. In this case, we can just use d_c as a new partitioning directive to replace $\mathrm{M}_p^\sharp$, i.e. we define $\mathrm{M}_p^{\sharp\prime} = d_c$, and $\mathrm{M}_p^{\sharp\prime}$ is obviously valid with respect to d_c. For example, $d_p = \text{part}\langle \text{Inv}, \ell, \mathrm{M}_p^\sharp = \mathcal{x} < 0 \rangle$ is invalid with respect to $d_c = \mathcal{x} \leq 0$, and we can replace it by a new partitioning directive $\text{part}\langle \text{Inv}, \ell, \mathrm{M}_p^\sharp = \mathcal{x} \leq 0 \rangle$ which is trivially valid.

2. $\mathrm{M}_p^\sharp \not\sqsubseteq_{\mathbb{M}}^\sharp d_c \wedge d_c \not\sqsubseteq_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp \wedge d_c \sqcap_{\mathbb{M}}^\sharp \mathrm{M}_p^\sharp \neq \bot_{\mathbb{M}}^\sharp$: $\mathrm{M}_p^\sharp$ overlaps with d_c, and they are incomparable. In this case, there are two possible ways to create new partitioning directives to replace $\mathrm{M}_p^\sharp$:

   a) Define a new partitioning directive $\mathrm{M}_p^{\sharp\prime} = \mathrm{M}_p^\sharp \sqcup_{\mathbb{M}}^\sharp d_c$.

      Obviously, $\mathrm{M}_p^{\sharp\prime}$ is valid with respect to d_c since $d_c \sqsubseteq_{\mathbb{M}}^\sharp \mathrm{M}_p^{\sharp\prime}$. For example, $d_p = \text{part}\langle \text{Inv}, \ell, \mathrm{M}_p^\sharp = \mathcal{x} \in [1; \infty] \rangle$ is invalid with respect to the cognizance

directive $d_c = \mathcal{x} \in [0; 1]$ that indicates the observer cannot distinguish the value 0 and 1 of $\mathcal{x}$, then we can replace it by a new partitioning directive $\text{part}\langle \text{Inv}, \mathcal{l}, \mathrm{M}_p^\sharp = \mathcal{x} \in [0; \infty] \rangle$. It is worthy mentioning that, convex abstract domains (such as the polyhedra domain) cannot exactly represent unions, which must be over-approximated (e.g. the convex hull for polyhedra). If the incurred loss of precision is unacceptable and we need the exact union, we could use the disjunctive completion as a new partitioning directive, although it may be costly and does not scale well.

b) Or, we split $\mathrm{M}_p^\sharp \sqcup_{\mathbb{M}}^\sharp d_c$ by defining two new partitioning directives: $\mathrm{M}_p^{\sharp\prime} = d_c$ and $\mathrm{M}_p^{\sharp\prime\prime} = \mathrm{M}_p^\sharp \sqcap_{\mathbb{M}}^\sharp \neg d_c$.

It is not hard to see that $d_c \sqsubseteq_{\mathbb{M}}^\sharp \mathrm{M}_p^{\sharp\prime}$ and $d_c \sqcap_{\mathbb{M}}^\sharp \mathrm{M}_p^{\sharp\prime\prime} = \bot_{\mathbb{M}}^\sharp$, thus these two new partitioning directives are valid. Specially, $\mathrm{M}_p^{\sharp\prime\prime}$ under-approximates $\mathrm{M}_p^\sharp$, thus the correspondingly created partition preserves the desired property of partitioning by $\mathrm{M}_p^\sharp$. However, the classic numerical domains (such as intervals, octagons, polyhedra) do not support the complement operation $\neg$, e.g. the complement of a polyhedron is a disjunction of affine inequalities, thus $\mathrm{M}_p^\sharp \sqcap_{\mathbb{M}}^\sharp \neg d_c$ may not be expressed by a single element in $\mathcal{D}_{\mathbb{M}}^\sharp$. If this happens, instead of defining a single partitioning directive to represent $\mathrm{M}_p^\sharp \sqcap_{\mathbb{M}}^\sharp \neg d_c$, we define a list of partitioning directives, each of which is a conjunction of $\mathrm{M}_p^\sharp$ and an affine inequality from $\neg d_c$. For example, $d_p = \text{part}\langle \text{Inv}, \mathcal{l}, \mathrm{M}_p^\sharp = \mathcal{x} \leq 10 \rangle$ is invalid with respect to the cognizance directive $d_c = \mathcal{x} \geq 0 \wedge y > 0$. The complement of d_c is the disjunction of $\mathcal{x} < 0$ and $y \leq 0$. Thus, we create three new partitioning directives:

$\mathrm{M}_p^{\sharp\prime} = d_c = x \geq 0 \wedge y > 0$, $\mathrm{M}_p^{\sharp\prime\prime} = \mathrm{M}_p^\sharp \sqcap_{\mathbb{M}}^\sharp x < 0 = x < 0$, and $\mathrm{M}_p^{\sharp\prime\prime\prime} = \mathrm{M}_p^\sharp \sqcap_{\mathbb{M}}^\sharp y \leq 0 = x \leq 10 \wedge y \leq 0$. In addition, when the number of affine inequality from $\neg d_c$ is large, we could heuristically select part of them to create new partitioning directives, reducing the cost incurred by trace partitioning without harm to the soundness.

To sum up, in this chapter, we have discussed the user specification of system behaviors and cognizance in the abstract, proposed a sound approach to check if the partitioning directives are valid with respect to the user specified cognizance, and sketched some possible methods to retrieve the validity for invalid partitioning directives.

Chapter 8

Abstract Responsibility Analysis

The concrete responsibility analysis $\alpha_R([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \mathcal{B}, \mathcal{T})$ proposed in chapter 5 is undecidable, and an implementation of it has to abstract sets of finite or infinite traces involved in $[\![\mathrm{P}]\!]^{\mathsf{Max}}$, $\mathcal{L}^{\mathsf{Max}}$, $\mathbb{C}$, $\mathcal{B}$, and $\mathcal{T}$. Up to now, we have discussed the abstraction of maximal trace semantics $[\![\mathrm{P}]\!]^{\mathsf{Max}}$ by trace partitioning automata that are constructed by over-approximating forward reachability analysis (section 2.3) with trace partitioning (chapter 3), the abstraction of system behaviors $\mathcal{B}$ by abstract invariants (section 7.1), and the abstraction of cognizance $\mathbb{C}$ by abstract cognizance function (section 7.2). Moreover, it is assumed that the lattice of behaviors $\mathcal{L}^{\mathsf{Max}}$ consists of only $\mathcal{B}$ and its complement (besides the top and bottom), and the set of traces to be analyzed $\mathcal{T}$ is the whole maximal trace semantics, thus all the components in responsibility analysis have been abstracted.

In this chapter, we propose the framework of responsibility analysis in the abstract, which essentially consists of an iteration of forward (possible success) reachability analysis with trace partitioning and backward impossible failure accessibility analysis. In addition, this abstract responsibility analysis is proved to be sound.

8.1 The Framework of Abstract Responsibility Analysis

As shown in Fig.8.1, given a program P with the user specified behavior of interest $\mathcal{B}^\sharp \in \mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}$ and abstract cognizance $\mathbb{C}^\sharp \in \mathbb{L} \mapsto \wp(\mathcal{D}^\sharp_{\mathbb{M}})$, the abstract responsibility analysis can determine the responsible entities in P that are potentially responsible for $\mathcal{B}^\sharp$ to the cognizance of $\mathbb{C}^\sharp$.

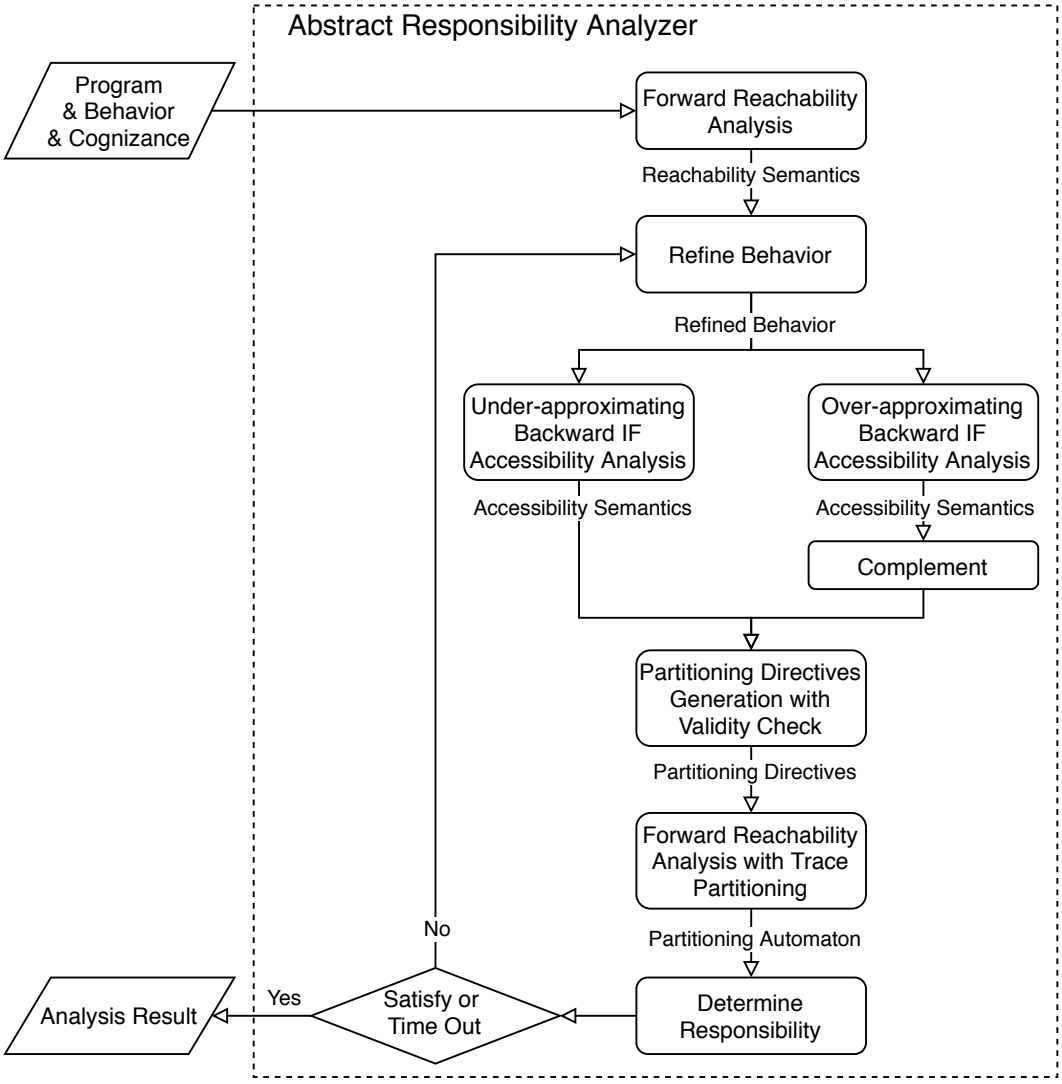

Figure 8.1: Trace Framework of Abstract Responsibility Analysis

More precisely, the abstract responsibility analysis starts with a forward reachability analysis $\mathcal{S}^{\sharp}_{\overrightarrow{ps}}[\![\mathrm{P}]\!]$, which produces an over-approximation of the program's reachability semantics. Then, after refining the behavior of interest $\mathcal{B}^{\sharp}$ by the intersection with the computed reachability semantics, we perform in parallel both an under-approximating backward impossible failure accessibility analysis $\check{\mathcal{S}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^{\sharp})$ and an over-approximating backward impossible failure accessibility analysis $\hat{\mathcal{S}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^{\sharp})$, and the correspondingly computed accessibility semantics (or its complement) are transformed into partitioning directives of form "$d_p = \mathrm{part}\langle \mathrm{Inv}, \ell, \mathrm{M}^{\sharp}_p \rangle$". Further, using the partitioning directives that are valid with respect to $\mathbb{C}^{\sharp}$, a new round of forward reachability analysis is conducted, which computes a refined reachability semantics and a trace partitioning automaton. In such an automaton, nodes created by partitioning directives from the complement of $\hat{\mathcal{S}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^{\sharp})$ are marked as left bounds, while nodes created by partitioning directives from $\check{\mathcal{S}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^{\sharp})$ are marked as right bounds. It follows that, along each path in the automaton, the responsible entities must be located after the left bounds (if any) and before the right bounds (if any). Thus, at this point we can determine responsible entities in the trace partitioning automaton, and stop if we are satisfied with the results or the time cost exceeds the pre-specified threshold. Otherwise, we start a new round of backward-forward analysis with the behavior $\mathcal{B}^{\sharp}$ that is refined again by the new reachability semantics, which may improve the precision of responsibility analysis result.

It is not hard to see that, most components in this framework of abstract responsibility analysis have been discussed in previous chapters. In the rest of this chapter, we summarize these components and illustrate how they collaborate to determine responsibility in the abstract, with the example of the access control program in Fig. 1.4.

8.1.1 The Preprocessing Phase

The abstract responsibility analysis starts with a preprocessing phase, in which the user specifies the behavior of interest and the observer's cognizance, and a preliminary forward reachability analysis is conducted to compute the reachability semantics.

The abstract behavior $\mathcal{B}^\sharp$ and the abstract cognizance $\mathbb{C}^\sharp$ have been elaborated in chapter 7, and the over-approximating forward reachability analysis $\mathcal{S}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{pre}})$ has been formalized in section 2.3, thus here we reuse them and supplement with some practical tips that could facilitate the coming analysis phrases.

For any program P to be analyzed, we insert a dummy initial program point ℓ_0 followed by a dummy action that does not affect the program execution (e.g. skip) in front of P, such that the variable initialization action at the beginning of program execution is explicitly mimicked by this dummy action. Therefore, when the dummy initial action is determined as responsible for a behavior $\mathcal{B}^\sharp$, it means that whether $\mathcal{B}^\sharp$ occurs or not may be decided by the variable initialization.

In addition, for the over-approximating forward reachability analysis $\mathcal{S}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{pre}})$, the abstract precondition $\mathsf{I}^\sharp_{\mathsf{pre}} \in \mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}$ is always defined such that the abstract environment element for the dummy initial point is the top (i.e. $\mathsf{I}^\sharp_{\mathsf{pre}}(\ell_0) = \top^\sharp_{\mathbb{M}}$) and it is the bottom for all other program points (i.e. $\mathsf{I}^\sharp_{\mathsf{pre}}(\ell) = \bot^\sharp_{\mathbb{M}}$ for $\ell \neq \ell_0$). Moreover, the precision of this forward reachability analysis can be improved by trace partitioning, which is optional. Although until this step we have not obtained any partitioning directives that are related with memory states and of form "part$\langle$Inv, ℓ, $\mathrm{M}^\sharp_p\rangle$", we can still conduct the trace partitioning by partitioning directives related with the control flow (e.g. part$\langle$If, ℓ, $b\rangle$ and part$\langle$While, ℓ, $n\rangle$), which can be derived as in the preprocessing phase of [43].

Example 23 (Access Control, Continued) *For the access control program in Fig.1.4, we insert a dummy initial point ℓ_0 as well as a dummy action before the point ℓ_1, which has no affect on the result of forward reachability analysis in this phase. Suppose the user is interested in the behavior "the access to o fails", then the user can specify the abstract behavior $\mathcal{B}^\sharp \in \mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}$ such that $\mathcal{B}^\sharp(\ell_8) = acs \in [\text{-}\infty; 0]$, while $\mathcal{B}^\sharp(\ell) = \top^\sharp_{\mathbb{M}}$ for other program points $\ell \neq \ell_8$. Here we consider two types of observers: an omniscient observer, whose abstract cognizance function $\mathbb{C}^\sharp_o \in \mathbb{L} \mapsto \wp(\mathcal{D}^\sharp_{\mathbb{M}})$ is specified such that $\mathbb{C}^\sharp_o(\ell) = \{\bot^\sharp_{\mathbb{M}}\}$ for every program point $\ell \in \mathbb{L}$; and an observer that does not know the input of the 1st admin, and the corresponding abstract cognizance function $\mathbb{C}^\sharp \in \mathbb{L} \mapsto \wp(\mathcal{D}^\sharp_{\mathbb{M}})$ is defined such that, if $\ell \in \{\ell_0, \ell_1, \ell_2\}$, then $\mathbb{C}^\sharp(\ell) = \{\bot^\sharp_{\mathbb{M}}\}$, otherwise $\mathbb{C}^\sharp(\ell) = \{i1 \in [-1; 2]\}$.*

Since there is no conditional or while loop in the access control program, we do the forward reachability analysis without trace partitioning, and the corresponding forward reachability semantics $\mathcal{S}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{pre}})$ is listed in table 8.1 (which is almost the same as the table 2.2). For the sake of clarity and to be consistent with the analysis result from the Interproc analyzer [50], the trivial constraints like $acs \in [\text{-}\infty; \infty]$ are omitted in the table. □

ℓ	$\mathcal{S}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{pre}})\ell$
ℓ_0	$\top^\sharp_{\mathbb{M}}$
ℓ_1	$\top^\sharp_{\mathbb{M}}$
ℓ_2	$apv \in [1; 1]$
ℓ_3	$apv \in [1; 1] \wedge i1 \in [\text{-}1; 2]$
ℓ_4	$apv \in [\text{-}1; 1] \wedge i1 \in [\text{-}1; 2]$
ℓ_5	$apv \in [\text{-}1; 1] \wedge i1 \in [\text{-}1; 2] \wedge i2 \in [\text{-}1; 2]$
ℓ_6	$apv \in [\text{-}1; 1] \wedge i1 \in [\text{-}1; 2] \wedge i2 \in [\text{-}1; 2]$
ℓ_7	$apv \in [\text{-}1; 1] \wedge i1 \in [\text{-}1; 2] \wedge i2 \in [\text{-}1; 2] \wedge typ \in [1; 2]$
ℓ_8	$apv \in [\text{-}1; 1] \wedge i1 \in [\text{-}1; 2] \wedge i2 \in [\text{-}1; 2] \wedge typ \in [1; 2] \wedge acs \in [\text{-}2; 2]$

Table 8.1: Abstract Forward Reachability Semantics for the Access Control Program

8.1.2 The Backward Analysis Phase

The objective of this backward analysis phase is to create partitioning directives of the form "part$\langle \text{Inv},\ \ell,\ \mathrm{M}_p^\sharp \rangle$" that can either guarantee that the behavior $\mathcal{B}^\sharp$ always hold or guarantee the existence of at least one execution trace that fails behavior $\mathcal{B}^\sharp$.

8.1.2.1 Behavior Refinement with Reachability Semantics

After completing a forward reachability analysis, the first step is to refine the behavior $\mathcal{B}^\sharp$ of interest by the intersection with the computed reachability semantics $\mathcal{S}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{pre}})$.

If the reachability semantics is computed without trace partitioning, the intersection of $\mathcal{S}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{pre}}) \in \mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}$ with $\mathcal{B}^\sharp \in \mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}$ is simply the pointwise meet $\sqcap^\sharp_{\mathbb{M}}$ of abstract environments, and the refined behavior is $\mathcal{S}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{pre}}) \dot{\sqcap}^\sharp_{\mathbb{M}} \mathcal{B}^\sharp$. However, if the trace partitioning is involved in the forward reachability analysis, then $\mathcal{S}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{pre}}) \in \mathbb{L}_T \mapsto \mathcal{D}^\sharp_{\mathbb{M}} \triangleq \mathbb{L} \times T \mapsto \mathcal{D}^\sharp_{\mathbb{M}}$ (where T is the set of partitioning tokens) has to be transformed into the form $\mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}$ before the intersection with $\mathcal{B}^\sharp$ can be performed.

There are possibly several ways to do so: (1) A naive method is to apply to $\mathcal{S}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{pre}})$ the forget function π_τ, which is defined in the trace partitioning abstract domain (section 3.1) to remove partitioning tokens from extended program points, such that abstract environments at the same point with different partitioning tokens are joined together. Formally, we construct $\mathsf{I}^\sharp \in \mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}$ such that $\forall \ell \in \mathbb{L}.\ \mathsf{I}^\sharp(\ell) = \sqcup^\sharp_{\mathbb{M}}\{\mathcal{S}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{pre}})\langle \ell,\ t\rangle \mid t \in T\}$, and the refined behavior would be $\mathsf{I}^\sharp \dot{\sqcap}^\sharp_{\mathbb{M}} \mathcal{B}^\sharp$. (2) The naive method can be improved if we do the intersection with $\mathcal{B}^\sharp$ before joining the abstract environments together. Formally, the refined behavior is $\mathcal{B}^{\sharp\prime} \in \mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}$ such that $\mathcal{B}^{\sharp\prime}(\ell) = \sqcup^\sharp_{\mathbb{M}}\{\mathcal{S}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{pre}})\langle \ell,\ t\rangle \sqcap^\sharp_{\mathbb{M}} \mathcal{B}(\ell) \mid t \in T\}$. (3) Another alternative method is to use multiple behaviors to represent

the intersection of $\mathcal{B}^\sharp$ with $\mathcal{S}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{pre}})$. More specifically, $\mathcal{S}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{pre}})$ can be equivalently viewed as a trace partitioning automaton, thus for each path in this automaton we can do an intersection with $\mathcal{B}^\sharp$, and construct a new behavior if the path is still valid (i.e. no node is attached with $\bot^\sharp_{\mathbb{M}}$). This method is the most precise one for refining the behavior of interest, but the cost of introducing multiple behaviors to the following backward analysis is prohibitive, hence it is not adopted in this dissertation.

Example 24 (Access Control, Continued) *Following the example 23, the trace partitioning is not used in the forward reachability analysis, hence the abstract behavior $\mathcal{B}^\sharp$ can be refined simply by the pointwise meet $\dot{\sqcap}^\sharp_{\mathbb{M}}$ with $\mathcal{S}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{pre}})$ from table 8.1. For the sake of conciseness, the refined behavior is still called $\mathcal{B}^\sharp$, thus we have: $\mathcal{B}^\sharp(\ell_8) = apv \in [\text{-}1; 1] \wedge i1 \in [\text{-}1; 2] \wedge i2 \in [\text{-}1; 2] \wedge typ \in [1; 2] \wedge acs \in [\text{-}2; 0]$, and $\mathcal{B}^\sharp(\ell) = \mathcal{S}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{pre}})\ell$ for program points ℓ other than ℓ_8.* □

8.1.2.2 Under-approximating/Over-approximating Backward Impossible Failure Accessibility Analysis

Using the under-approximating backward impossible failure accessibility analysis formally defined in section 2.4.2, we get $\check{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^\sharp) \in \mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}$ such that, for every program point ℓ, $\check{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^\sharp)\ell$ is an under-approximation of the weakest sufficient precondition for $\mathcal{B}^\sharp$. Since an under-approximation of the weakest sufficient precondition is still a sufficient condition, every concrete valid trace that begins from a state $\langle \ell,\ \rho \rangle$ such that $\rho \in \gamma_{\mathbb{M}}(\check{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^\sharp)\ell)$ must satisfy the behavior $\mathcal{B}^\sharp$.

Similarly, using the over-approximating backward impossible failure accessibility analysis formalized in section 2.4.3, we get $\hat{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathsf{I}^{\sharp\prime}_{\mathsf{post}}) \in \mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}$ such that, for

every program point ℓ, $\hat{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^\sharp)\ell$ over-approximates the weakest sufficient precondition for $\mathcal{B}^\sharp$. Since an over-approximation of the weakest sufficient precondition is not necessarily a sufficient condition, $\hat{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^\sharp)\ell$ does not guarantee that the occurrence of behavior $\mathcal{B}^\sharp$. However, it is guaranteed that, if all the concrete valid traces that begin from a state $\langle \ell,\ \rho\rangle$ have the behavior $\mathcal{B}^\sharp$, then ρ must satisfy the environment property $\hat{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^\sharp)\ell$ (i.e. $\rho \in \gamma_{\mathbb{M}}(\hat{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^\sharp)\ell)$). That is to say, from a state $\langle \ell,\ \rho\rangle$ such that ρ does not satisfy $\hat{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^\sharp)\ell$ (i.e. $\rho \notin \gamma_{\mathbb{M}}(\hat{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^\sharp)\ell)$), there must exist at least one concrete valid trace that fails the behavior $\mathcal{B}^\sharp$.

In order to make use of the environments that do not satisfy $\hat{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^\sharp)\ell$, we want to compute the complement of $\hat{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^\sharp)$, or even better, $\mathcal{S}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{pre}})\backslash\hat{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^\sharp)$ (i.e. $\mathcal{S}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{pre}})\dot{\sqcap}^\sharp_{\mathbb{M}}(\dot{\neg}\hat{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^\sharp))$), such that invalid environments can be excluded before entering the next step. Yet, most abstract environment domains do not directly support the complement operation, including the classic numerical domains (such as the interval, octagon and polyhedron domain). For example, the complement of a polyhedron is a disjunction of affine inequalities. Nevertheless, similar to the disjunctive completion, we can define the complement of $\hat{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^\sharp) \in \mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}$ as $\dot{\neg}\hat{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^\sharp) \in \mathbb{L} \mapsto \wp(\mathcal{D}^\sharp_{\mathbb{M}})$, such that each abstract environment element in $\dot{\neg}\hat{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^\sharp)\ell$ represents an affine inequality in the disjunction at the point ℓ.

It is worthy to mention that, the number of affine inequalities in the complement of some abstract environment element from $\mathcal{D}^\sharp_{\mathbb{M}}$ may be large, especially for polyhedra. However, it is safe to remove part of these affine inequalities and keep only the heuristically selected ones, without any harm to the soundness of abstract responsibility analysis.

Example 25 (Access Control, Continued) *Following the example 24, we conduct an under-*

approximating backward impossible failure accessibility analysis on $\mathcal{B}^\sharp$, and the corresponding result $\check{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^\sharp)$ is listed in table 8.2. Similarly, the result of the over-approximating backward impossible failure accessibility analysis on $\mathcal{B}^\sharp$ is listed in table 8.3. Notice that we have adopted the disjunctive completion in $\check{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^\sharp)\ell_5$ to gain the precision, otherwise it would be $apv \in [\text{-}1; 1] \wedge i1 \in [\text{-}1; 2] \wedge i2 \in [\text{-}1; 2]$ instead, which is equal to $\mathcal{S}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{pre}})\ell$.

ℓ	$\check{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^\sharp)\ell$
ℓ_0	$\bot^\sharp_{\mathbb{M}}$
ℓ_1	$\bot^\sharp_{\mathbb{M}}$
ℓ_2	$\bot^\sharp_{\mathbb{M}}$
ℓ_3	$\bot^\sharp_{\mathbb{M}}$
ℓ_4	$\bot^\sharp_{\mathbb{M}}$
ℓ_5	$apv \in [\mathbf{1}; \mathbf{1}] \wedge i1 \in [\text{-}1; 2] \wedge i2 \in [\mathbf{\text{-}1}; \mathbf{0}]$
ℓ_6	$apv \in [\mathbf{\text{-}1}; \mathbf{0}] \wedge i1 \in [\text{-}1; 2] \wedge i2 \in [\text{-}1; 2]$
ℓ_7	$apv \in [\mathbf{\text{-}1}; \mathbf{0}] \wedge i1 \in [\text{-}1; 2] \wedge i2 \in [\text{-}1; 2] \wedge typ \in [1; 2]$
ℓ_8	$apv \in [\text{-}1; 1] \wedge i1 \in [\text{-}1; 2] \wedge i2 \in [\text{-}1; 2] \wedge typ \in [1; 2] \wedge acs \in [\mathbf{\text{-}2}; \mathbf{0}]$

Table 8.2: The Under-approximating Backward IF Accessibility Semantics for $\mathcal{B}^\sharp$

ℓ	$\hat{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^\sharp)\ell$
ℓ_0	$\bot^\sharp_{\mathbb{M}}$
ℓ_1	$\bot^\sharp_{\mathbb{M}}$
ℓ_2	$\bot^\sharp_{\mathbb{M}}$
ℓ_3	$apv \in [1; 1] \wedge i1 \in [\mathbf{\text{-}1}; \mathbf{0}]$
ℓ_4	$apv \in [\mathbf{\text{-}1}; \mathbf{0}] \wedge i1 \in [\text{-}1; 2]$
ℓ_5	$\{apv \in [\mathbf{\text{-}1}; \mathbf{0}] \wedge i1 \in [\text{-}1; 2] \wedge i2 \in [\text{-}1; 2],$ $apv \in [\mathbf{1}; \mathbf{1}] \wedge i1 \in [\text{-}1; 2] \wedge i2 \in [\mathbf{\text{-}1}; \mathbf{0}]\}$
ℓ_6	$apv \in [\mathbf{\text{-}1}; \mathbf{0}] \wedge i1 \in [\text{-}1; 2] \wedge i2 \in [\text{-}1; 2]$
ℓ_7	$apv \in [\mathbf{\text{-}1}; \mathbf{0}] \wedge i1 \in [\text{-}1; 2] \wedge i2 \in [\text{-}1; 2] \wedge typ \in [1; 2]$
ℓ_8	$apv \in [\text{-}1; 1] \wedge i1 \in [\text{-}1; 2] \wedge i2 \in [\text{-}1; 2] \wedge typ \in [1; 2] \wedge acs \in [\mathbf{\text{-}2}; \mathbf{0}]$

Table 8.3: The Over-approximating Backward IF Accessibility Semantics for $\mathcal{B}^\sharp$ with Disjunctive Completion

Furthermore, the complement of $\hat{\mathcal{S}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^{\sharp})$ *is listed in table 8.4. Notice that, instead of simply using the direct complement of* $\hat{\mathcal{S}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^{\sharp})$*, here we adopt* $\mathcal{S}^{\sharp}_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^{\sharp}_{\mathsf{pre}})\backslash\hat{\mathcal{S}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^{\sharp})$*, or say,* $\mathcal{S}^{\sharp}_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^{\sharp}_{\mathsf{pre}})\dot{\sqcap}^{\sharp}_{\mathbb{M}}(\dot{\neg}\hat{\mathcal{S}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^{\sharp}))$*, such that invalid environments would not be included. For example, at point* ℓ_2*, the direct complement of* $\hat{\mathcal{S}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^{\sharp})\ell_2 = \bot^{\sharp}_{\mathbb{M}}$ *is* $\top^{\sharp}_{\mathbb{M}}$*. After the meet* $\sqcap^{\sharp}_{\mathbb{M}}$ *with the reachability semantics* $\mathcal{S}^{\sharp}_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^{\sharp}_{\mathsf{pre}})\ell_2$*, we can get the more precise* $apv \in [1;1]$*. Similarly, at point* ℓ_3*, the direct complement of* $\hat{\mathcal{S}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^{\sharp})\ell_3 = apv \in [1;1] \wedge i1 \in [\text{-}1;0]$ *is the disjunction of* $\{apv \in [\text{-}\infty;0], apv \in [2;\infty], i1 \in [\text{-}\infty;\text{-}2], i1 \in [1;\infty]\}$*, most of which are invalid (or say, unreachable in the concrete). After the meet with the reachability semantics* $\mathcal{S}^{\sharp}_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^{\sharp}_{\mathsf{pre}})\ell_3 = apv \in [1;1] \wedge i1 \in [\text{-}1;2]$*, it is refined to* $\{apv \in [1;1] \wedge i1 \in [1;2]\}$*, which is much more precise than direct complement.* □

ℓ	$\mathcal{S}^{\sharp}_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^{\sharp}_{\mathsf{pre}})\ell\backslash\hat{\mathcal{S}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^{\sharp})\ell$
ℓ_0	$\{\top^{\sharp}_{\mathbb{M}}\}$
ℓ_1	$\{\top^{\sharp}_{\mathbb{M}}\}$
ℓ_2	$\{apv \in [1;1]\}$
ℓ_3	$\{apv \in [1;1] \wedge i1 \in [\mathbf{1};\mathbf{2}]\}$
ℓ_4	$\{apv \in [\mathbf{1};\mathbf{1}] \wedge i1 \in [\text{-}1;2]\}$
ℓ_5	$\{apv \in [\mathbf{1};\mathbf{1}] \wedge i1 \in [\text{-}1;2] \wedge i2 \in [\mathbf{1};\mathbf{2}]\}$
ℓ_6	$\{apv \in [\mathbf{1};\mathbf{1}] \wedge i1 \in [\text{-}1;2] \wedge i2 \in [\text{-}1;2]\}$
ℓ_7	$\{apv \in [\mathbf{1};\mathbf{1}] \wedge i1 \in [\text{-}1;2] \wedge i2 \in [\text{-}1;2] \wedge typ \in [1;2]\}$
ℓ_8	$\{apv \in [\text{-}1;1] \wedge i1 \in [\text{-}1;2] \wedge i2 \in [\text{-}1;2] \wedge typ \in [1;2] \wedge acs \in [\mathbf{1};\mathbf{2}]\}$

Table 8.4: The Complement of Over-approximating Backward IF Accessibility Semantics for $\mathcal{B}^{\sharp}$ with Disjunctive Completion

8.1.2.3 Partitioning Directives Generation with Validity Check

Using the under-approximating backward impossible failure accessibility semantics $\check{\mathcal{S}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^{\sharp})$ and the complement of over-approximating backward impossible failure ac-

cessibility semantics $\mathcal{S}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathrm{I}^\sharp_{\mathsf{pre}}) \backslash \hat{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^\sharp)$, this step aims at constructing a partition function $\mathbb{P}^\sharp \in \mathbb{L} \mapsto \wp(\mathcal{D}^\sharp_{\mathbb{M}})$, such that $\forall \ell \in \mathbb{L}.\ \forall \mathrm{M}^\sharp_p \in \mathbb{P}^\sharp(\ell).\ \mathrm{part}\langle \mathrm{Inv},\ \ell,\ \mathrm{M}^\sharp_p \rangle$ is a partitioning directive that is valid with respect to the specified cognizance function $\mathbb{C}^\sharp$ and will be used in the next round of forward reachability analysis. Sometimes, a partitioning directive $d_p = \mathrm{part}\langle \mathrm{Inv},\ \ell,\ \mathrm{M}^\sharp_p \rangle$ is called as $\mathrm{M}^\sharp_p$ for short, when the program point ℓ is known from the context.

More specifically, here we design 4 types of partitioning directives that are based on the environments, and accordingly the partition function $\mathbb{P}^\sharp$ can be splitted into 4 parts:

(1) Right-bound partitioning directives. For any point ℓ, $\check{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^\sharp)\ell$ is a right-bound partitioning directive, if it is not $\bot^\sharp_{\mathbb{M}}$ and is valid with respect to all cognizance directives assigned to ℓ. Formally, we define the right-bound partition function $\mathbb{P}^\sharp_R$:

$$
\begin{array}{rcll}
\mathbb{P}^\sharp_R & \in & \mathbb{L} \mapsto \wp(\mathcal{D}^\sharp_{\mathbb{M}}) & \text{right-bound partition function} \\
\mathbb{P}^\sharp_R(\ell) & \triangleq & \{\mathrm{M}^\sharp_p \mid \mathrm{M}^\sharp_p = \check{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^\sharp)\ell \wedge \mathrm{M}^\sharp_p \neq \bot^\sharp_{\mathbb{M}} \wedge \forall d_c \in \mathbb{C}^\sharp(\ell).\ \mathrm{isValid}_d(d_c, \mathrm{M}^\sharp_p)\}
\end{array}
$$

By the definition of $\check{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^\sharp)$, it is easy to see that the partitions generated by right-bound partitioning directives during the next forward reachability analysis would guarantee the occurrence of $\mathcal{B}^\sharp$.

In addition, the time cost of forward reachability analysis with trace partitioning greatly depends on the number of created partitions, while typically $\check{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^\sharp)$ contains redundant elements in consecutive program points, thus adopting every element in $\check{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^\sharp)$ as partitioning directives may bring unnecessary burden to the forward reachability analysis without benefits in improving the precision. Therefore, in practice, we can keep the partitioning directives only for the program points of importance (e.g. the points immediately after external inputs) and discard the rest of them.

(2) Left-bound partitioning directives. Similar to the generation of right-bound partitioning directives from $\check{\mathcal{S}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^{\sharp})$, the left-bound partitioning directives are derived from the complement of $\hat{\mathcal{S}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^{\sharp})$ (i.e. $\mathcal{S}^{\sharp}_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathrm{I}^{\sharp}_{\mathsf{pre}}) \backslash \hat{\mathcal{S}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^{\sharp})$). Specifically, for any point ℓ, every element in $\mathcal{S}^{\sharp}_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathrm{I}^{\sharp}_{\mathsf{pre}})\ell \backslash \hat{\mathcal{S}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^{\sharp})\ell$ is a left-bound partitioning directive, if it is not $\bot^{\sharp}_{\mathbb{M}}$ and is valid with respect to all cognizance directives assigned to ℓ. The formal definition of left-bound partition function $\mathbb{P}^{\sharp}_{L}$ is:

$$
\begin{array}{rcll}
\mathbb{P}^{\sharp}_{L} & \in & \mathbb{L} \mapsto \wp(\mathcal{D}^{\sharp}_{\mathbb{M}}) & \text{left-bound partition function} \\
\mathbb{P}^{\sharp}_{L}(\ell) & \triangleq & \{\mathrm{M}^{\sharp}_{p} \mid \mathrm{M}^{\sharp}_{p} \in \mathcal{S}^{\sharp}_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathrm{I}^{\sharp}_{\mathsf{pre}})\ell \backslash \hat{\mathcal{S}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^{\sharp})\ell \wedge \mathrm{M}^{\sharp}_{p} \neq \bot^{\sharp}_{\mathbb{M}} \\
 & & \quad \wedge \forall d_c \in \mathbb{C}^{\sharp}(\ell).\ \mathrm{isValid}_{d}(d_c, \mathrm{M}^{\sharp}_{p})\} &
\end{array}
$$

By the definition of $\hat{\mathcal{S}}^{\sharp}_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^{\sharp})$, we know that from every partition generated by the left-bound partitioning directive, there must exist at least one concrete valid trace that fails the behavior $\mathcal{B}^{\sharp}$. Moreover, similar to the right-bound partitioning directives, it is of practical use to keep the left-bound partitioning directives only for the selected program points of importance and discard the rest of them.

(3) Dual-right-bound partitioning directives. Intuitively, the left-bound partitioning directives can determine the points from which there is still possibility to fail $\mathcal{B}^{\sharp}$, and the right-bound partitioning directives are used to determine the points at which $\mathcal{B}^{\sharp}$ is guaranteed and the responsibility analysis could stop. Besides these two types of partitioning directive, the responsibility analysis would benefit from another type of partitioning directive, which are used to determine the points at which the behavior $\mathcal{B}^{\sharp}$ is guaranteed to fail and the responsibility analysis can also stop. Such partitioning directives are called dual-right-bound partitioning directives, which marks the finishing point for responsibility analysis on the traces failing $\mathcal{B}^{\sharp}$; without such partitioning directives, the responsibility analysis may last much longer than necessary.

Theoretically, the dual-right-bound partitioning directives can be derived from backward impossible failure accessibility analyses for the complements of $\mathcal{B}$, but the cost of doing so would be prohibitive and the analysis results overlaps with the left-bound partitioning directives. In practice, to mark the finishing point of responsibility analysis on the traces failing $\mathcal{B}^\sharp$, we can simply use the complements of $\mathcal{B}^\sharp$, or more precisely, $\mathcal{S}^\sharp_{\overrightarrow{p\$}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{pre}})\backslash\mathcal{B}^\sharp$. Specifically, for every point ℓ of interest where the original behavior (before the refinement) $\mathcal{B}^\sharp(\ell) \neq \top^\sharp_{\mathbb{M}}$, we compute the complement of $\mathcal{B}^\sharp(\ell)$ which is represented by the disjunctive completion (e.g. a disjunction of affine inequalities for the polyhedron domain), do the meet with $\mathcal{S}^\sharp_{\overrightarrow{p\$}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{pre}})$ for every element in the disjunction, and collect the valid ones in the dual-right-bound partition function $\mathbb{P}^\sharp_{\tilde{R}}$. Usually, there are not many dual-right-bound partitioning directives, since the original behavior $\mathcal{B}^\sharp$ is specified $\top^\sharp_{\mathbb{M}}$ at most program points.

$$
\begin{array}{rcll}
\mathbb{P}^\sharp_{\tilde{R}} & \in & \mathbb{L} \mapsto \wp(\mathcal{D}^\sharp_{\mathbb{M}}) & \text{dual-right-bound partition function} \\
\mathbb{P}^\sharp_{\tilde{R}}(\ell) & \triangleq & \{\mathrm{M}^\sharp_p \mid \mathrm{M}^\sharp_p \in \mathcal{S}^\sharp_{\overrightarrow{p\$}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{pre}})\ell\backslash\mathcal{B}^\sharp(\ell) \wedge \mathrm{M}^\sharp_p \neq \bot^\sharp_{\mathbb{M}} \\
 & & \qquad \wedge \forall d_c \in \mathbb{C}^\sharp(\ell).\ \mathrm{isValid}_d(d_c, \mathrm{M}^\sharp_p)\} &
\end{array}
$$

(4) No-bound partitioning directives. In order to make sure that the trace partitioning automaton (or say, the extended transition system in [43]) constructed by the partitioning directives introduced above is a covering of the original transition system (i.e. every transition in the original transition system is simulated by at least one transition in the trace partitioning automaton), we introduce some complementary partitioning directives to ensure every reachable state is covered by at least one partition. Such partitioning directives are called no-bound partitioning directives, and we define a no-bound partition function $\mathbb{P}^\sharp_o \in \mathbb{L} \mapsto \wp(\mathcal{D}^\sharp_{\mathbb{M}})$.

Formally, it is required that: $\forall \ell \in \mathbb{L}.\ \cup\{\gamma_{\mathbb{M}}(\mathrm{M}_p^\sharp) \mid \mathrm{M}_p^\sharp \in \mathbb{P}_R^\sharp(\ell) \cup \mathbb{P}_L^\sharp(\ell) \cup \mathbb{P}_{\tilde{R}}^\sharp(\ell) \cup \mathbb{P}_o^\sharp(\ell)\} \supseteq \gamma_{\mathbb{M}}(\mathcal{S}_{\overrightarrow{ps}}^\sharp[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{pre}}^\sharp)\ell)$, where $\mathcal{S}_{\overrightarrow{ps}}^\sharp[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{pre}}^\sharp)\ell$ over-approximates the set of all reachable concrete environments at point ℓ. Ideally, the no-bound partitioning directives $\mathbb{P}_o^\sharp(\ell)$ can be computed by the subtraction of $\mathbb{P}_R^\sharp(\ell) \cup \mathbb{P}_L^\sharp(\ell) \cup \mathbb{P}_{\tilde{R}}^\sharp(\ell)$ from $\mathcal{S}_{\overrightarrow{ps}}^\sharp[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{pre}}^\sharp)\ell$. However, in some cases it may be difficult to do such a subtraction operation. If this happens, it is always safe to define $\mathbb{P}_o^\sharp(\ell) = \mathcal{S}_{\overrightarrow{ps}}^\sharp[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{pre}}^\sharp)\ell$, or even, $\mathbb{P}_o^\sharp(\ell) = \top_{\mathbb{M}}^\sharp$, which are guaranteed to be valid with respect to any cognizance function.

Combining the above four types of partitioning directives together, we can get a partition function $\mathbb{P}^\sharp \in \mathbb{L} \mapsto \wp(\mathcal{D}_{\mathbb{M}}^\sharp)$ such that $\mathbb{P}^\sharp(\ell) \triangleq \mathbb{P}_R^\sharp(\ell) \cup \mathbb{P}_L^\sharp(\ell) \cup \mathbb{P}_{\tilde{R}}^\sharp(\ell) \cup \mathbb{P}_o^\sharp(\ell)$. For every program point ℓ, every partitioning directive in $\mathbb{P}^\sharp(\ell)$ is valid with respect to every cognizance directive d_c in $\mathbb{C}^\sharp(\ell)$, thus by the definition of $\mathrm{isValid}_{\mathbb{P}}$, the partition function $\mathbb{P}^\sharp$ is valid with respect to the cognizance function $\mathbb{C}^\sharp$. Besides, it is assumed that $\mathbb{P}^\sharp(\ell_0) = \emptyset$ for the dummy initial point ℓ_0, such that the correspondingly constructed trace partitioning automaton has only one initial node.

Example 26 (Access Control, Continued) *Using the backward analysis result $\check{\mathcal{S}}_{\overleftarrow{if}}^\sharp[\![\mathrm{P}]\!](\mathcal{B}^\sharp)$ and $\mathcal{S}_{\overrightarrow{ps}}^\sharp[\![\mathrm{P}]\!](\mathsf{I}_{\mathsf{pre}}^\sharp) \backslash \hat{\mathcal{S}}_{\overleftarrow{if}}^\sharp[\![\mathrm{P}]\!](\mathcal{B}^\sharp)$ from the example 25, here we generate partitioning directives for two different cognizance functions that are specified in the example 23.*

1) Consider the omniscient cognizance function $\mathbb{C}_o^\sharp$ such that $\mathbb{C}_o^\sharp(\ell) = \{\bot_{\mathbb{M}}^\sharp\}$ for every point $\ell \in \mathbb{L}$. In this case, every partitioning directive is trivially valid with respect to $\mathbb{C}_o^\sharp$, and the corresponding partition function $\mathbb{P}^\sharp$ is displayed in table 8.5. As mentioned before, the partition function $\mathbb{P}^\sharp$ may keep the partitioning directives only for the selected program points of importance, and in this example such program points include: ℓ_1 that is immediately after the variable initialization action (i.e. the dummy initial action); ℓ_3, ℓ_5 and ℓ_7 that are

immediately after external inputs; and ℓ_8 that is specified with the behavior $\mathcal{B}^\sharp$ of interest. Meanwhile, the partitioning directives at other points (ℓ_2, ℓ_4 and ℓ_6) are optional and would not affect the final result of abstract responsibility analysis, thus are omitted here.

ℓ	$\mathbb{P}^\sharp_R(\ell)$	$\mathbb{P}^\sharp_L(\ell)$	$\mathbb{P}^\sharp_{\tilde{R}}(\ell)$	$\mathbb{P}^\sharp_o(\ell)$
ℓ_0	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
ℓ_1	$\emptyset$	$\{\top^\sharp_{\mathbb{M}}\}$	$\emptyset$	$\emptyset$
ℓ_2	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
ℓ_3	$\emptyset$	$\{apv \in [1;1] \wedge i1 \in [\mathbf{1};\mathbf{2}]\}$	$\emptyset$	$\{apv \in [1;1] \wedge i1 \in [\mathbf{\text{-}1};\mathbf{0}]\}$
ℓ_4	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
ℓ_5	$\{apv \in [\mathbf{1};\mathbf{1}] \wedge i1 \in [\text{-}1;2] \wedge i2 \in [\mathbf{\text{-}1};\mathbf{0}]\}$	$\{apv \in [\mathbf{1};\mathbf{1}] \wedge i1 \in [\text{-}1;2] \wedge i2 \in [\mathbf{1};\mathbf{2}]\}$	$\emptyset$	$\{apv \in [\mathbf{\text{-}1};\mathbf{0}] \wedge i1 \in [\text{-}1;2] \wedge i2 \in [\mathbf{\text{-}1};\mathbf{2}]\}$
ℓ_6	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
ℓ_7	$apv \in [\mathbf{\text{-}1};\mathbf{0}] \wedge i1 \in [\text{-}1;2] \wedge i2 \in [\text{-}1;2] \wedge typ \in [1;2]$	$\{apv \in [\mathbf{1};\mathbf{1}] \wedge i1 \in [\text{-}1;2] \wedge i2 \in [\text{-}1;2] \wedge typ \in [1;2]\}$	$\emptyset$	$\emptyset$
ℓ_8	$\{apv \in [\text{-}1;1] \wedge i1 \in [\text{-}1;2] \wedge i2 \in [\text{-}1;2] \wedge typ \in [1;2] \wedge acs \in [\mathbf{\text{-}2};\mathbf{0}]\}$	$\{apv \in [\text{-}1;1] \wedge i1 \in [\text{-}1;2] \wedge i2 \in [\text{-}1;2] \wedge typ \in [1;2] \wedge acs \in [\mathbf{1};\mathbf{2}]\}$	$\mathbb{P}^\sharp_L(\ell_8)$	$\emptyset$

Table 8.5: The Partition Function for the Omnisicent Cognizance

Take the point ℓ_5 as an example, the forward reachability semantics $\mathcal{S}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{pre}})\ell_5 = apv \in [\text{-}1;1] \wedge i1 \in [\text{-}1;2] \wedge i2 \in [\text{-}1;2]$ is partitioned into three parts: the right-bound partitioning directives $\mathbb{P}^\sharp_R(\ell_5) = \{apv \in [1;1] \wedge i1 \in [\text{-}1;2] \wedge i2 \in [\text{-}1;0]\}$ that guarantee "the access to o fails"; the left-bound partitioning directives $\mathbb{P}^\sharp_L(\ell_5) = \{apv \in [1;1] \wedge i1 \in [\text{-}1;2] \wedge i2 \in [1;2]\}$, which ensures there exists at least one valid concrete trace such that "the access to o succeeds"; the no-bound partitioning directives $\mathbb{P}^\sharp_o(\ell_5) = \{apv \in [\text{-}1;0] \wedge i1 \in [\text{-}1;2] \wedge i2 \in [\text{-}1;2]\}$ are complementary to the two other types of partitioning directives such that every reachable environment at point ℓ_5 is covered. Although $\mathbb{P}^\sharp_o(\ell_5)$ actually guarantee

"the access to o fails" in this very example, we cannot take advantage of this information, since typically the no-bound partitioning directives cannot guarantee anything.

2) Consider a non-omniscient cognizance function $\mathbb{C}^\sharp$ *such that, if* $\ell \in \{\ell_0, \ell_1, \ell_2\}$*, then* $\mathbb{C}^\sharp(\ell) = \{\bot^\sharp_{\mathbb{M}}\}$*, otherwise* $\mathbb{C}^\sharp(\ell) = \{i1 \in [-1; 2]\}$*. In this case, every partitioning directive from the table 8.5 needs to be checked with respect to the cognizance. Since the abstract environment domain is the interval domain, checking the validity of partitioning directives is quite easy by the condition (7.9), and we can find that only the partitioning directives at point* ℓ_3 *are invalid. Take* $\mathrm{M}^\sharp_p = apv \in [1; 1] \wedge i1 \in [1; 2] \in \mathbb{P}^\sharp_L(\ell_3)$ *as an example, the only cognizance directive at* ℓ_3 *is* $\mathrm{d}_c = i1 \in [-1; 2] \in \mathbb{C}^\sharp(\ell_3)$*, thus* $\mathrm{M}^\sharp_p|_{vars(\mathrm{M}^\sharp_p)\cap vars(\mathrm{d}_c)} = i1 \in [1; 2]$*, and it is obvious the condition (7.9) does not hold. Similarly, the partitioning directive in* $\mathbb{P}^\sharp_o(\ell_3)$ *is found invalid. Therefore, after removing the invalid partitioning directives at* ℓ_3*, we get the partition function as in table 8.6, which is valid with respect to* $\mathbb{C}^\sharp$*.*

ℓ	$\mathbb{P}^\sharp_R(\ell)$	$\mathbb{P}^\sharp_L(\ell)$	$\mathbb{P}^\sharp_{\tilde{R}}(\ell)$	$\mathbb{P}^\sharp_o(\ell)$
ℓ_0	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
ℓ_1	$\emptyset$	$\{\top^\sharp_{\mathbb{M}}\}$	$\emptyset$	$\emptyset$
ℓ_2	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
ℓ_3	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
ℓ_4	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
ℓ_5	$\{apv \in [\mathbf{1}; \mathbf{1}] \wedge i1 \in [\text{-}1; 2] \wedge i2 \in [\text{-}\mathbf{1}; \mathbf{0}]\}$	$\{apv \in [\mathbf{1}; \mathbf{1}] \wedge i1 \in [\text{-}1; 2] \wedge i2 \in [\mathbf{1}; \mathbf{2}]\}$	$\emptyset$	$\{apv \in [\text{-}\mathbf{1}; \mathbf{0}] \wedge i1 \in [\text{-}1; 2] \wedge i2 \in [\text{-}\mathbf{1}; \mathbf{2}]\}$
ℓ_6	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
ℓ_7	$apv \in [\text{-}\mathbf{1}; \mathbf{0}] \wedge i1 \in [\text{-}1; 2] \wedge i2 \in [\text{-}1; 2] \wedge typ \in [1; 2]$	$\{apv \in [\mathbf{1}; \mathbf{1}] \wedge i1 \in [\text{-}1; 2] \wedge i2 \in [\text{-}1; 2] \wedge typ \in [1; 2]\}$	$\emptyset$	$\emptyset$
ℓ_8	$\{apv \in [\text{-}1; 1] \wedge i1 \in [\text{-}1; 2] \wedge i2 \in [\text{-}1; 2] \wedge typ \in [1; 2] \wedge acs \in [\text{-}\mathbf{2}; \mathbf{0}]\}$	$\{apv \in [\text{-}1; 1] \wedge i1 \in [\text{-}1; 2] \wedge i2 \in [\text{-}1; 2] \wedge typ \in [1; 2] \wedge acs \in [\mathbf{1}; \mathbf{2}]\}$	$\mathbb{P}^\sharp_L(\ell_8)$	$\emptyset$

Table 8.6: The Partition Function for the Non-omnisicent Cognizance

8.1.3 The Forward Analysis Phase

The objective of this forward analysis phase is to construct a trace partitioning automaton with the partitioning directives from the last phase, mark left bounds and right bounds of responsibility in the automaton, and determine responsible entities.

Trace Partitioning Automaton Generation. Using the partitioning directives generated in the last backward analysis phase (i.e. $\{\text{part}\langle \text{Inv}, \ell, \mathrm{M}_p^\sharp\rangle \mid \ell \in \mathbb{L} \wedge \mathrm{M}_p^\sharp \in \mathbb{P}^\sharp(\ell)\}$) and optionally the partitioning directives based on the control flow (e.g. $\text{part}\langle \text{If}, \ell, b\rangle$), we perform an over-approximating forward reachability analysis with trace partitioning (chapter 3), compute the refined forward reachability semantics and construct a trace partitioning automaton. Specially, the nodes generated by left-bound partitioning directives are marked as "*left-bound nodes*" in the automaton, the nodes generated by right-bound partitioning directives are marked as "*right-bound nodes*", and the nodes generated by dual-right-bound partitioning directives are marked as "*dual-right-bound nodes*".

Furthermore, after the forward reachability analysis with trace partitioning completes, we can improve the constructed automaton by propagating the right-bounds or dual-right-bounds: for any node in the automaton which is not marked as any bound, if all its successors are marked as right-bound nodes (respectively, dual-right-bound nodes), we mark this node as a right-bound node (respectively, a dual-right-bound node) as well.

Determining Responsible Entities. Now, we can determine the responsibility in the generated trace partitioning automaton. The intuition is: every path in the automaton represents a set of concrete traces; if a path contains a dual-right-bound node, then the path does not have the behavior $\mathcal{B}^\sharp$, hence there is no responsible entity along this path;

otherwise, the responsible entities are the edges (i.e. actions), which are located after the left-bound nodes (if any) and before the right-bound nodes (if any) along the path. That is to say, for any path that does not contain a dual-right-bound node, all the actions between the rightmost left-bound node (if any) and the leftmost right-bound node (if any) are potentially responsible for the behavior $\mathcal{B}^\sharp$. Specially, if there is neither a left-bound node nor a right-bound node along a certain path, then the analysis is not precise enough and every action along that path would be determined as potentially responsible.

Since only the actions with free choices can be possibly responsible for a behavior, we can further restrict the potentially responsible entities to the actions such as external inputs, random number generation, and variable initialization (which is mimicked as the dummy initial action).

In addition, we do not only find potentially responsible entities, but also get some hints on when these entities are actually responsible, and this is the so called "responsible under the condition". Suppose an edge $\langle \ell,\ t,\ \mathrm{M}^\sharp \rangle \rightarrow \langle \ell',\ d_p :: t,\ \mathrm{M}^{\sharp\prime} \rangle$ in the automaton is found potentially responsible, it means that the action a from ℓ to ℓ' (which can be retrieved from the program source code) is potentially responsible under the condition that the partitioning token t holds at point ℓ and the action a satisfies the partitioning directive d_p. For example, for the access control program in Fig. 1.4, the edge $\langle \ell_4,\ t,\ \mathrm{M}^\sharp \rangle \rightarrow \langle \ell_5,\ d_p :: t,\ \mathrm{M}^{\sharp\prime} \rangle$ is determined responsible, where $t = \mathit{apv} \in [1;1] \wedge \mathit{i1} \in [1;2]$ and $d_p = \mathit{apv} \in [1;1] \wedge \mathit{i1} \in [\text{-}1;2] \wedge \mathit{i2} \in [\text{-}1;0]$. Instead of claiming that the action $\mathit{i2} := [\text{-}1;2]$ is responsible for "the access to o fails" in all executions, we state that $\mathit{i2} := [\text{-}1;2]$ is responsible under the condition that: the partitioning token $\mathit{apv} \in [1;1] \wedge \mathit{i1} \in [1;2]$ holds at ℓ_4, and the action $\mathit{i2} := [\text{-}1;2]$ satisfies the new partitioning

directive $apv \in [1;1] \wedge i1 \in [\text{-}1;2] \wedge i2 \in [\text{-}1;0]$. That is to say, the input from 2nd admin is responsible for the behavior "the access to o fails" if the input from 1st admin is positive and the input from 2nd admin is negative or zero, which is much more informative than simply claiming the input from 2nd admin is responsible.

Termination or a New Round of Analysis. Up until this step, we have already successfully inferred some information about the responsible entities. If such an analysis result is satisfactory or the time and cost exceeds the prespecified threshold, we could terminate the analyzer and return the found responsible entities to the user. Otherwise, if the precision of forward reachability semantics $\mathcal{S}^{\sharp}_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^{\sharp}_{\mathsf{pre}})$ is improved in the last forward analysis phase, then we could start a new round of backward accessibility analysis (section 8.1.2) followed by the forward reachability analysis (section 8.1.3) to seek for more precise responsibility analysis results.

Intuitively, in the new round of analysis, using the refined behavior of interest (possibly with the disjunctive completion), the backward impossible failure accessibility analysis is expected to be more precise, which creates more partitioning directives to construct a refined automaton, and further improves the responsibility analysis result. The extreme case is that we create as many partitioning directives as possible and construct the most precise trace partitioning automaton, such that every path in the automaton represents a single concrete valid trace. From such a trace partitioning automaton, we can get exactly the same analysis result as the concrete responsibility analysis (part II), yet the time cost is in general prohibitive.

Example 27 (Access Control, Continued) *Following the example 26, we conduct a for-*

ward reachability analysis with trace partitioning, construct the trace partitioning automaton and determine responsible entities. Since the partition function varies for different cognizance functions, the corresponding constructed trace partitioning automata are different.

1) First, consider the omniscient cognizance function $\mathbb{C}^\sharp_o$. In this case, we adopt the partitioning directives from the partition function defined in the table 8.5, and the correspondingly constructed trace partitioning automaton is displayed in Fig. 8.2, in which various types of nodes are represented by different circles.

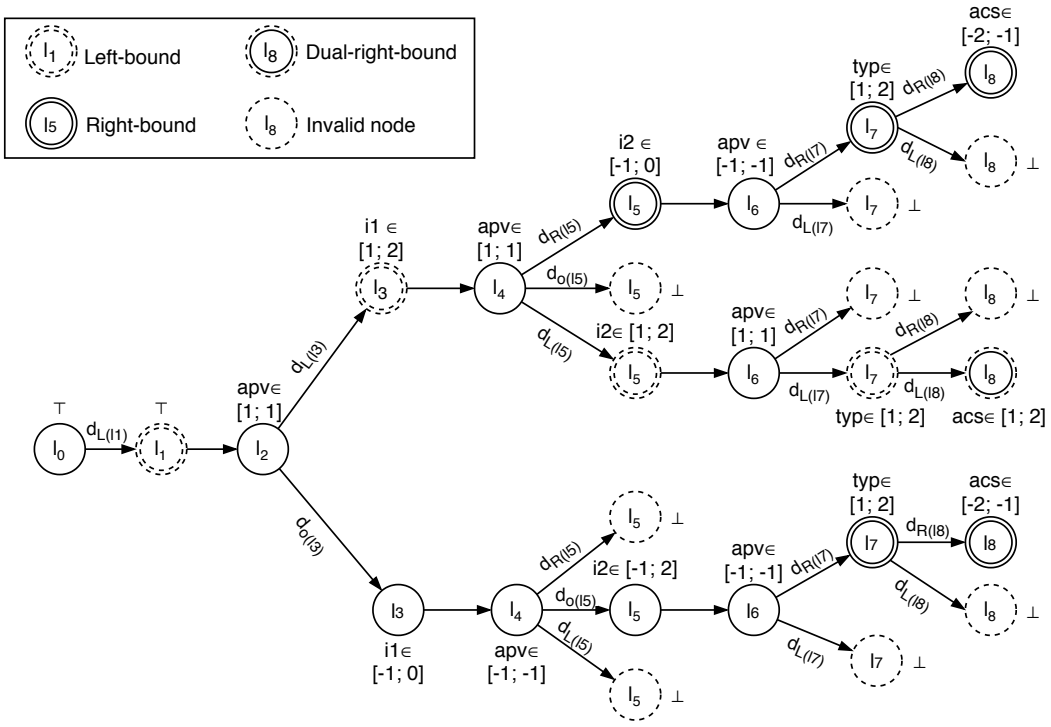

Figure 8.2: Trace Partitioning Automaton for the Omniscient Cognizance

Since there is at most one element in $\mathbb{P}^\sharp_L(\ell)$ for every program point ℓ, we simply use the notation $\mathrm{d}_{L(\ell)}$ for short to refer the partitioning directive part$\langle Inv,\ \ell,\ \mathrm{M}^\sharp\rangle$, where $\mathrm{M}^\sharp$ is the only element in $\mathbb{P}^\sharp_L(\ell)$. For instance, $\mathrm{d}_{L(\ell_3)}$ refers to the partitioning directive part$\langle Inv,\ \ell,$

apv $\in [1;1] \wedge$ *i1* $\in [\mathbf{1};\mathbf{2}]\rangle$, *where apv* $\in [1;1] \wedge$ *i1* $\in [\mathbf{1};\mathbf{2}] \in \mathbb{P}^\sharp_L(\ell_3)$. *Similarly, we use the notations* $\mathrm{d}_{R(\ell)}$, $\mathrm{d}_{\tilde{R}(\ell)}$ *and* $\mathrm{d}_{o(\ell)}$ *to refer the partitioning directives from* $\mathbb{P}^\sharp_R(\ell)$, $\mathbb{P}^\sharp_{\tilde{R}}(\ell)$, *and* $\mathbb{P}^\sharp_o(\ell)$. *Besides, for the sake of conciseness, instead of explicitly drawing partitioning tokens inside the nodes of the automaton, we comment some edges with a partitioning directive* d *such that every node after the edge has the partitioning directive* d *pushed into its stack of directives (i.e. the partitioning token). For instance, for the node at point* ℓ_3 *with double dashed circles in upper path of the automaton, its partitioning token is "*$\mathrm{d}_{L(\ell_3)} :: \mathrm{d}_{L(\ell_1)}$*".*

Furthermore, the automaton in Fig. 8.2 can be refined by removing the invalid node whose associated abstract environment element is $\bot^\sharp_{\mathbb{M}}$ *(i.e. it is unreachable) and propagating right-bound nodes, and we get a simpler trace partitioning automaton as in Fig. 8.3. For example, the node at point* ℓ_5 *created by* $\mathrm{d}_{o(\ell_5)}$ *in the upper path is invalid and can be removed; the node at point* ℓ_6 *in the lower path has only one valid successor that is marked as a right-bound node, thus we mark the node at point* ℓ_6 *also as a right-bound node, as well as its predecessors.*

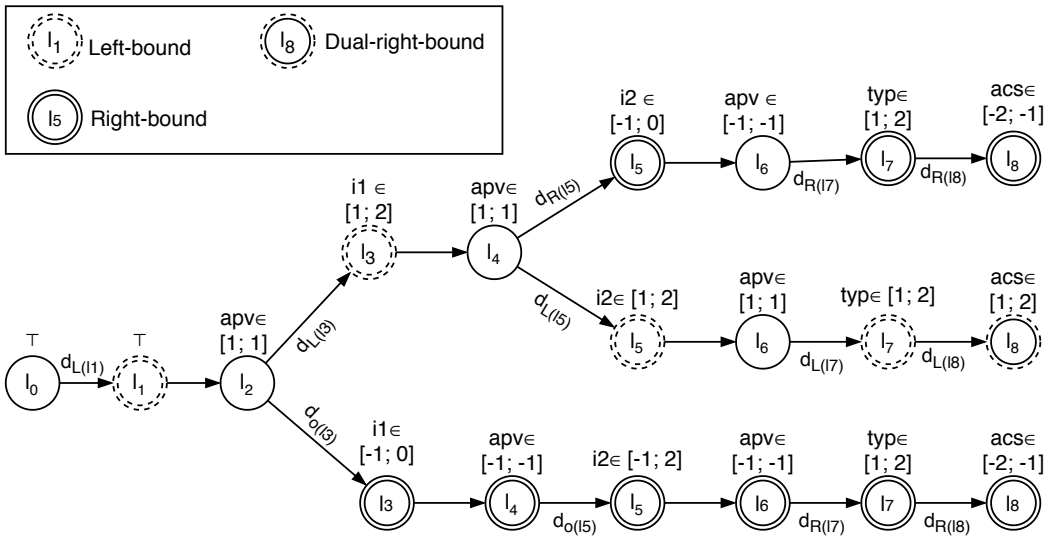

Figure 8.3: The Refined Trace Partitioning Automaton for the Omniscient Cognizance

From the above automaton, we can clearly see that there are three maximal paths from ℓ_0 *to* ℓ_8 *in the automaton, which over-approximate all the concrete valid traces of the program.*

For the upper path, the rightmost left-bound node is at ℓ_3 *and the leftmost right-bound node is at* ℓ_5*, thus the responsible entities must be located between* ℓ_3 *and* ℓ_5*. Since the action "apv* $:= (i1 \leq 0)\ ?\ \text{-}1 : apv$*" has no free choice, only the action "i2* $:= [\text{-}1; 2]$*" is determined responsible under the condition: apv* $\in [1; 1] \wedge i1 \in [1; 2]$ *hold at point* ℓ_4*, and the action "i2* $:= [\text{-}1; 2]$*" satisfies apv* $\in [1; 1] \wedge i1 \in [\text{-}1; 2] \wedge i2 \in [1; 2]$*. It indicates that, the input from 2nd admin is responsible if the input from 1st admin is positive and the input from 2nd admin is negative or zero.*

For the path in the middle, the node at ℓ_8 *is marked as a dual-right-bound node, which means that every concrete trace represented by this path does not have the behavior "the access to o fails". Thus, there is no responsible entity along this path.*

For the lower path, the rightmost left-bound node is at ℓ_1 *and the leftmost right-bound node is at* ℓ_3*. Since the action "apv* $:= 1$*" from* ℓ_1 *to* ℓ_2 *has no free choice, only the action i1* $:= [\text{-}1; 2]$ *from* ℓ_2 *to* ℓ_3 *is determined responsible, under the condition that apv* $\in [1; 1] \wedge i1 \in [-1; 0]$ *holds at point* ℓ_3*. That is to say, the input from 1st admin is responsible if it is* $\text{-}1$ *or* 0*.*

To sum up, for the omniscient cognizance in the access control program example, the abstract responsibility analysis finds that the input from 1st admin or 2nd admin is potentially responsible for "the access to o fails" under certain conditions, while other actions with free choice (e.g. the variable initialization, and the input from system settings) are not responsible. This analysis result is almost as precise as the concrete responsibility analysis, thus there is no need to conduct a new round of analysis and we can terminate the analysis here.

2) Second, consider the trace partitioning automaton constructed for the non-omniscient

cognizance function $\mathbb{C}^\sharp$ such that the observer does not know the input of 1st admin (i.e. the observer cannot distinguish the value of i1 in the interval $[-1; 2]$). In this case, we adopt the partitioning directives from the partition function defined in table 8.6, and the correspondingly constructed trace partitioning automaton is in Fig. 8.4, in which we represent various types of nodes by different circles as in Fig. 8.2.

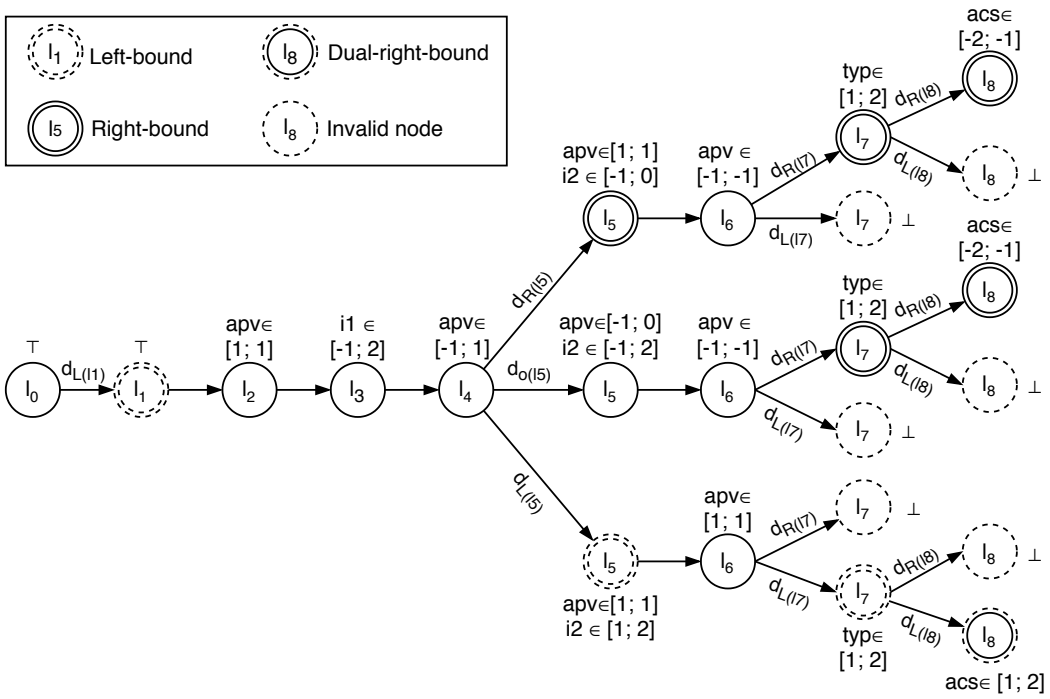

Figure 8.4: The Trace Partitioning Automaton for a Non-omniscient Cognizance

Compared with the trace partitioning automaton for the omniscient cognizance, we do not have the partitioning directives at point l_3, while the partitioning directives at other points are still valid and preserved. After removing the invalid nodes and propagating right-bound nodes, the refined trace partitioning automaton is in Fig.8.5.

Similar to the automaton in Fig.8.3, there are three maximal paths in the refined automa-

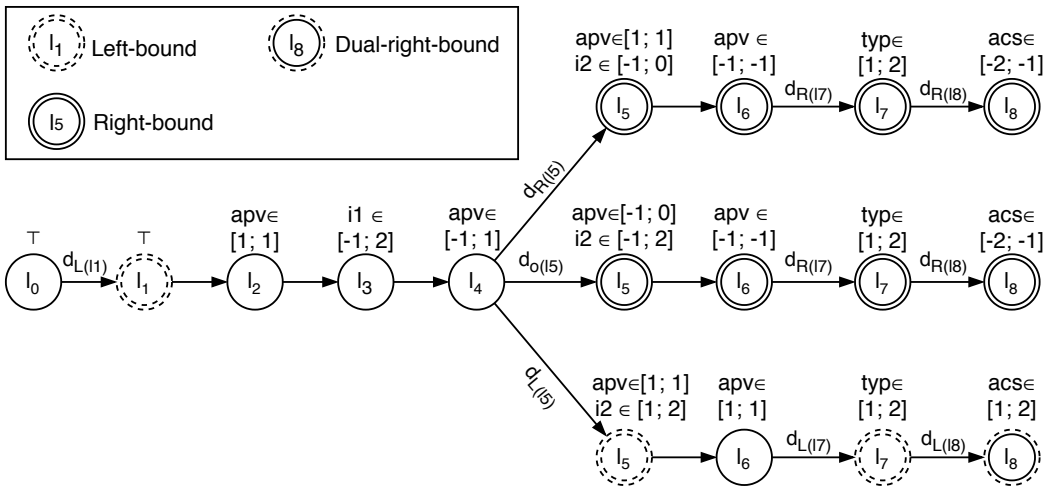

Figure 8.5: The Refined Trace Partitioning Automaton for a Non-omniscient Cognizance

ton for the non-omniscient cognizance, which over-approximate the concrete valid traces.

For the lower path, the node at ℓ_8 is marked as a dual-right-bound node, which means that the behavior of interest does not hold, thus there is no responsible entity along the path.

In contrast, along both the upper path and the middle path, the rightmost left-bound node is at point ℓ_1 and the leftmost right-bound node is at point ℓ_5, thus the responsible entities must be located between ℓ_1 and ℓ_5. After filtering out the actions without free choices, we would determine both "i1 $:= [-1; 2]$*" and "i2* $:= [-1; 2]$*" potentially responsible for the behavior. More precisely, "i1* $:= [-1; 2]$*" is responsible under no condition, while "i2* $:= [-1; 2]$*" is responsible under the condition that the partitioning directive apv* $\in [1; 1] \wedge$ *i1* $\in [-1; 2] \wedge$ *i2* $\in [-1; 0]$ *or apv* $\in [-1; 0] \wedge$ *i1* $\in [-1; 2] \wedge$ *i2* $\in [-1; 2]$ *holds at point ℓ_5.*

To sum up, for the non-omniscient cognizance such that the observer does not know the input from 1st admin, the abstract responsibility analysis find both the input from 1st admin and the input from 2nd admin are potentially responsible for the behavior "the access to o

fails" in every execution where the behavior occurs. Compared with the concrete responsibility analysis that determines only the input from 2nd admin responsible, this abstract analysis result is less precise, but it is still sound, since every entity that is responsible in the concrete is also found responsible in the abstract. □

8.2 The Soundness of Abstract Responsibility Analysis

In this section, we prove that the abstract responsibility analysis introduced in section 8.1 is sound with respect to the concrete responsibility analysis defined in section 5.4.

Theorem 3 *Every entity that is responsible in the concrete must be found responsible in the abstract responsibility analysis.*

Proof. Given a program P along with the user specified behavior of interest $\mathcal{B}^\sharp \in \mathbb{L} \mapsto \mathcal{D}^\sharp_{\mathbb{M}}$ and cognizance function $\mathbb{C}^\sharp \in \mathbb{L} \mapsto \wp(\mathcal{D}^\sharp_{\mathbb{M}})$, the corresponding concrete behavior of interest $\mathcal{B}$ and lattice of concrete behaviors $\mathcal{L}^{\mathsf{Max}}$ are formalized in section 7.1, as well as the concrete cognizance function $\mathbb{C}$ in section 7.2. Suppose that the behavior $\mathcal{B}$ holds in a valid concrete trace σ of P, and a concrete transition $\tau = \langle \ell,\ \rho\rangle \xrightarrow{a} \langle \ell',\ \rho'\rangle$ (in which a may be omitted and can be retrieved from the source code) in σ is found responsible for $\mathcal{B}$ by the definition 5.5 of concrete responsibility analysis (i.e. the trace σ is splitted into $\sigma = \sigma_{\mathrm{H}}\tau\sigma_{\mathrm{F}}$ such that $\emptyset \subsetneq \mathbb{O}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma_{\mathrm{H}}\tau) \subseteq \mathcal{B} \wedge \mathbb{O}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma_{\mathrm{H}}) \not\subseteq \mathcal{B}$), then we would like to prove that the action a must be found responsible in the abstract responsibility analysis.

Since the trace partitioning automaton constructed in the abstract responsibility analysis is a covering of the concrete trace semantics of P, every valid concrete trace

is simulated by at least one path in the automaton. Let $\sigma^\sharp$ be a path in the trace partitioning automaton that simulates the concrete trace σ, and $\tau^\sharp = \langle \ell,\ t,\ \mathrm{M}^\sharp \rangle \xrightarrow{a} \langle \ell',\ t',\ \mathrm{M}^{\sharp\prime} \rangle \in (\mathbb{L}_T \times \mathcal{D}^\sharp_{\mathbb{M}}) \times (\mathbb{L}_T \times \mathcal{D}^\sharp_{\mathbb{M}})$ be the edge on the path $\sigma^\sharp$ that represents the transition τ. Thus, we need to prove that $\tau^\sharp$ must be found responsible in the abstract responsibility analysis.

To start with, we prove that there is no dual-right-bound node along the abstract path $\sigma^\sharp$ by contradiction. Assume there is a dual-right-bound node at point $\ell_{\tilde{R}}$ on $\sigma^\sharp$, which is created by a dual-right-bound partitioning directive part$\langle \mathrm{Inv},\ \ell_{\tilde{R}},\ \mathrm{M}^\sharp_{\tilde{R}} \rangle$. By the definition of dual-right-bound partition function, we know that $\mathrm{M}^\sharp_{\tilde{R}}$ guarantees the complement of $\mathcal{B}^\sharp$ (i.e. $\mathrm{M}^\sharp_{\tilde{R}} \in \mathcal{S}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{pre}})\ell_{\tilde{R}} \backslash \mathcal{B}^\sharp(\ell_{\tilde{R}})$), thus all the concrete traces represented by $\sigma^\sharp$ must fail the behavior $\mathcal{B}$ at point $\ell_{\tilde{R}}$. This contradicts with our assumption that σ is simulated by $\sigma^\sharp$ and the behavior $\mathcal{B}$ holds in σ. Thus, along the path $\sigma^\sharp$, there is no dual-right-bound node, and all the edges between the rightmost left-bound-node (if any) and the leftmost right-bound-node are determined potentially responsible by the abstract responsibility analysis. Specially, if there is no left-bound-node or right-bound-node along $\sigma^\sharp$, every edge is determined potentially responsible, which obviously includes $\tau^\sharp$.

Furthermore, we prove that if there is a left-bound node along $\sigma^\sharp$, then $\tau^\sharp$ must be located after that node. Assume that there is a left-bound node along $\sigma^\sharp$, which is created by a left-bound partitioning directive part$\langle \mathrm{Inv},\ \ell_L,\ \mathrm{M}^\sharp_L \rangle$, and a concrete state $s_L = \langle \ell_L,\ \rho_L \rangle$ on σ is represented by the left-bound node. By the definition of the left-bound partition function, the abstract environment $\mathrm{M}^\sharp_L$ is from the complement of the over-approximating backward impossible failure semantics for the behavior $\mathcal{B}^\sharp$ (i.e. $\mathrm{M}^\sharp_L \in \mathcal{S}^\sharp_{\overrightarrow{ps}}[\![\mathrm{P}]\!](\mathsf{I}^\sharp_{\mathsf{pre}})\ell_L \backslash \hat{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^\sharp)\ell_L$). That is to say, from every concrete state that is

represented by the left-bound node, there must exist at least one valid concrete trace that fails the behavior $\mathcal{B}$. If we split σ into σ' and σ'' such that σ' ends with s_L while σ'' begins with s_L, then it is obvious that σ' cannot guarantee the occurrence of $\mathcal{B}$, thus $\mathbb{I}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma') \not\subseteq \mathcal{B}$. Since $\mathbb{I}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma') \subseteq \mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma')$, we have $\mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma') \not\subseteq \mathcal{B}$. As $\mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma_{\mathrm{H}}\tau) \subseteq \mathcal{B}$ and the observation function $\mathbb{O}$ is decreasing (lemma 3), we find that $\sigma_{\mathrm{H}}\tau$ must be greater (longer) than σ'. Therefore, the responsible transition τ must be located after the state s_L, and accordingly the edge $\tau^\sharp$ must be located after the left-bound node.

Last, we prove that if there is a right-bound node along $\sigma^\sharp$, then $\tau^\sharp$ must be located before that node. Assume that there is a right-bound node along $\sigma^\sharp$, which is created by a right-bound partitioning directive part$\langle \mathrm{Inv},\ \ell_R,\ \mathrm{M}^\sharp_R \rangle$, and a concrete state $s_R = \langle \ell_R,\ \rho_R \rangle$ on σ is represented by the right-bound node. By the definition of the right-bound partition function, the abstract environment $\mathrm{M}^\sharp_R$ is from the under-approximating backward impossible failure semantics for the behavior $\mathcal{B}^\sharp$ (i.e. $\mathrm{M}^\sharp_R = \check{\mathcal{S}}^\sharp_{\overleftarrow{if}}[\![\mathrm{P}]\!](\mathcal{B}^\sharp)\ell_R$). That is to say, every concrete trace starting from the states represented by the right-bound node is guaranteed to have the behavior $\mathcal{B}$. If we split σ into σ' and σ'' such that σ' ends with s_R while σ'' begins with s_R, then it is easy to know $\mathcal{B}$ holds in σ' (since $\mathcal{B}$ holds in the whole trace σ), and every trace with the prefix σ' is guaranteed to have the behavior $\mathcal{B}$. Hence, we get $\mathbb{I}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma') \subseteq \mathcal{B}$. Now we consider the traces that are equivalent to σ' according to the cognizance $\mathbb{C}^\sharp$. For any trace σ'_e such that $\sigma'_e \overset{\mathbb{C}^\sharp}{\sim} \sigma'$, the behavior $\mathcal{B}$ must hold during the execution of σ'_e (since $\mathbb{O}([\![\mathrm{P}]\!]^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma_{\mathrm{H}}\tau) \subseteq \mathcal{B}$). By the theorem 2, σ'_e must be represented by the same path as σ' in the automaton, thus the last state in σ'_e is also represented by the same right-bound node in the automaton. Thus,

every trace with the prefix σ'_e is guaranteed to have the behavior $\mathcal{B}$, which implies that $\mathbb{I}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \sigma'_e) \subseteq \mathcal{B}$. By the definition of $\mathbb{O}$, we get $\mathbb{O}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma') \subseteq \mathcal{B}$. Since the observation function $\mathbb{O}$ is decreasing (lemma 3) and $\mathbb{O}(\llbracket \mathrm{P} \rrbracket^{\mathsf{Max}}, \mathcal{L}^{\mathsf{Max}}, \mathbb{C}, \sigma_{\mathrm{H}}) \not\subseteq \mathcal{B}$, it is easy to see that σ' is strictly greater (longer) than σ_{H}. Therefore, the responsible transition τ must be located before the state s_R, and accordingly the edge $\tau^\sharp$ must be located before the right-bound node.

To sum up, we have proved that for every concrete trace σ with a responsible entity which is a transition $\tau = \langle \ell,\ \rho \rangle \xrightarrow{a} \langle \ell',\ \rho' \rangle$, there exists an abstract path $\sigma^\sharp$ with an edge $\tau^\sharp = \langle \ell,\ t,\ \mathrm{M}^\sharp \rangle \xrightarrow{a} \langle \ell',\ t',\ \mathrm{M}^{\sharp\prime} \rangle$ in the corresponding trace partitioning automaton, and the edge $\tau^\sharp$ must be located after all the left-bound nodes (if any) and before all the right-bound nodes (if any) on the path $\sigma^\sharp$. Thus, by the abstract responsibility analysis designed in section 8.1, the edge $\tau^\sharp$ must be determined responsible for $\mathcal{B}^\sharp$. □

Chapter 9

Conclusion

This dissertation formally defines responsibility as an abstraction of trace semantics. Typically, the responsibility analysis consists of four steps: collect the trace semantics, build a lattice of system behaviors of interest, create an observation function for each observer, and apply the responsibility abstraction on analyzed traces. Compared to current dependency and causality analysis methods, the responsibility analysis is demonstrated to be more generic and precise in several examples. In addition, a sound framework of abstract responsibility analysis is proposed, which is based on trace partitioning automata constructed by the iteration of over-approximating forward reachability analysis with trace partitioning and under-approximating/over-approximating backward impossible failure accessibility analysis. It is guaranteed that actions that are not found responsible in the abstract analysis are definitely not responsible in the concrete.

We hope this dissertation has successfully demonstrated that the responsibility analysis constitutes a worthy avenue of research. In the future, there are a number of directions that deserve further exploration.

Analysis of Probabilistic Programs. The definition of responsibility proposed in this dissertation can be extended to probabilistic programming languages such that the degree of responsibility of each responsible entity can be quantified, which is similar to the degree of blame designed to quantify actual causality [36]. More precisely, instead of identifying a single responsible entity for each specific trace as in (5.5), we can collect all the potentially responsible entities for the whole system, and assign to each of them with a probability of being responsible for the behavior of interest.

Generalization of Abstract Analysis. The framework of abstract responsibility analysis can be applied to new abstract domains other than the classic numeric domains discussed in this dissertation, such that we can analyze the responsibility of more behaviors (which cannot be expressed by intervals, octagons or polyhedra). The main challenges are expected to come from designing a sound under-approximating backward impossible failure accessibility analysis for the new abstract domain. In addition, we suggest specifying the abstract cognizance function by abstract relational invariants [40, 37] that can directly express relational properties about two executions of the program, such that we don't have the restrictions that two equivalent traces must be of the same length and have the same control flow.

Alternative Definitions of Responsibility. In the philosophy literature, there is a protracted controversy concerning the meaning of responsibility. Just like the law varies from one nation to another, there cannot exist a perfect universal rule of defining responsibility [46] that deals well with all scenarios. In our current definition (5.5), whether a transition τ_{R} (or say, the corresponding action a_{R}) is responsible or not in the trace $\sigma_{\mathrm{H}}\tau_{\mathrm{R}}\sigma_{\mathrm{F}}$ solely depends on its history σ_{H}, while its future σ_{F} has no impact on deciding

the responsibility. For instance, in the forest fire example, whether an arsonist A is responsible or not solely depends on if there is another arsonist that already drop a lit before A or not. This definition of responsibility is quite intuitive and works in many scenarios, but not necessarily all scenarios. In some scenarios, the future part σ_{F} may also need to be taken into account for determining responsibility. We wish to design a lattice of responsibility definitions, each of which adopts a distinct rule of defining responsibility, and for every specific scenario there is at least one definition from the lattice that can handle it well.

Bibliography

[1] Helen Beebee, Christopher Hitchcock, and Peter Menzie. *The Oxford Handbook of Causation*. Oxford University Press, 2009.

[2] Patrick Cousot. *Principles of Abstract Interpretation*. MIT Press, To Be Published in Fall 2021.

[3] Patrick Cousot and Radhia Cousot. "Abstract Interpretation: A Unified Lattice Model for Static Analysis of Programs by Construction or Approximation of Fixpoints". In: *POPL*. ACM, 1977, pp. 238–252.

[4] Patrick Cousot and Radhia Cousot. "Systematic Design of Program Analysis Frameworks". In: *POPL*. ACM Press, 1979, pp. 269–282.

[5] Patrick Cousot and Radhia Cousot. "Abstract Interpretation Frameworks". In: *J. Log. Comput.* 2.4 (1992), pp. 511–547.

[6] Patrick Cousot and Radhia Cousot. "Static determination of dynamic properties of programs". In: *Proceedings of the Second International Symposium on Programming*. Dunod, Paris, France, 1976, pp. 106–130.

[7] Patrick Cousot and Nicolas Halbwachs. "Automatic discovery of linear restraints among variables of a program". In: *Conference Record of the Fifth Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*. Tucson, Arizona: ACM Press, New York, NY, 1978, pp. 84–97.

[8] David Park. “Fixpoint induction and proofs of program properties”. In: *Machine intelligence* 5 (1969).

[9] David Park. “On the semantics of fair parallelism”. In: *Abstract Software Specifications*. Springer. 1980, pp. 504–526.

[10] Bertrand Jeannet and Antoine Miné. “Apron: A Library of Numerical Abstract Domains for Static Analysis”. In: *Computer Aided Verification, 21st International Conference, CAV 2009, Grenoble, France, June 26 - July 2, 2009. Proceedings*. Ed. by Ahmed Bouajjani and Oded Maler. Vol. 5643. Lecture Notes in Computer Science. Springer, 2009, pp. 661–667. DOI: 10.1007/978-3-642-02658-4_52.

[11] Michael R. Clarkson and Fred B. Schneider. “Hyperproperties”. In: *Proceedings of the 21st IEEE Computer Security Foundations Symposium, CSF 2008, Pittsburgh, Pennsylvania, USA, 23-25 June 2008*. IEEE Computer Society, 2008, pp. 51–65. DOI: 10.1109/CSF.2008.7.

[12] Marco Pistoia et al. “Interprocedural Analysis for Privileged Code Placement and Tainted Variable Detection”. In: *ECOOP*. Vol. 3586. Lecture Notes in Computer Science. Springer, 2005, pp. 362–386.

[13] Patrick Cousot et al. “The ASTREÉ Analyzer”. In: *Programming Languages and Systems, 14th European Symposium on Programming,ESOP 2005, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2005, Edinburgh, UK, April 4-8, 2005, Proceedings*. Ed. by Shmuel Sagiv. Vol. 3444. Lecture Notes in Computer Science. Springer, 2005, pp. 21–30. DOI: 10.1007/978-3-540-31987-0_3.

[14] Laurent Mauborgne and Xavier Rival. “Trace Partitioning in Abstract Interpretation Based Static Analyzers”. In: *ESOP*. Vol. 3444. Lecture Notes in Computer Science. Springer, 2005, pp. 5–20.

[15] Caterina Urban and Peter Müller. “An Abstract Interpretation Framework for Input Data Usage”. In: *ESOP*. Vol. 10801. Lecture Notes in Computer Science. Springer, 2018, pp. 683–710.

[16] Radha Jagadeesan et al. “Towards a Theory of Accountability and Audit”. In: *ESORICS*. Vol. 5789. Lecture Notes in Computer Science. Springer, 2009, pp. 152–167.

[17] Bryant Chen, Judea Pearl, and Elias Bareinboim. “Incorporating Knowledge into Structural Equation Models Using Auxiliary Variables”. In: *IJCAI*. IJCAI/AAAI Press, 2016, pp. 3577–3583.

[18] Antoine Miné. “A New Numerical Abstract Domain Based on Difference-Bound Matrices”. In: *Programs as Data Objects, Second Symposium, PADO 2001, Aarhus, Denmark, May 21-23, 2001, Proceedings*. Ed. by Olivier Danvy and Andrzej Filinski. Vol. 2053. Lecture Notes in Computer Science. Springer, 2001, pp. 155–172. DOI: 10.1007/3-540-44978-7_10.

[19] Martín Abadi et al. “A Core Calculus of Dependency”. In: *POPL*. ACM, 1999, pp. 147–160.

[20] Matthias Kuntz, Florian Leitner-Fischer, and Stefan Leue. “From Probabilistic Counterexamples via Causality to Fault Trees”. In: *Computer Safety, Reliability, and Security - 30th International Conference, SAFECOMP 2011, Naples, Italy, September 19-22, 2011. Proceedings*. Ed. by Francesco Flammini, Sandro Bologna, and Valeria Vittorini. Vol. 6894. Lecture Notes in Computer Science. Springer, 2011, pp. 71–84. DOI: 10.1007/978-3-642-24270-0_6.

[21] Roberto Bagnara et al. “Possibly Not Closed Convex Polyhedra and the Parma Polyhedra Library”. In: *Static Analysis, 9th International Symposium, SAS 2002, Madrid, Spain, September 17-20, 2002, Proceedings*. Ed. by Manuel V. Hermenegildo

and Germán Puebla. Vol. 2477. Lecture Notes in Computer Science. Springer, 2002, pp. 213–229. DOI: 10.1007/3-540-45789-5_17.

[22] Alexey Bakhirkin, Josh Berdine, and Nir Piterman. "Backward Analysis via over-Approximate Abstraction and under-Approximate Subtraction". In: *Static Analysis - 21st International Symposium, SAS 2014, Munich, Germany, September 11-13, 2014. Proceedings*. Ed. by Markus Müller-Olm and Helmut Seidl. Vol. 8723. Lecture Notes in Computer Science. Springer, 2014, pp. 34–50. DOI: 10.1007/978-3-319-10936-7_3.

[23] Patrick Cousot. "Abstract Semantic Dependency". In: *Static Analysis - 26th International Symposium, SAS 2019, Porto, Portugal, October 8-11, 2019, Proceedings*. Ed. by Bor-Yuh Evan Chang. Vol. 11822. Lecture Notes in Computer Science. Springer, 2019, pp. 389–410. DOI: 10.1007/978-3-030-32304-2_19.

[24] Chaoqiang Deng and Patrick Cousot. "Responsibility Analysis by Abstract Interpretation". In: *Static Analysis - 26th International Symposium, SAS 2019, Porto, Portugal, October 8-11, 2019, Proceedings*. Ed. by Bor-Yuh Evan Chang. Vol. 11822. Lecture Notes in Computer Science. Springer, 2019, pp. 368–388. DOI: 10.1007/978-3-030-32304-2_18.

[25] Xavier Rival. "Understanding the Origin of Alarms in Astrée". In: *SAS*. Vol. 3672. Lecture Notes in Computer Science. Springer, 2005, pp. 303–319.

[26] Joseph A. Goguen and José Meseguer. "Security Policies and Security Models". In: *IEEE Symposium on Security and Privacy*. IEEE Computer Society, 1982, pp. 11–20.

[27] Adrian Beer et al. "Symbolic Causality Checking Using Bounded Model Checking". In: *Model Checking Software - 22nd International Symposium, SPIN 2015, Stellenbosch, South Africa, August 24-26, 2015, Proceedings*. Ed. by Bernd Fischer

and Jaco Geldenhuys. Vol. 9232. Lecture Notes in Computer Science. Springer, 2015, pp. 203–221. DOI: 10.1007/978-3-319-23404-5_14.

[28] Jonathan Frankle et al. "Practical Accountability of Secret Processes". In: *USENIX Security Symposium*. USENIX Association, 2018, pp. 657–674.

[29] Florian Leitner-Fischer and Stefan Leue. "Causality Checking for Complex System Models". In: *Verification, Model Checking, and Abstract Interpretation, 14th International Conference, VMCAI 2013, Rome, Italy, January 20-22, 2013. Proceedings*. Ed. by Roberto Giacobazzi, Josh Berdine, and Isabella Mastroeni. Vol. 7737. Lecture Notes in Computer Science. Springer, 2013, pp. 248–267. DOI: 10.1007/978-3-642-35873-9_16.

[30] Antoine Miné. "Symbolic Methods to Enhance the Precision of Numerical Abstract Domains". In: *Verification, Model Checking, and Abstract Interpretation, 7th International Conference, VMCAI 2006, Charleston, SC, USA, January 8-10, 2006, Proceedings*. Ed. by E. Allen Emerson and Kedar S. Namjoshi. Vol. 3855. Lecture Notes in Computer Science. Springer, 2006, pp. 348–363. DOI: 10.1007/11609773_23.

[31] Antoine Miné. "The Octagon Abstract Domain". In: *Proceedings of the Eighth Working Conference on Reverse Engineering, WCRE'01, Stuttgart, Germany, October 2-5, 2001*. Ed. by Elizabeth Burd, Peter Aiken, and Rainer Koschke. IEEE Computer Society, 2001, p. 310. DOI: 10.1109/WCRE.2001.957836.

[32] Daniel J. Weitzner et al. "Information accountability". In: *Commun. ACM* 51.6 (2008), pp. 82–87.

[33] Chaoqiang Deng and Patrick Cousot. "Responsibility Analysis by Abstract Interpretation". In: *CoRR* abs/1907.08251 (2019). arXiv: 1907.08251.

[34] Antoine Miné. “Inferring Sufficient Conditions with Backward Polyhedral Under-Approximations”. In: *Electron. Notes Theor. Comput. Sci.* 287 (2012), pp. 89–100. DOI: 10.1016/j.entcs.2012.09.009.

[35] Patrick Cousot et al. “Why does Astrée scale up?” In: *Formal Methods Syst. Des.* 35.3 (2009), pp. 229–264. DOI: 10.1007/s10703-009-0089-6.

[36] Hana Chockler and Joseph Y. Halpern. “Responsibility and Blame: A Structural-Model Approach”. In: *J. Artif. Intell. Res.* 22 (2004), pp. 93–115.

[37] Alejandro Aguirre et al. “A relational logic for higher-order programs”. In: *J. Funct. Program.* 29 (2019), e16. DOI: 10.1017/S0956796819000145.

[38] Antoine Miné. “The octagon abstract domain”. In: *High. Order Symb. Comput.* 19.1 (2006), pp. 31–100. DOI: 10.1007/s10990-006-8609-1.

[39] James Cheney, Amal Ahmed, and Umut A. Acar. “Provenance as dependency analysis”. In: *Mathematical Structures in Computer Science* 21.6 (2011), pp. 1301–1337.

[40] Alejandro Aguirre et al. “A relational logic for higher-order programs”. In: *PACMPL* 1.ICFP (2017), 21:1–21:29.

[41] Roberto Bagnara, Patricia M. Hill, and Enea Zaffanella. “The Parma Polyhedra Library: Toward a complete set of numerical abstractions for the analysis and verification of hardware and software systems”. In: *Sci. Comput. Program.* 72.1-2 (2008), pp. 3–21. DOI: 10.1016/j.scico.2007.08.001.

[42] Antoine Miné. “Backward under-approximations in numeric abstract domains to automatically infer sufficient program conditions”. In: *Sci. Comput. Program.* 93 (2014), pp. 154–182. DOI: 10.1016/j.scico.2013.09.014.

[43] Xavier Rival and Laurent Mauborgne. "The trace partitioning abstract domain". In: *ACM Trans. Program. Lang. Syst.* 29.5 (2007), p. 26.

[44] Bishoksan Kafle et al. "An iterative approach to precondition inference using constrained Horn clauses". In: *Theory Pract. Log. Program.* 18.3-4 (2018), pp. 553–570. DOI: 10.1017/S1471068418000091.

[45] Mark Weiser. "Program Slicing". In: *IEEE Trans. Software Eng.* 10.4 (1984), pp. 352–357.

[46] Henry Frankel. "Harré on Causation". In: *Philosophy of Science* 43.4 (Dec. 1976), pp. 560–569.

[47] Joseph Y. Halpern and Judea Pearl. "Causes and Explanations: A Structural-Model Approach: Part 1: Causes". In: *UAI*. Morgan Kaufmann, 2001, pp. 194–202.

[48] Joseph Y Halpern and Judea Pearl. "Causes and explanations: A structural-model approach. Part I: Causes". In: *The British journal for the philosophy of science* 56.4 (2005), pp. 843–887.

[49] Thomas A Henzinger, Anna Lukina, and Christian Schilling. "Outside the Box: Abstraction-Based Monitoring of Neural Networks". In: *arXiv preprint arXiv:1911.09032* (2019).

[50] Bertrand Jeannet. *The Interproc Analyzer*. URL: http://pop-art.inrialpes.fr/interproc/interprocweb.cgi.

[51] Janusz Laski and William Stanley. "Program Dependencies". In: *Software Verification and Analysis: An Integrated, Hands-On Approach*. London: Springer London, 2009, pp. 125–142. ISBN: 978-1-84882-240-5. DOI: 10.1007/978-1-84882-240-5_6.

[52] Tal Lev-Ami et al. “Backward analysis for inferring quantified preconditions”. In: *Tr-2007-12-01, Tel Aviv University* (2007).

[53] David Lewis. “Causation”. In: *The journal of philosophy* 70.17 (1973), pp. 556–567.

[54] David Lewis. *Counterfactuals*. John Wiley & Sons, 2013.

[55] Antoine Miné. *The Banal Static Analyzer Prototype*. URL: https://www-apr.lip6.fr/-mine/banal/.

[56] Duong Nguyen Que. “Robust and generic abstract domain for static program analyses: the polyhedral case”. PhD thesis. Paris, ENMP, 2010.

[57] Judea Pearl. *Causality: Models, Reasoning and Inference*. 2nd. Cambridge University Press, 2013.

[58] Elies van Sliedregt. *Individual Criminal Responsibility in International Law*. Oxford Monographs in International Law. Oxford University Press, 2012.

[59] Alfred Tarski et al. “A lattice-theoretical fixpoint theorem and its applications.” In: *Pacific journal of Mathematics* 5.2 (1955), pp. 285–309.

[60] Westland J. Christopher. *Structural Equation Models, From Paths to Networks*. Studies in Systems, Decision and Control 22. Springer, 2015.